UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.01 – Writing proofs

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Introduction to proofs

Mathematics as a science is characterised by the concept of mathematical proof. A mathematical proof comprises of a series of logical deductions built from a set of fundamental truths (axioms). A valid mathematical proof establishes the result as truth with complete certainty. (Compare this with the concept of scientific proof, which can only ever be based on empirical results and thus can never be considered completely certain.)

The concept of mathematical proof developed around the time of the Ancient Greeks, most famously celebrated by Euclid's *Elements*, composed around the 3rd century BCE. There is evidence of civilisations practising expansive mathematical knowledge before this point, but these other cultures would accept established mathematical properties as fact without further explanation. In modern mathematics, no claim is accepted as true until it can be logically proven.

Studying this topic

The main subject of this topic is methods of mathematical proof.

There is no general algorithm we can follow to prove an arbitrary statement, so instead we will learn about methods and strategies of proofs by example.

Please note that the technical details we use in each example, and the results of the proofs in each example, are not really what is being tested. Your focus should be on the method of proof in each example, and you should reflect on how these methods can be adapted to proving other statements.

An assessment question based on this topic will likely not resemble anything you have seen before, so the only way you can prepare for the unknown is to practise!

Types of statements that can be proved

- Simple statement

  e.g. The positive square root of 2 is irrational.

- Existential statement

  e.g. There exists some irrational number whose square is 2.

- Universal statement

  e.g. For all rational numbers x, we have $x^2 \neq 2$.

- Conditional statement

  e.g. If x is a rational number, then its square is not 2.

- Negation of a statement (disproof)

  e.g. The claim "the positive square root of 2 is rational" is false.

Types of proof techniques

- Direct proof.

  Deduce the result via a series of logical steps.

- Proof by exhaustion of cases.

  Consider all possible cases and prove them individually.

- Proof by counterexample.

  Disprove a universal statement by finding an example that shows the claim is false.

- Proof by contradiction.

  Assume the result is false and deduce an obviously false conclusion.

- Proof by contrapositive.

  Prove "if A then B" by proving "if not B then not A".

- Proof by induction.

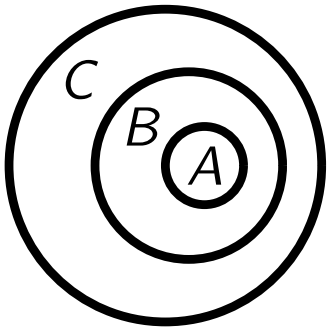
  Prove all cases in a sequence by confirming a base case, and that any case implies its subsequent case.

We will look at each of these proof techniques in detail throughout Topic 3.

Three attempts at a proof

Example. Prove that if A, B, C are sets such that $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Attempt 1



As seen in the Venn diagram, clearly $A \subseteq C$.

Attempt 2

$x \in A \Rightarrow x \in B \quad (A \subseteq B)$
$x \in B \Rightarrow x \in C \quad (B \subseteq C)$
$\therefore A \subseteq C$

Attempt 3

Let $x \in A$.
Then $x \in B$, since $A \subseteq B$.
Hence $x \in C$, since $B \subseteq C$.
So any element of A is an element of C.
That is, $A \subseteq C$. $\square$

Three attempts at a proof – pros and cons

Attempt 1

- Useful for understanding the context/mechanics behind a problem.
- Not easy to follow to an outside observer.
- Diagram dependency is a potential danger.

Attempt 2

- Provides a good step-by-step structure.
- Very dense symbolically and can be difficult to parse. (Symbols like $\therefore$ are almost never seen in published mathematics.)
- This sort of proof might be seen in a more informal context, for example during a tutorial, when the person presenting the proof can provide additional information verbally.

Attempt 3

- This would be considered the best proof of the three. It can be easily read and understood by anyone with sufficient foundational knowledge.
- Though it might look verbose and "less mathematical", it does the best job of communicating the mathematical ideas behind the proof.

What makes a good proof?

Three cornerstones of a good proof are structure, clarity, and readability.

Structure

- Make it clear where your proof begins and ends. For example:
  - The start of a proof can be indicated by the title "**Proof.**"
  - The end of a proof can be stated in words (e.g. "This concludes the proof") or symbolically (by writing an open box, or the letters QED).
- If it is not already provided, write out the statement you aim to prove (preceded by something like "**Theorem.**")
- Follow the standard structure for whatever type of proof you are providing.
  - In this case, the expected structure was "Let $x \in A$ ... Then $x \in C$."
- The logical flow of the proof should be correct and clear.

What makes a good proof?

Clarity

- A proof should be written in complete sentences, with correct spelling, grammar, and punctuation.
  - Every sentence should begin with a capital letter and end with a full stop.
  - A sentence tends to end at the conclusion of a particular thought.
- Every sentence and clause should begin with a word and not a mathematical symbol.
- It is fine (and in fact standard) to write in first person, but never in singular form (use "we", not "I").
- Similarly, we typically write in present tense as opposed to past (or future).

What makes a good proof?

Readability

- Provide reasons or explanations for any step that could otherwise give the reader pause.
- Declare the properties of any new notation introduced.
- Provide the right level of detail. This depends on context and the expectations of the reader.
  - We did not start the previous proof by defining what a set is, or what the subset symbol means.
  - If you needed to use the fact that $A \subseteq B$ and $B \subseteq C$ implies $A \subseteq C$ in a much more complicated proof involving sets, it would probably be safe to omit the proof of this fact.

Variations of a good proof

Example (revisited). Prove that if A, B, C are sets such that $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Version 1

Let $x \in A$.
Then $x \in B$, since $A \subseteq B$.
Hence $x \in C$, since $B \subseteq C$.
So any element of A is also an element of C.
That is, $A \subseteq C$. □

Version 2

Theorem. Given sets A, B, C, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

Proof. We begin by supposing $A \subseteq B$ and $B \subseteq C$. Let x be any element of A. Since $A \subseteq B$, we have that x is also an element of B. Furthermore, since $B \subseteq C$, we have that x is also an element of C. Altogether this means that any element of A is also an element of C, and so A is a subset of C. This concludes the proof.

Both these proof styles are considered good. The first proof is more structured, while the second proof flows better.

Example – Improve the proof

Example. Improve the attempt at a proof provided below.

Theorem. Given any two odd integers m and n, the sum $m+n$ is even.

Let $m = 2a+1$, $n = 2b+1$. then using commutativity and distributivity I found that

$$m + n = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1)$$

$\therefore$ $m+n$ is an even $\mathbb{Z}$.

Theorem. Given any two odd integers m and n, the sum $m+n$ is even.

Proof. Let $m = 2a + 1$, and let $n = 2b + 1$ for some integers a and b. Then we find that

$$m + n = (2a + 1) + (2b + 1) = 2a + 2b + 2 = 2(a + b + 1).$$

Therefore $m + n$ is an even integer, since $a + b + 1$ is itself an integer.

Case study: Mochizuki and the *abc* conjecture

Reminder: "Case studies" are included for fun and are not examinable.

Conjecture: If a, b, c are pairwise coprime positive integers satisfying $a + b = c$, then c is "usually" not divisible by large powers of primes.

In 2012, mathematician Shinichi Mochizuki announced he had proved the *abc* conjecture. His work covered four papers and over 500 pages, however it was largely impenetrable to anyone in the global mathematical community. Several conferences have been held with the single goal to digest and understand Mochizuki's proof.

In 2018, experts in the field came to a contentious decision that there were significant gaps in the proof. To this day, Mochizuki is probably the only person in the world who understands his proof completely.

While the difficulties in understanding Mochizuki's proposed proof lie mainly in the fact it is built upon entirely new mathematical theory, this example certainly goes to show the importance of communication in mathematics!

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.02 – Direct proofs and general techniques

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Direct proofs and general proof techniques

Direct proofs are typically used to verify specific, simple results.

The logical steps of a direct proof are usually straightforward, although their method of discovery can involve working backwards.

The methods we'll see used in the following direct proof examples are also naturally applied to most other proof types – these other types just tend to have additional set-up or specific structure to them.

Example 1 – Straightforward proof

Example. Prove that $\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000000}$.

Working. $\frac{1}{1000} - \frac{1}{1001} = \frac{1001 - 1000}{1000 \times 1001} = \frac{1}{1001000} < \frac{1}{1000000}$.

Proof. Notice that

$$\frac{1}{1000} - \frac{1}{1001} = \frac{1001 - 1000}{1000 \times 1001} = \frac{1}{1001000}.$$

Since $1000000 < 1001000$ and both these numbers are positive, we know that

$$\frac{1}{1001000} < \frac{1}{1000000}.$$

Thus

$$\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000000}.$$

□

Example 1 – Notes

- In our working, we started with the left-hand side (LHS) expression and eventually reached the right-hand side (RHS) via simplification and a comparison argument.
- When writing up the proof, we supplemented the working with words, including explanatory sentences where needed. A proof resembling the working alone would not be sufficient.
- We made sure to follow all the conventions of structure, grammar, etc.
- The statement we were asked to prove is a fairly simple one, so the context implied we should carefully explain each step. If a more complicated problem used this fact as part of a more involved proof, we could get away with just providing the one-line explanation in the working.

Example 2 – Working backwards

Example. Prove that $\dfrac{12344^2 + 24689}{12345^2} = 1.$

Working. Rearranging, we want to show $12345^2 = 12344^2 + 24689$. Rearranging again, we see

$$12345^2 - 12344^2 = (12345 - 12344)(12345 + 12344) = 1 \times 24689.$$

Proof. Notice that

$$12345^2 - 12344^2 = (12345 - 12344)(12345 + 12344) = 1 \times 24689 = 24689.$$

Adding 12344^2 to both sides and dividing through by 12345^2, we arrive at the desired result

$$\frac{12344^2 + 24689}{12345^2} = 1.$$

Example 2 – Notes

- In our working, we started by assuming the given statement was true, and tried manipulating it until it resembled an expression that was obviously true.
- When writing out the proof, we wrote up our working in the opposite direction, starting with the obviously true statement and working back towards the goal.
- It is very important to make sure that all the steps of your proof still work in reverse, and that no information is lost or assumed.
- Can you think of a way to generalise this proof? (See Lecture 3.03.)

"Calculator" proofs

What can be said about this alternative proof of the previous example?

Proof. We have $\dfrac{12344^2 + 24689}{12345^2} = \dfrac{152399025}{152399025} = 1$, as required.

- Direct calculation can be a very useful tool for checking the veracity of a statement.
  - Indeed, increasingly many mathematical proofs are computation-based – though computational proof is not a focus of this course.
- Direct calculation is not always reliable due to inherent limitations of computers.
  - Try telling your favourite (non-mathematical) programming language to evaluate something like `1-1/2-1/3-1/6`.
- A proof that only uses direct calculation is difficult for the reader to follow and verify.
- Such a proof can obfuscate what is happening "under the hood", which can otherwise provide useful insight – for example when trying to generalise a statement.

Example 3 – Working backwards, carefully

Example. Prove that $100! < \sqrt{200!}$. (Note: $n! = 1 \times 2 \times \cdots \times n$.)

Working. Squaring both (positive) sides: $(100!)^2 < 200!$.
Expanding both sides and aligning allows for easy comparison:

$$\begin{aligned} \text{LHS} &= 1 \times 2 \times 3 \times \cdots \times 100 \times \ 1 \ \times \ 2 \ \times \ 3 \ \times \cdots \times 100, \\ \text{RHS} &= 1 \times 2 \times 3 \times \cdots \times 100 \times 101 \times 102 \times 103 \times \cdots \times 200. \end{aligned}$$

Proof. Since $1 < 101$, $2 < 102$, $3 < 103$, ... , $100 < 200$, we have

$$1 \times 2 \times 3 \times \cdots \times 100 < 101 \times 102 \times 103 \times \cdots \times 200.$$

Multiplying both sides by 100! gives

$$\begin{aligned} 100! \times 1 \times 2 \times 3 \times \cdots \times 100 &< 100! \times 101 \times 102 \times 103 \times \cdots \times 200, \\ 100! \times 100! &< 200!. \end{aligned}$$

Both sides of this inequation are clearly positive. Taking the positive square root of both sides then gives the result

$$100! < \sqrt{200!}.$$

Example 3 – Notes

- Similarly to Example 2, we started here by assuming the given statement was true, and tried manipulating it until it resembled an expression that was obviously true.
- The visual alignment used in the working was a helpful aide, and could even have been included in the proof, though the proof provided is slightly more formal.
- When working backwards to write up the proof, we had to be very careful that each step still held true in reverse.
  In particular, in general we cannot assume $x^2 < y^2$ implies $x < y$. For example, $1^2 < (-2)^2$ while $1 \not< -2$.
  The reason we were allowed to reverse this step in this instance is because we additionally knew that both terms in the result were positive – and so this had to be mentioned in the explanation.

What to watch out for when working backwards

We should watch out for the following common mistakes when working backwards through a proof.

- Taking even roots or even powers can break equality or reverse inequality unless additional conditions are met.
  - For example, $x^2 = y^2$ does not imply $x = y$, but does imply $|x| = |y|$.
  - For example, $x^2 < y^2$ does not imply $x < y$, but does imply $|x| < |y|$.
  - For example, $x < y$ does not imply $x^2 < y^2$ unless it is also known that $x, y > 0$.
- Multiplying or dividing an expression by an unknown value can cause information loss or incorrect conclusions in the case that the divisor is zero.
  - For example, $xz = yz$ does not imply $x = y$ unless it is also known that $z \neq 0$.
- In general, a step brought about by applying a non-injective function can only be safely reversed if its pre-image is sensible or additionally restricted.

Example 4 – Working backwards not working

Example. Is it true that for any $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, the expression $ac \equiv bc \pmod{m}$ can be simplified to $a \equiv b \pmod{m}$?

Working. $a \equiv b \pmod{m} \Rightarrow a = b + mk$ for some $k \in \mathbb{Z}$
$\Rightarrow ac = bc + mkc \Rightarrow ac \equiv bc \pmod{m}$ since $kc \in \mathbb{Z}$.

Non-Proof. Suppose $ac \equiv bc \pmod{m}$. Then $ac = bc + mkc$ for some integer kc. Dividing through by c, we find $a = b + mk$, so it follows that $a \equiv b \pmod{m}$ is always true.

What went wrong?

- Everything written in the working is correct, but the argument in reverse no longer holds.
- If kc is an integer, it is not necessarily true that k is an integer.
- If instead the proof had said $ac = bc + mkc$ for some integers k and c, then this would not be true in general, since the quotient might not be a multiple of c (specifically, if $\gcd(c, m) > 1$).
- (Also, we cannot divide through by c in the case that $c = 0$.)

Case study: $1 + 1 = 2$

Theorem. $1 + 1 = 2$.

Between 1910 and 1913, Alfred North Whitehead and Bertrand Russell published a three-volume work titled *Principia Mathematica*. Its goal was to express all mathematical knowledge in terms of formal logic, built only from a minimal set of axioms. While a great achievement of its time, it is probably best known for its proof of the fact $1 + 1 = 2$, which follows after thousands of established propositions over more than 850 pages. Once proven, the text infamously claims, "The above proposition is occasionally useful".

What made Whitehead and Russell's job particularly taxing is that they were trying to prove statements using only the most basic of axioms. But this example goes to show that sometimes even a direct proof of a very simple statement can take a lot of effort!

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.03 – Universal statements and exhaustion of cases

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Universal statements

Definition. A universal statement is a statement of the form

"For all $x \in D$, $P(x)$ is true".

- Here, D is called the domain of disclosure.
- $P(x)$ is some property/statement related to x, known as a proposition.

Notation. The universal quantifier symbol $\forall$ is read as "for all", "for every", "for any", "for each", "given arbitrary", etc.

The general structure for a proof of a universal statement "For all $x \in D$, $P(x)$ is true" is:

Let $x \in D$.
$\vdots$
Then $P(x)$ is true.

To disprove a universal statement, we only need to provide a single counterexample. (See Lecture 3.04)

Examples of universal statements

Exercise. Explain how the following statements are universal statements.

- For all real x, we have x^2 is not negative.
  $\forall x \in \mathbb{R} \quad x^2 \not< 0.$
- The property $P(x+1)$ is true given any integer x.
  $\forall x \in \mathbb{Z} \quad P(x+1)$ is true.
- Every borogove is mimsy.
  $\forall x \in \{\text{borogoves}\} \quad x$ is mimsy.
- The sets A and B satisfy $A \subseteq B$.
  $\forall x \in A \quad x \in B.$
- The functions $f : X \to Y$ and $g : X \to Y$ are equivalent.
  $\forall x \in X \quad f(x) = g(x).$
- The relation R on the set A is reflexive.
  $\forall a \in A \quad a \, R \, a.$

Example 1 – Generalising a previous example

Past example. Prove that $\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000000}$.

Generalised example. Prove that $\frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}$ for all $n \in \mathbb{Z}^+$.

Proof. Let $n \in \mathbb{Z}^+$. Notice that

$$\frac{1}{n} - \frac{1}{n+1} = \frac{(n+1)-n}{n(n+1)} = \frac{1}{n^2+n}.$$

Since $0 < n$, certainly $n^2 < n^2 + n$, and since both sides of this inequation are positive, we know that

$$\frac{1}{n^2+n} < \frac{1}{n^2}.$$

Thus

$$\frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}.$$

□

Example 1 – Notes

- To generalise the statement, we introduced a variable n and gave a natural domain of disclosure ("for all $n \in \mathbb{Z}^+$").
- The original proof didn't change much in structure.
  - Numbers were replaced with terms in n.
  - We added to the start of the proof "Let $n \in \mathbb{Z}^+$."
  - The explanatory sentence was changed slightly to account for the new variable n.
- It would not be sufficient to say "The statement works when $n = 1000$, so we are done." We need to show the statement holds for an infinite number of possible values for n.

Example 2 – Generalising another previous example

Past example. Prove that $\dfrac{12344^2 + 24689}{12345^2} = 1$.

Generalised example. Prove that $\dfrac{n^2 + (2n+1)}{(n+1)^2} = 1$ for all $n \in \mathbb{R} - \{-1\}$.

Proof. Let $n \in \mathbb{R} - \{-1\}$. Then $(n+1)^2 = n^2 + 2n + 1$, and since $n + 1 \neq 0$, we may divide both sides of the equation by $(n+1)^2$ to yield

$$\frac{n^2 + (2n+1)}{(n+1)^2} = 1,$$

as required. □

Example 2 – Notes

- In this case, when generalising the statement we had to be careful about what could and couldn't be included in the domain of disclosure.
- The original proof became far simpler in this case, but notice we still started with "Let $n \in \mathbb{R} - \{-1\}$."
- Can you take a similar approach to generalising Example 3 from Lecture 3.02?

Proof by exhaustion of cases

Sometimes when trying to prove universal statements, we will have to break the approach down into cases.

Typically the domain of disclosure can be partitioned into different groups that are individually easier to handle than the entire domain at once.

- For example, partitioning the reals into negatives and non-negatives.
- For example, partitioning the integers into odd and even numbers.

If the domain of disclosure is finite, it might be possible to consider each case individually.

It's important to make sure that a proof of this sort really has considered all possible cases.

Example 3 – Cases from absolute values

Example. Prove that for all real x we have $|x-3| \leq x^2 - 3x + 4$.

Proof. Let $x \in \mathbb{R}$. Then either $x - 3 \geq 0$ or $x - 3 < 0$. We consider each case in turn.

Case 1. Let $x - 3 \geq 0$. Then $|x-3| = x - 3$, and so we have

$$x^2 - 3x + 4 - |x-3| = x^2 - 4x + 7 = (x-2)^2 + 3 \geq 0,$$

where the final step comes from the fact that the square of any real number is non-negative.

Case 2. Let $x - 3 < 0$. Then $|x-3| = -x + 3$, and so we have

$$x^2 - 3x + 4 - |x-3| = x^2 - 2x + 1 = (x-1)^2 \geq 0,$$

where again the final step comes from the fact that the square of any real number is non-negative.

Having exhausted all possibilities, we can conclude that $x^2 - 3x + 4 - |x-3| \geq 0$ no matter the choice of x, so we have shown that $|x-3| \leq x^2 - 3x + 4$ for all real x.

Example 3 – Notes

- In this example, we split an infinite set of cases into two different infinite sets of cases that were easier to manipulate.
- The absolute value function is a natural indicator for splitting a proof into cases, since it is often not easy to manipulate until its contents is assumed to be positive or negative.
- This example also features the technique of working backwards. The trick of subtracting one side of an inequation from the other and comparing it to 0 is a useful one that can make your working easier and your argument clearer.
- Here we used the fact that the square of any real number is non-negative, which can be stated without proof and is probably the most useful inequality to commit to memory.

Example 4 – Cases from divisibility

Example. Prove that $7n^2 + 8n$ is never prime for any integer n.

Proof. Let $n \in \mathbb{Z}$. Then $7n^2 + 8n = n(7n + 8)$ is a product of two integers. If neither factor is ± 1, the expression is certainly not prime.
So the only cases where the expression might be prime are when $n = 1$, $n = -1$, $7n + 8 = 1$, or $7n + 8 = -1$. We consider each case in turn.

Case 1. Let $n = 1$. Then $7n^2 + 8n = 15$, which is not prime.
Case 2. Let $n = -1$. Then $7n^2 + 8n = -1$, which is not prime.
Case 3. Let $7n + 8 = 1$. Then $n = -1$, and so $7n^2 + 8n = -1$, which is not prime.
Case 4. Let $7n + 8 = -1$. Then $n = -\frac{9}{7}$, which is not an integer.

Since we have now considered all possible cases, we can conclude that $7n^2 + 8n$ is not prime for any integer n.

Example 4 – Notes

- In this example, we split an infinite set of cases into one simpler set of infinite cases and (arguably) four spare cases.
- A common tactic for problems dealing with primes is to try writing an integer as the product of two other integers, and checking whether either of them can be or is forced to be ± 1.

Example 5 – More cases from divisibility

Example. Prove that $n^5 + 4n$ is divisible by 5 for all integers n.

Proof. Let $n \in \mathbb{Z}$. Then in modulo 5, n can be congruent to 0, 1, 2, 3, or 4 only. We consider each case in turn.

Case 1. Let $n \equiv 0 \pmod 5$. Then
$n^5 + 4n \equiv 0^5 + 4 \times 0 \equiv 0 \pmod 5$.

Case 2. Let $n \equiv 1 \pmod 5$. Then
$n^5 + 4n \equiv 1^5 + 4 \times 1 \equiv 5 \equiv 0 \pmod 5$.

Case 3. Let $n \equiv 2 \pmod 5$. Then
$n^5 + 4n \equiv 2^5 + 4 \times 2 \equiv 40 \equiv 0 \pmod 5$.

Case 4. Let $n \equiv 3 \equiv -2 \pmod 5$. Then
$n^5 + 4n \equiv (-2)^5 + 4 \times (-2) \equiv -40 \equiv 0 \pmod 5$.

Case 5. Let $n \equiv 4 \equiv -1 \pmod 5$. Then
$n^5 + 4n \equiv (-1)^5 + 4 \times (-1) \equiv -5 \equiv 0 \pmod 5$.

Since $n^5 + 4n \equiv 0 \pmod 5$ for all possible values of n in modulo 5, we can conclude that $n^5 + 4n$ is divisible by 5 for any integer n.

Example 5 – Notes

- In this example, by introducing modular arithmetic we turned a problem with an infinite set of cases into one with just five cases!
- Considering statements of this kind in appropriate moduli can be a very powerful tool, especially if the result is related to divisibility or remainders.
- A slightly less efficient way to handle this problem without introducing modular arithmetic would be to consider the five cases where $n = 5k, 5k+1, 5k+2, 5k-1$, and $5k-2$ for any integer k.
- A slightly more efficient (though harder to find) approach might have been to notice that

$$n^5 + 4n \equiv n(n-1)(n+1)(n-2)(n+2) \pmod 5.$$

Case study: The Four-Colour Theorem

Theorem. Given any map (a plane separated into contiguous regions), at most four different colours are needed to colour the regions in such a way that no two adjacent regions share the same colour.

Though first conjectured in the mid-1800s, this theorem was not proven until 1976 by Kenneth Appel and Wolfgang Haken. Controversially (at the time), the proof they presented had been verified by computer. Appel and Haken had whittled the problem down to checking 1834 different cases, which were then checked by a computer, apparently taking over one thousand hours. To many, it is surprising that such a simply-stated theorem has only been solved in a comparatively complicated way, though no alternative method of proof has yet been found (however the initial number of cases to check has been gradually reduced over time).

This example goes to show that sometimes a proof by exhaustion of cases really can be exhausting! But if it gets the job done in a finite amount of time, it's as good as any other method of proof.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.04 – Existential statements and counterexamples

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Existential statements

Definition. An existential statement is a statement of the form

"There exists $x \in D$, such that $P(x)$ is true".

Note that the "such that" can sometimes be omitted, but this doesn't change the meaning, and usually including the "such that" phrase will improve readability.

Notation. The existential quantifier symbol $\exists$ is read as "there exists", "there is some", "for some", "for at least one", "for a particular", etc.

The general structure for a proof of an existential statement "There exists $x \in D$, such that $P(x)$ is true" is:

Choose $x \in D$ to be ...
⋮
Then $P(x)$ is true.

To disprove an existential statement, we need to show the property doesn't hold for every element in the domain (a universal statement).

Examples of existential statements

Exercise. Explain how the following statements are existential statements.

- There exists a real number x such that x^2 is not positive.
  $\exists x \in \mathbb{R} \quad x^2 \not> 0.$
- $\sqrt{x} > x$ for some rational x.
  $\exists x \in \mathbb{Q} \quad \sqrt{x} > x.$
- At least one bandersnatch is frumious.
  $\exists x \in \{\text{bandersnatches}\} \quad x \text{ is frumious.}$
- The set $A \cap B$ is not empty.
  $\exists x \in A \quad x \in B.$
- The real function curves $y = f(x)$ and $y = g(x)$ intersect.
  $\exists x \in \mathbb{R} \quad f(x) = g(x).$
- $a \equiv b \pmod{m}$.
  $\exists k \in \mathbb{Z} \quad a = b + mk.$

Example 1 – Easy existence

Example. Prove that there exist distinct positive integers a and b such that $a^b = b^a$.

Proof. Choose $a = 2$ and $b = 4$. Then

$$a^b = 2^4 = 16 = 4^2 = b^a.$$

Since both a and b are distinct positive integers here, we have proven the statement to be true.

Example 1 – Notes

- The only sensible way to find our solution was to guess and check by testing small values. While this will not always be an efficient technique, it can be a powerful time-saver in certain cases.
- We did not explain in the proof how we found our solution; we just declared it and showed that it satisfied the conditions.
- It turns out the solution we gave is the only possible one for this question, though note we did not have to prove this fact.

Example 2 – Harder existence

Example. Prove that $4^n < n!$ for some non-negative integer n.

Proof. Choose $n = 18$. Then by comparing aligned terms in the expanded product, we can see that

$$\begin{aligned} 18! &= 1 \times 2 \times 3 \times 4 \times 5 \times \cdots \times 15 \times 16 \times 17 \times 18 \\ &> 1 \times 2 \times 3 \times \underbrace{4 \times 4 \times \cdots \times 4}_{\text{12 times}} \times 4^2 \times 4^2 \times 4^2 \\ &> 4^{18}. \end{aligned}$$

So we have found that $4^{18} < 18!$, thus proving the claim.

Example 2 – Notes

- Here, the given solution was likely found by gradually increasing the value of n until it clearly satisfied the requirements.
- Notice that the smallest possible solution to the inequation is $n = 9$, but there is nothing wrong with providing a suboptimal solution, since we are only interested in proving the existence of any solution at all.
- Notice also that we could have used even simpler arguments by choosing even larger values of n, for example $n = 4^4$.

Example 3 – A non-constructive proof

Example. Prove that $e^x = 3x^3$ has a solution over the reals.

Proof. Set $f(x) = e^x - 3x^3$. Then $e^x = 3x^3$ has a solution precisely when $f(x) = 0$.

Choose $x = 0$ and $x = 1$. Then

$$f(0) = 1 > 0 \quad \text{and} \quad f(1) = e - 3 < 0.$$

Since $f(x)$ is continuous, it must cross the x-axis somewhere between $x = 0$ and $x = 1$ (by the Intermediate Value Theorem). That is, $f(x) = 0$ for some $x \in (0, 1)$, which means $e^x = 3x^3$ has at least one real solution.

Example 3 – Notes

- This existential statement was proven using a non-constructive proof, which means the existence of a solution was proven, but not explicitly provided.
- We made use of continuity and the Intermediate Value Theorem here, which is assumed knowledge, but is not a focus of the Discrete Mathematics course.
- This example demonstrates how it can be useful to introduce new notation (like $f(x)$ here) to help improve the clarity and readability of an argument.

Example 4 – The Division Theorem (partial)

Example. Let a and $b \neq 0$ be integers. Prove that there exist integers q and r satisfying $a = bq + r$ and $0 \leq r < |b|$.

Proof. First consider the case where $b > 0$.

Choose $q = \left\lfloor \frac{a}{b} \right\rfloor$, and then $r = a - bq$, which are both well-defined ($b \neq 0$) and clearly integers. Then we have $a = bq + r$ as required, and furthermore

$$q \leq \frac{a}{b} < q + 1$$

by definition of the floor function. Subtracting q from each expression and then multiplying each expression by the positive integer b, we get

$$0 \leq a - bq < b,$$

which is equivalent to the inequations $0 \leq r < |b|$ (since $b > 0$) as required.

The case where $b < 0$ works simiarly, except that we set $q = \left\lceil \frac{a}{b} \right\rceil$.

Example 4 – Notes

- In this example, the statement began by declaring the fixed variables a and b. Notice that we were not allowed to choose what values a and b took, but that our solution did define q and r in terms of a and b.
- On the other hand, it can certainly help to pick specific values for fixed variables like a and b here, to help get a handle on what sort of roles they play and to try to predict how they will be used in the generalised proof.
- This of course proves part of the Division Theorem – but can we also prove that the values found for q and r are unique?

Example 4^+ – The Division Theorem (complete)

Example. Let a and $b \neq 0$ be integers. Prove that there exist unique integers q and r satisfying $a = bq + r$ and $0 \leq r < |b|$.

Proof. We have already shown that there is at least one possible construction giving $a = bq + r$ with $0 \leq r < |b|$. Suppose there is a second solution $a = bq' + r'$ with $0 \leq r' < |b|$. Then equating both values for a and rearranging, we find

$$b(q - q') = r' - r.$$

Notice that because each of r and r' can be at least 0 and at most $|b| - 1$, we have that $-b < r' - r < b$. Since $r' - r = b(q - q')$ is an integer multiple of b, the only value it can take strictly between $-b$ and b is 0. Thus $r = r'$ and $q = q'$, meaning there is only one possible value for each of q and r.

Example 4^+ – Notes

- The general structure for proving uniqueness of a solution to an existential statement "There exists a unique $x \in D$, such that $P(x)$ is true" is:

  Suppose $x, x' \in D$ and both $P(x)$ and $P(x')$ are true.
  $\vdots$
  Then $x = x'$.

  Does this sort of proof structure look familiar?

- Sometimes the symbols $\exists!$ are used to mean "there uniquely exists".

Proof by counterexample

Typically when trying to disprove universal statements, we will want to provide a counterexample.

Counterexample proofs are often short, simply stating the counterexample and explaining why it disproves the statement.

Often the trickiest part of proving by counterexample is finding the counterexample itself. But when it comes to writing up the proof, we usually do not explain the derivation of the counterexample.

It's important to make sure your counterexample comes from the domain of disclosure, and to show that it really doesn't satisfy the property being disproved.

Example 5 – Mutual divisibility

Example. Disprove the following statement: For all integers a and b, if $a \mid b$ and $b \mid a$, then $a = b$.

Proof. Choose $a = 1$ and $b = -1$. Then we have

$$1 \mid (-1) \quad \text{and} \quad (-1) \mid 1,$$

but clearly $a \neq b$. Thus we have disproved the statement by counterexample.

Example 5 – Notes

- As before, we could have provided many different counterexamples (e.g. $a = 2$, $b = -2$), but only needed to provide one to disprove the claim.
- We could also have provided a more general counterexample, for example by choosing $b = -a$. However we would need to be a little more careful in our explanation (what if $a = 0$?), and might need to give more explanation (it would be good to justify why $a \mid (-a)$). Because of this, in general we tend to prefer specific counterexamples to more general ones.

Example 6 – Unequal functions

Example. Show that the functions $f, g : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \left\lfloor x + \frac{1}{2} \right\rfloor$ and $g(x) = \left\lceil x - \frac{1}{2} \right\rceil$ are not equal.

Proof. Choose $x = \frac{1}{2}$. Then $f\left(\frac{1}{2}\right) = \left\lfloor 1 \right\rfloor = 1$, while $g\left(\frac{1}{2}\right) = \left\lceil 0 \right\rceil = 0$. Since $f(x)$ does not return the same value as $g(x)$ for at least one value of x, the functions f and g are not equal.

Example 6 – Notes

- While there were infinitely many possible counterexamples to choose here, it's possible none may have been obvious to you before trying to sketch a graph of the two functions.
- Notice that claiming two functions are equal is a universal statement, which is why showing two functions are not equal can be proven with a counterexample.

Case study: Perfect numbers

A perfect number is an integer that is equal to the sum of its positive proper divisors. (A proper divisor of a number is any divisor other than the number itself.) The first few perfect numbers are $6, 28, 496, 8128, 33550336, \ldots$

Theorem (Euclid-Euler). All even perfect numbers are of the form $2^{p-1}(2^p - 1)$ whenever both p and $2^p - 1$ are prime.

Conjecture. There are no odd perfect numbers.

Remarkably, we know exactly how to generate a list of all even perfect numbers, but it is not known if an odd perfect number exists. Many mathematicians have attempted to either find an odd perfect number or prove the non-existence of odd perfect numbers, but not much progress has been made in either pursuit. To date, all odd numbers up to 10^{1500} have been checked!

Would we expect that the existential proof or the counterexample is likely to be the easier approach to this particular conjecture?

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.05 – Conditional statements, converses, and biconditionals

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Conditional statements

Definition. A conditional statement is a statement of the form

"If P is true, then Q is true".

Notation. The implication symbol $\Rightarrow$, in the context of an expression like "$P \Rightarrow Q$", is read as "P implies Q", "if P is true then Q is true", "whenever P is true, Q is true", "Q is true if P is true", "P is true only if Q is true", "P is a sufficient condition for Q", "Q is a necessary condition for P", etc.

- The example using "only if" is particularly easy to get confused, because it does not always translate to English sensibly.
- Notice that any universal statement ("For all $x \in D$, $P(x)$ is true") can be written as a conditional statement ("If $x \in D$, then $P(x)$ is true").

The general structure for a proof of a conditional statement "If P is true, then Q is true" is:

Suppose P is true.

$\vdots$

Then Q is true.

To disprove a conditional statement "If P is true, then Q is true", we must provide a counterexample where P is true but Q is false.

Examples of conditional statements

Example. Explain how the following statements are conditional statements.

- If $P(x)$ is true, then $P(x+1)$ is true.
  $P(x) \Rightarrow P(x+1)$.
- Whenever a number is real, its square is non-negative.
  $x \in \mathbb{R} \Rightarrow x^2 \geq 0$.
- You will lose if you battle Cynthia.
  Battling Cynthia $\Rightarrow$ losing.
- You will lose only if you battle Cynthia.
  Losing $\Rightarrow$ battling Cynthia.
  (The only way you can lose is if you battle Cynthia.)
- The relation represented by the set of ordered pairs R is symmetric.
  $(x, y) \in R \Rightarrow (y, x) \in R$.

Notice "if you've studied, you will pass" means the same as "you've studied only if you will pass", though the latter makes less sense in English.

Example 1 – Equivalence classes

Example. Prove that given an equivalence relation $\sim$ on a set X and elements $x, y \in X$, if $x \sim y$, then $[x] = [y]$.

Proof. Suppose $x \sim y$. Then we wish to show the sets $[x]$ and $[y]$ are equal.

Let $a \in [x]$. Then $a \sim x$, and so since we also have $x \sim y$, we have $a \sim y$ by the transitivity of $\sim$. So $a \in [y]$, and thus $[x] \subseteq [y]$.

Now let $a \in [y]$. Then $a \sim y$. Also, since $x \sim y$ we have $y \sim x$ by the symmetry of $\sim$. Thus by the transitivity of $\sim$, we know $a \sim x$, and so $a \in [x]$. Thus $[y] \subseteq [x]$.

Therefore since both sets are subsets of each other, we have $[x] = [y]$ as required.

Example 1 – Notes

- We followed the expected structure for a proof of a conditional statement "$P \Rightarrow Q$" by starting with "Suppose P is true" and ending with "Thus Q is true."
  - Nested inside this structure was the standard proof structure for showing that two sets are equal (which we have seen is a universal statement).
- Note that since we were given that $\sim$ is an equivalence relation, we could freely use the properties of equivalence without having to prove or assume anything.

Example 2 – Modular multiplication

Example. Prove that given $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, if $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$.

Proof. Suppose $a \equiv b \pmod{m}$. Then we can write $a = b + mk$ for some integer k. Multiplying both sides by c gives $ac = bc + mkc$, which means $ac \equiv bc \pmod{m}$ since kc is an integer. □

Converse statements

Definition. The converse of a conditional statement "If P is true, then Q is true" is the conditional statement

"If Q is true, then P is true".

Notation. The reverse implication symbol $\Leftarrow$ can replace the implication symbol in an expression to create its converse. That is, the converse of $P \Rightarrow Q$ is $P \Leftarrow Q$, although it is more natural to write the converse as $Q \Rightarrow P$.

It is very important to note that the converse of a statement is independent of the original statement. Whether a statement is true has no bearing on whether its converse is true.

For example, "If it's raining, it's cloudy" is always true, but the converse statement "If it's cloudy, it's raining" is not always true.

In particular, we cannot prove $P \Rightarrow Q$ by showing that $Q \Rightarrow P$. Thinking otherwise is known as the converse fallacy.

Examples of converse statements

Exercise. Write the converse of each statement below, and decide which statements/converse statements are true.

- If a triangle's sides are all equal, then its interior angles are all equal.
  Converse: If a triangle's interior angles are all equal, then its sides are all equal. (True)
- If a quadrilateral is a square, then its sides are all equal.
  Converse: If a quadrilateral's sides are all equal, then it is a square. (False)
- If it's a tiger, it has stripes.
  Converse: If it has stripes, it's a tiger. (False)
- If it's a tiger, it has tiger offspring.
  Converse: If it has tiger offspring, it's a tiger. (True)
- The equivalence relation R is symmetric.
  Converse: The equivalence relation R is symmetric. (True)
  (This is because the converse of $(x, y) \in R \Rightarrow (y, x) \in R$ is $(y, x) \in R \Rightarrow (x, y) \in R$.)

Example 3 – Equivalence classes – converse

Example. Given an equivalence relation $\sim$ on a set X and elements $x, y \in X$, is the converse of "if $x \sim y$, then $[x] = [y]$" true?

Proof. We shall show that the converse is true. That is, we shall prove that if $[x] = [y]$, then $x \sim y$.

Suppose $[x] = [y]$. Since $\sim$ is reflexive, we know $x \sim x$, so $x \in [x]$. Thus $x \in [y]$, which means $x \sim y$ as required.

Example 3 – Notes

- Since the example here asked whether the converse is true, we must start by declaring whether we believe the statement to be true or not, and provide a proof or disproof.
- Notice that in this case, the proof of the converse was more straightforward than the original proof.

Example 4 – Modular division

Example. Given $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, is the converse of "if $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$" true?

Proof. We shall show that the converse is false. That is, we shall disprove that if $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.

We proceed by providing a counterexample.
Notice that $16 \equiv 4 \pmod{6}$, so we have $ac \equiv bc \pmod{m}$ where $a = 4$, $b = 1$, $c = 4$, and $m = 6$.
However the claim "$a \equiv b \pmod{m}$" is then false, since clearly $4 \not\equiv 1 \pmod{6}$. □

Example 4 – Notes

- Here we disproved a statement "if P is true, then Q is true" by finding a counterexample, specifically a case where P was true but Q was false.
- As before with proofs by counterexample, we didn't need to supply any motivation or reasoning for our choices of a, b, c, m, and only had to demonstrate that they disprove the claim.

Biconditional statements

Definition. A biconditional statement is a statement of the form

"P is true if and only if Q is true".

It means "both $P \Rightarrow Q$ and $Q \Rightarrow P$". The term "iff" is often used as shorthand for "if and only if."

Notation. The double implication symbol $\Leftrightarrow$, in the context of an expression like "$P \Leftrightarrow Q$", is read as "P if and only if Q", "P iff Q", "P exactly when Q", "P is equivalent to Q", "P implies Q and Q implies P", "P is a necessary and sufficient condition for Q", etc.

The general structure for a proof of a biconditional statement "P is true if and only if Q is true" is:

Suppose P is true.
$\vdots$
Then Q is true.
Conversely, suppose Q is true.
$\vdots$
Then P is true.

To disprove a biconditional statement, we only have to disprove either implication direction.

Examples of biconditional statements

Exercise. Explain how the following statements are biconditional statements.

- Given an equivalence relation $\sim$, we have $a \sim b$ exactly when $[a] = [b]$.
  $a \sim b \Leftrightarrow [a] = [b]$.
- An equilateral triangle is the same thing as an equiangular triangle.
  A triangle has equal sides $\Leftrightarrow$ a triangle has equal angles.
- Being a tiger is a necessary and sufficient condition for having tiger offspring.
  It's a tiger $\Leftrightarrow$ it has tiger offspring.
- If you past the test then you will get cake, and conversely.
  You pass the test $\Leftrightarrow$ you get cake.
- The sets A and B satisfy $A = B$.
  $x \in A \Leftrightarrow x \in B$.

Example 5 – Divisibility

Example. Given $a, b, d \in \mathbb{Z}$ with $\gcd(a, d) = 1$, prove that $d \mid b$ if and only if $d \mid ab$.

Proof. We prove both implication directions in turn.

Forward implication. We want to show that if $d \mid b$, then $d \mid ab$.

Suppose $d \mid b$. Then $b = dk$ for some integer k. Multiplying both sides by a gives $ab = adk = d(ak)$, which means that $d \mid ab$ since ak is an integer.

Backward implication. We want to show that if $d \mid ab$, then $d \mid b$.

Suppose $d \mid ab$. Then $ab = dk$ for some integer k. Since $\gcd(a, d) = 1$, we know by Bézout's identity that $1 = ax + dy$ for some integers x and y. Multiplying both sides by b gives

$$b = abx + bdy = dkx + bdy = d(kx + by).$$

Since $kx + by$ is an integer, it follows that $d \mid b$.

With both implication directions proven, we can conclude that the biconditional statement is proven. □

Example 5 – Notes

- Here we proved the biconditional by providing two separate proofs, which we called the forward and backward implications.
  - It's convenient to label each proof somehow, for example with subtitles or by clearly declaring the start and end of each proof.
  - It can also be useful to write out what each implication direction means before attempting to prove it (though be sure to indicate that it has yet to be proven, for example by saying "We want to show that...").
- Notice that proving one direction was somewhat simpler than the other direction. Notice also that the proof for the backward implication is not just the proof for the forward implication written backwards!
  - Sometimes a proof may work in both directions, but it is still recommended to write out a separate proof for each implication direction.

Case study: The four-vertex theorem

The curvature of a curve is a measurement of the "roundness" of the curve at any particular point. Its value is the reciprocal of the radius of the circle most closely resembling the curve at that point.

The curvature of a curve typically changes as we travel along the curve. If we imagine a graph plotting the change in curvature while travelling along the curve, this graph can have local maxima and minima, which are known as vertices. Intuitively, they are the points where the curve is locally "most or least round."

Theorem. A continuous planar curve is simple (doesn't cross itself) and closed (forms a loop) if and only if it has at least four vertices.

The forward direction of this statement (which feels more intuitive in practice) was proven by Alfred Kneser in 1912.

Interestingly, it took another 85 years for the reverse direction of this statement to be proven by Björn Dahlberg in 1997. This serves as a perhaps extreme demonstration of the fact that sometimes proving one direction of a biconditional statement can be significantly easier than the other!

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.06 – Multiple quantifiers and negation

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Multiple quantifiers

It is possible for a statement to contain more than one quantifier.

For example, the statement "every real number has an additive inverse" can be interpreted as "for any real number, there exists another real number such that their sum is zero."

This example would be written symbolically as

$$\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R} \quad x + y = 0.$$

The general structure for a proof of a statement using multiple quantifiers is built by adapting the proof style for each clause in turn. For example, the general structure for proving the statement "for all $x \in D_1$, there exists $y \in D_2$ such that $P(x, y)$ is true" is:

Let $x \in D_1$.
Choose $y \in D_2$ to be ...
⋮
Then $P(x, y)$ is true.

Multiple quantifiers – order

Typically, the order in which the quantifiers appear is important.

- $\forall x \in D_1 \quad \forall y \in D_2 \quad P(x, y)$ is true means the same as
  $\forall y \in D_2 \quad \forall x \in D_1 \quad P(x, y)$ is true.

  If $D_1 = D_2$, we can also write: $\forall x, y \in D_1 \quad P(x, y)$ is true.

- $\exists x \in D_1 \quad \exists y \in D_2 \quad P(x, y)$ is true means the same as
  $\exists y \in D_2 \quad \exists x \in D_1 \quad P(x, y)$ is true.

  If $D_1 = D_2$, we can also write: $\exists x, y \in D_1 \quad P(x, y)$ is true.

- $\forall x \in D_1 \quad \exists y \in D_2 \quad P(x, y)$ is true does not mean the same as
  $\exists y \in D_2 \quad \forall x \in D_1 \quad P(x, y)$ is true.

  Consider for example the statements

$$\forall x \in \mathbb{R}^+ \quad \exists y \in \mathbb{R}^+ \quad y^2 = x, \quad \text{and}$$
$$\exists y \in \mathbb{R}^+ \quad \forall x \in \mathbb{R}^+ \quad y^2 = x.$$

  The first statement says "every positive real has a positive real square root", which is true. The second statement says "there is a positive real whose square is every positive real", which is false.

Reading statements with multiple quantifiers

Exercise. Interpret each of the following statements.

- $\forall x \in \{\text{dogs}\} \quad \forall y \in \{\text{people}\} \quad y$ likes x.
  Everyone likes every dog.
- $\exists x \in \{\text{dogs}\} \quad \exists y \in \{\text{people}\} \quad y$ likes x.
  Someone likes a particular dog.
- $\forall x \in \{\text{dogs}\} \quad \exists y \in \{\text{people}\} \quad y$ likes x.
  Each dog is liked by someone.
- $\exists y \in \{\text{people}\} \quad \forall x \in \{\text{dogs}\} \quad y$ likes x.
  Someone likes all the dogs.
- $\exists x \in \{\text{dogs}\} \quad \forall y \in \{\text{people}\} \quad y$ likes x.
  A particular dog is liked by everyone.
- $\forall y \in \{\text{people}\} \quad \exists x \in \{\text{dogs}\} \quad y$ likes x.
  Every person has a dog that they like.

Examples of statements with multiple quantifiers

Exercise. Rewrite the following statements using multiple quantifiers.

- There are integers x and y such that $1 = 2x + 3y$.
  $\exists x \in \mathbb{Z} \quad \exists y \in \mathbb{Z} \quad 1 = 2x + 3y.$
- Set intersection is a commutative operation.
  $\forall A \subseteq \mathcal{U} \quad \forall B \subseteq \mathcal{U} \quad A \cap B = B \cap A.$
- There is a real number that doesn't change the value of any real number it is multiplied by.
  $\exists x \in \mathbb{R} \quad \forall y \in \mathbb{R} \quad xy = y.$
- Every non-zero real number has a multiplicative inverse.
  $\forall x \in \mathbb{R} - \{0\} \quad \exists y \in \mathbb{R} \quad xy = 1.$
- The function $f : X \to Y$ is surjective.
  $\forall y \in Y \quad \exists x \in X \quad f(x) = y.$
- The function $f : X \to Y$ is injective.
  $\forall x_1 \in X \quad \forall x_2 \in X \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$
- The poset $(S, \preceq)$ has a greatest element.
  $\exists x \in S \quad \forall y \in S \quad y \preceq x.$

Example 1 – Bounded function

Example. A real function $f(x)$ is bounded if and only if

$$\exists M \in \mathbb{R}^+ \quad \forall x \in \mathbb{R} \quad |f(x)| \leq M.$$

Prove that the function $f(x) = 3\sin(x) + 2$ is bounded.

Proof. Choose the bounding value M to be 5, and let $x \in \mathbb{R}$. We know that $|\sin(x)| \leq 1$, so

$$|f(x)| = |3\sin(x) + 2| \leq |3\sin(x)| + |2| = 3|\sin(x)| + 2 \leq 3 \times 1 + 2 = 5$$

(where the first inequation above comes from the triangle inequality).

We have therefore found a bounding value $M \in \mathbb{R}^+$ (namely $M = 5$) that satisfies $|f(x)| \leq M$ for all real x, and so the function is indeed bounded.

Example 1 – Notes

- Here the statement we wanted to prove began with an existential clause followed by a universal clause, so our proof started with a "choose..." clause followed by a "let..." clause.
- As we have seen before, we didn't give any derivation or motivation for our choice of M when proving the existential clause.

Example 2 – Limit of a function at infinity

Example. The limit of a real function $f(x)$ as x approaches infinity exists and has value L if and only if

$$\forall \varepsilon \in \mathbb{R}^+ \quad \exists N \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad x > N \Rightarrow |f(x) - L| < \varepsilon.$$

Prove that the limit of $f(x) = \dfrac{x+1}{x}$ as x approaches infinity is 1.

Proof. Let $\varepsilon \in \mathbb{R}^+$. Choose the threshold value N to be $\frac{1}{\varepsilon}$, and let $x \in \mathbb{R}$. Suppose that $x > N$.

Then in particular, we have $x > \frac{1}{\varepsilon}$, and so

$$|f(x) - 1| = \left|\frac{x+1}{x} - 1\right| = \left|\frac{1}{x}\right| = \frac{1}{x} < \varepsilon,$$

where we were able to ignore the absolute value function since ε and hence x are both positive.

We have therefore found a threshold value $N \in \mathbb{R}$ for any positive real ε (namely $N = \frac{1}{\varepsilon}$) that satisfies $|f(x) - 1| < \varepsilon$ for all real $x > N$, and so the limit of $f(x)$ as x approaches infinity is indeed 1.

Example 2 – Notes

- The statement here was a little more complicated, but could still be parsed by interpreting each clause in turn. The clauses in order were universal, existential, universal, conditional, and so our proof structure started with the skeleton "Let..., choose..., let..., suppose..."
- Notice that typically when an existential clause follows a universal clause, the value we choose for the existential variable will most likely be in terms of the universal variable.
- Notice that in the last line when we said "for all real $x > N$", this was really conflating the two facts "for all real x whenever $x > N$."

Negation

Definition. The negation of a statement is a statement that is true precisely when the original statement is false.

Notation. The negation symbol $\sim$ is read as "not", "never", etc. Some texts might instead use the symbol $\neg$.

The negation of a simple statement is the "opposite" statement:

- $\sim (x = y)$ means the same as $x \neq y$.
- $\sim (x \leq y)$ means the same as $x \not\leq y$, that is, $x > y$.
- $\sim (A \subseteq B)$ means the same as $A \not\subseteq B$.

The negation of a universal statement "$\forall x \in D, P(x)$ is true" is the existential statement "$\exists x \in D$ such that $P(x)$ is false."

The negation of an existential statement "$\exists x \in D$ such that $P(x)$ is true" is the universal statement "$\forall x \in D, P(x)$ is false."

The negation of a conditional statement "$P \Rightarrow Q$" is the statement "P is true and Q is false."

The negation of a biconditional statement "$P \Leftrightarrow Q$" is the statement "$\sim (P \Rightarrow Q)$ or $\sim (Q \Rightarrow P)$."

Examples of statement negations

Example. Write the negation of each statement below.

- For all real x, we have x^2 is positive.
  $\exists x \in \mathbb{R} \quad x^2 \leq 0.$
- $x < \sqrt{x}$ for some natural number x.
  $\forall x \in \mathbb{N} \quad x \geq \sqrt{x}.$
- You will lose if you battle Cynthia.
  You will battle Cynthia and win.
- You will get cake if and only if you pass the test.
  You got the cake and didn't pass the test, or
  you passed the test and didn't get cake.
- The sets A and B satisfy $A \subseteq B$.
  $\exists x \in A \quad x \notin B.$
- The real function curves $y = f(x)$ and $y = g(x)$ intersect.
  $\forall x \in \mathbb{R} \quad f(x) \neq g(x).$
- For all integers x, whenever $12 \mid x^2$ we have $12 \mid x$.
  $\exists x \in \mathbb{Z} \quad 12 \mid x^2$ and $12 \nmid x.$

Negating multiple quantifiers

When negating a statement with multiple quantifiers, simply negate each quantifying component in turn. For example, the following statements are all equivalent:

- $\sim (\exists x \quad \forall y \quad \exists z \quad P(x,y,z) \text{ is true}).$
- $\forall x \quad \sim (\forall y \quad \exists z \quad P(x,y,z) \text{ is true}).$
- $\forall x \quad \exists y \quad \sim (\exists z \quad P(x,y,z) \text{ is true}).$
- $\forall x \quad \exists y \quad \forall z \quad \sim (P(x,y,z) \text{ is true}).$
- $\forall x \quad \exists y \quad \forall z \quad P(x,y,z) \text{ is false}.$

Exercise. Rewrite each statement below both with and without the negation symbol.

- The function $f : X \to Y$ is not surjective.
  $\sim (\forall y \in Y \quad \exists x \in X \quad f(x) = y).$
  $\exists y \in Y \quad \forall x \in X \quad f(x) \neq y.$
- The function $f : X \to Y$ is not injective.
  $\sim (\forall x_1 \in X \quad \forall x_2 \in X \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$
  $\exists x_1 \in X \quad \exists x_2 \in X \quad f(x_1) = f(x_2) \text{ and } x_1 \neq x_2.$

Example 3 – Unbounded function

Example. A real function $f(x)$ is bounded if and only if

$$\exists M \in \mathbb{R}^+ \quad \forall x \in \mathbb{R} \quad |f(x)| \leq M.$$

Prove that the function $f(x) = \sqrt{x}$ is unbounded.

Proof. Let $M \in \mathbb{R}^+$, and choose $x = (M+1)^2$. Then clearly $x \in \mathbb{R}$, and

$$|f(x)| = |\sqrt{x}| = |\sqrt{(M+1)^2}| = M + 1 > M.$$

We have therefore found that for any proposed bounding value $M \in \mathbb{R}^+$, there is some $x \in \mathbb{R}$ (namely $x = (M+1)^2$) such that $|f(x)| > M$, and so $f(x)$ is indeed unbounded.

Example 3 – Notes

- We showed the function was unbounded by disproving the statement corresponding to $f(x)$ being bounded. This meant proving the negation of the definition of boundedness.
- The statement we were trying to prove contained a universal clause ("for all M") followed by an existential clause ("there exists an x"), and we saw once again that the existential variable we chose was given in terms of the universal one (x was given in terms of M).
- The choice of x was not the only valid one. We could have used the tighter bound $x = M^2 + 1$, for example, though our choice of $x = (M + 1)^2$ made the argument easier to follow.

Example 4 – Non-limit of a function at infinity

Example. The limit of a real function $f(x)$ as x approaches infinity exists and has value L if and only if

$$\forall \varepsilon \in \mathbb{R}^+ \quad \exists N \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad x > N \Rightarrow |f(x) - L| < \varepsilon.$$

Prove that the limit of $f(x) = \dfrac{x+1}{x}$ as x approaches infinity is not 0.

Proof. Choose $\varepsilon = 1$. Let $N \in \mathbb{R}$, and choose $x = |N| + 1$. Then clearly $x > N$, and since $x > 0$,

$$|f(x) - 0| = \left|\frac{x+1}{x} - 0\right| = \frac{x+1}{x} = 1 + \frac{1}{x} > 1 = \varepsilon.$$

We have therefore found a positive real ε (namely $\varepsilon = 1$) such that for any real number N, there is a real number x (namely $x = |N| + 1$) such that $x > N$ and $|f(x) - 0| \not< \varepsilon$. So the limit of $f(x)$ as x approaches infinity is not 0.

Example 4 – Notes

- We showed the limit of the function was not 0 by disproving the affirmative statement. This meant proving the negation of the definition of a limit at infinity.
- The statement we were trying to prove contained a universal clause ("for all N") followed by an existential clause ("there exists an x"), and we saw once again that the existential variable we chose was given in terms of the universal one (x was given in terms of N).
- The choices of ε and x could be tricky to motivate before drawing a sketch of the situation. There are of course other possible choices for these variables that you may have used.

Case study: Complexity of algorithmic multiplication

The time complexity of an algorithm measures the amount of time taken for the algorithm to run as a function of the length of its input. Using "Big O" asymptotic notation, an algorithm with linear time complexity has complexity $O(n)$.

In 1960, Andrey Kolmogorov presented the following conjecture.

Conjecture. The most efficient algorithm for multiplying two n-digit numbers has computational complexity $O(n^2)$.

Within one week, Anatoly Karatsuba had proven that this conjecture was false. He provided a counterexample in the form of an algorithm that multiplied two n-digit numbers with $O(n^{\log_2 3})$ complexity. This measure of efficiency has been improved over time, with the latest improvement being an $O(n \log(n))$ algorithm designed by David Harvey (UNSW) and Joris van der Hoeven in 2019. While it is believed by many that this may be the most efficient the multiplication algorithm can get, Harvey has claimed he wouldn't be surprised if further improvements were found in the future.

This example goes to show that it is always possible a conjecture might be false, and that proving its negation with a counterexample might well be the more impressive task.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.07 – Contraposition and contradiction

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Contraposition

Definition. The contrapositive of a conditional statement "If P is true, then Q is true" is the conditional statement "If Q is false, then P is false".

Symbolically, the contrapositive of $P \Rightarrow Q$ is $\sim Q \Rightarrow \sim P$.

The contrapositive of a statement is equivalent to the original statement. This means that to prove any conditional statement, we can instead prove its contrapositive.

The general structure for a proof of the contrapositive of a statement "If P is true, then Q is true" is:

Suppose Q is false.

$\vdots$

Then P is false.

Examples of contrapositive statements

Exercise. Write the contrapositive of each statement below.

- If $A \subseteq B$, then $A \in \mathcal{P}(B)$.
  Contrapositive: $A \notin \mathcal{P}(B) \Rightarrow A \not\subseteq B$.
- Whenever a number is real, its square is non-negative.
  Contrapositive: $x^2 < 0 \Rightarrow x \notin \mathbb{R}$.
- If a quadrilateral is a square, then its sides are all equal.
  Contrapositive: If a quadrilateral's sides are not all equal, then it is not a square.
- You will lose if you battle Cynthia.
  Contrapositive: If you haven't lost, you haven't battled Cynthia.
- You will lose only if you battle Cynthia.
  Contrapositive: If you don't battle Cynthia, you won't lose.

Example 1 – Mersenne primes

Example. Given any natural number $n > 1$, prove that if $2^n - 1$ is prime, then n is prime.

Proof. We proceed by proving the contrapositive. That is, we want to show that if n is composite, then $2^n - 1$ is composite.

Suppose that n is composite. Then we may write $n = ab$ for some positive integers a and b that are both greater than 1. Substituting into $2^n - 1$ gives

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + 2^{a(b-3)} + \cdots + 2^a + 1\right).$$

Since both a and b are greater than 1, both factors in the above expression are themselves greater than 1. So $2^n - 1$ can be written as the product of two factors neither of which are 1, which is to say $2^n - 1$ is composite.

Example 1 – Notes

- Here it helped to use the contrapositive, because it is generally easier to manipulate composite numbers (by writing them as a product) than it can be to manipulate primes.
- Notice that we started by declaring we would prove the contrapositive, and then wrote out exactly what the contrapositive of the statement is.

Example 2 – Even squares

Example. Given $n \in \mathbb{Z}$, prove that n is even if and only if n^2 is even.

Proof. We prove both implication directions in turn.

Forward implication. We want to show that given $n \in \mathbb{Z}$, if n is even, then n^2 is even.
Suppose n is even. Then we may write $n = 2k$ for some integer k. Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, and thus n^2 is even since it is 2 times the integer $2k^2$.

Backward implication. We want to show that given $n \in \mathbb{Z}$, if n^2 is even, then n is even.
We proceed by proving the contrapositive. That is, we want to show that if n is odd, then n^2 is odd.
Suppose n is odd. Then we may write $n = 2k + 1$ for some integer k. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, and thus n^2 is odd since it is 1 more than 2 times the integer $2k^2 + 2k$.

With both implication directions proven, we can conclude that n is even if and only if n^2 is even. □

Example 2 – Notes

- Here the original statement was a biconditional one, so we used the overarching structure of two sub-proofs titled as the forward and backward implications.
  - Notice this is another example where proving one direction can be more straightforward than the other.
- Within the backward implication, we found that proving the contrapositive of that statement was much easier than proving the original statement.
- This result is quite a useful one for certain types of proofs, which we might encounter soon...

Proof by contradiction

To prove a statement by contradiction, we assume the required result is false, and eventually derive a fact that is obviously false, which affirms that the original result was in fact true.

The general structure for a proof by contradiction of a simple statement "P is true" is:

> Suppose (by way of contradiction) P is false.
>
> $\vdots$
>
> But this result is false, so the initial assumption was false.
> That is, P is true.

The general structure for a proof by contradiction of a conditional statement "If P is true, then Q is true" is:

> Suppose P is true.
> Suppose (by way of contradiction) Q is false.
>
> $\vdots$
>
> But this result is false, so the initial assumption was false.
> That is, Q is true.

Example 3 – Diophantine quadratic

Example. Prove that there are no integer solutions to $4x^2 - y^2 = 1$.

Proof. Suppose by way of contradiction that there are integers x and y that satisfy $4x^2 - y^2 = 1$. Factorising gives $1 = (2x - y)(2x + y)$, where $2x - y$ and $2x + y$ must both be integers. Since each term is a factor of 1, we have two possible cases: either both terms equal 1, or both terms equal -1.

Case 1. Suppose $2x - y = 1$ and $2x + y = 1$. Then adding one equation to the other yields $4x = 2$, which has non-integer solution $x = \frac{1}{2}$. This is a contradiction.

Case 2. Suppose $2x - y = -1$ and $2x + y = -1$. Then adding one equation to the other yields $4x = -2$, which has non-integer solution $x = -\frac{1}{2}$. This is again a contradiction.

Since in all possible cases we arrive at a contradiction, the original assumption must have been false. That is, there are no integer solutions to $4x^2 - y^2 = 1$.

Example 3 – Notes

- It is quite natural to approach this sort of statement with a proof by contradiction, since there's not much else to work with but the factorisable equation. Notice that our working was essentially the same as if we were trying to prove something directly, except that the end of our working stopped at an obviously false result instead of an obviously true one.
- We also encountered an application of a proof by exhaustion of cases nested within the proof by contradiction.

Example 4 – Irrationality

Example. Prove that $\sqrt{2}$ is irrational.

Proof. Suppose by way of contradiction that $\sqrt{2}$ is rational. Then we may write $\sqrt{2}$ as a fraction in its simplest form, that is, we may write $\sqrt{2} = \frac{p}{q}$ for some $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$ satisfying $\gcd(p, q) = 1$.

Squaring both sides and rearranging gives $2q^2 = p^2$, so p^2 must be even since q^2 is an integer. Notice that from Example 2, we know that this implies p is even, so we may write $p = 2k$ for some integer k.

Substituting gives $2q^2 = (2k)^2 = 4k^2$, so we have $q^2 = 2k^2$. Now we can similarly see that q^2 must be even, and so we can likewise conclude that q is even. However, since both p and q are even, we know their greatest common divisor is at least 2, contradicting the original assumption that they were coprime.

So the original assumption must have been false, which is to say the positive square root of 2 is irrational.

Example 4 – Notes

- This sort of proof by contradiction is considered a classic, and can be applied to many other known irrational values.
- Notice we had to declare $\sqrt{2}$ could be written as a fraction in simplest form, which was necessary for the contradiction to occur. It is fine to include this in the initial assumption, since it is true that all rational numbers have a simplest form.
- An alternative approach could be to ignore the "simplest form" requirement and instead note that the deductions about p and q being even can be extended to k and any other new variables introduced indefinitely, implying both p and q must have infinitely many factors of 2 (this is known as contradiction by "infinite descent").

Example 5 – Infinite primes

Example. Prove that there are infinitely many primes.

Proof. Suppose by way of contradiction that there are finitely many primes. Let us label the complete finite list of primes in increasing order as $p_1, p_2, p_3, \ldots, p_k$ for some natural number n. Consider the number

$$p = p_1 p_2 p_3 \ldots p_k + 1.$$

Clearly $p \equiv 1 \pmod{p_i}$ for all $1 \leq i \leq k$, and so since the smallest prime is 2, we know $p_i \nmid p$ for all $1 \leq i \leq k$. So either p itself is prime, or it can be written as the product of smaller primes, none of which are included in the list $p_1, p_2, p_3, \ldots, p_k$. But this list of primes was meant to be complete, and so we have reached a contradiction.

So the original assumption must have been false, which is to say there are infinitely many primes.

Example 5 – Notes

- This is another classic example of a proof by contradiction, first found in Euclid's *Elements* from around 300 BCE!
- The difficulty of this proof comes from thinking to create the number p in the first place. Although it might be hard to motivate, it is hopefully reachable if you know to begin with the contradicting assumption that there is a finite number of primes (and so in particular, a largest prime, which leads us to wonder how all the integers larger than that prime can be described in terms of the finite list).

Case study: The halting problem

An arbitrary algorithm (or program) can take any input and either halt (by returning an expected output or a terminating error) or continue running forever (for example, by getting stuck in an infinite loop).

Th'm. There is no program that can decide whether any program is halting.

Alan Turing provided a proof of this statement by contradiction in 1936. The proof supposes that a program A exists that correctly outputs either "halting" or "not halting" for any input program. It then constructs a new program B that takes any program as input, runs A on that input program, and then terminates if A returns "not halting", or else loops forever if A returns "halting". Consider the result of inputting B into the program B.

- If B is halting, then A outputs "halting", which implies B loops forever and is not halting.
- If B is not halting, then A outputs "not halting", which implies B terminates and is halting.

Both cases lead to a contradiction, so such a program A cannot exist. This proof implied there is inherent incompleteness in the theory of algorithms, with far-reaching implications. A similar result based on axiomatic mathematics is known as Gödel's Incompleteness Theorem.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.08 – Mathematical induction

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Proof by induction

The technique of mathematical induction is a particular style of proof that allows proving universal statements whose domain of disclosure is countable. Typically this means a universal statement about all natural numbers, or some infinite subset of the natural numbers (like the positive integers).

Proving the statement "For all $n \in \mathbb{N}$, $P(n)$ is true," is broken down into two parts:

- Base case: Prove that $P(0)$ is true.
- Induction: Prove that $P(k) \Rightarrow P(k+1)$ for all $k \in \mathbb{N}$.

This approach works because knowing $P(0)$ is true implies $P(1)$ is true, which in turn implies $P(2)$ is true, and so on.

The general structure for a proof by induction of a statement "For all integers $n \geq n_0$, $P(n)$ is true" is:

> First, $P(n_0)$ is true because...
> Suppose $P(k)$ is true for some integer $k \geq n_0$.
> $\vdots$
> Then $P(k+1)$ is true.

Example 1 – Divisibility

Example. Prove that for all $n \in \mathbb{Z}^+$, we have that $5^{2n} - 1$ is divisible by 24.

Proof. We proceed by mathematical induction on n. Let $P(n)$ be the statement "$5^{2n} - 1$ is divisible by 24."

Base case. When $n = 1$, the statement $P(1)$ becomes "$5^{2\times 1} - 1 = 24$ is divisible by 24", which is certainly true since $24 = 1 \times 24$.

Induction. Suppose that $P(k)$ is true for some $k \in \mathbb{Z}^+$. That is, suppose $5^{2k} - 1 = 24m$ for some integer m. Then we wish to show that $P(k+1)$ is true, that is, we want to show that $5^{2(k+1)} - 1$ is divisible by 24. Notice that

$$\begin{aligned} 5^{2(k+1)} - 1 &= 5^2 \times 5^{2k} - 1 \\ &= 25 \times (24m + 1) - 1 \qquad \text{(by the inductive hypothesis)} \\ &= 25 \times 24m + 25 - 1 \\ &= 24(25m + 1), \end{aligned}$$

so $5^{2(k+1)} - 1$ is in fact a multiple of 24 since $25m + 1$ is an integer. So whenever $P(k)$ is true, $P(k+1)$ is true.

It follows by mathematical induction that $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Example 1 – Notes

- Notice that because we needed to prove the statement was true for all positive integers, our base case started at the smallest positive integer, namely 1.
- We started the proof by declaring it will be a proof by mathematical induction, which helps inform the reader of the ensuing proof structure.
- Although not necessary, the base case and induction steps were labelled with subtitles here to make it clear where each part starts and ends.
- It can be useful to write out what exactly the inductive hypothesis "$P(k)$ is true" means, and also to write out what exactly the goal "$P(k+1)$ is true" should mean.
- We labelled when the inductive hypothesis was used in the proof, so that it is clear what has happened algebraically and also that we really were proving by induction.
- You might like to try proving this using a different method, for example modular arithmetic.

Example 2 – Consecutive cube sum

Example. Prove for all $n \in \mathbb{N}$, that $0^3 + 1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$.

Proof. We proceed by mathematical induction on n. Let $P(n)$ be the statement "$0^3 + 1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$."

Base case. When $n = 0$, the left-hand side of the equation in $P(0)$ is 0, while the right-hand side is $\frac{1}{4}0^2(0+1)^2 = 0$. So $P(0)$ is true.

Induction. Suppose that $P(k)$ is true for some $k \in \mathbb{N}$. That is, suppose $0^3 + 1^3 + 2^3 + \cdots + k^3 = \frac{1}{4}k^2(k+1)^2$. Then we wish to show that $P(k+1)$ is true, that is, we want to show that $0^3 + 1^3 + 2^3 + \cdots + (k+1)^3$ is equal to $\frac{1}{4}(k+1)^2((k+1)+1)^2$.

Notice that

$$\begin{aligned} 0^3 + 1^3 + \cdots + (k+1)^3 &= (0^3 + 1^3 + \cdots + k^3) + (k+1)^3 \\ &= \tfrac{1}{4}k^2(k+1)^2 + (k+1)^3 \quad \text{(by the inductive hypothesis)} \\ &= \tfrac{1}{4}(k+1)^2\left(k^2 + 4(k+1)\right) \\ &= \tfrac{1}{4}(k+1)^2(k+2)^2, \end{aligned}$$

as required. So $P(k+1)$ is indeed true whenever $P(k)$ is true.

It follows by mathematical induction that $P(n)$ is true for all $n \in \mathbb{N}$.

Example 2 – Notes

- Here the statement held for all natural numbers, so our base case started at the smallest natural number, namely 0.
- Notice the structure of this proof is very similar to the structure of the previous one, and is the sort of structure that can be easily modified for any proof of this type.
- Always make it clear whether a statement you are writing has been proven or not. Here we made sure to use the phrase "we want to show that" where needed.

Strong induction

A more general form of mathematical induction is known as strong induction, which can be useful for problems involving relations between more than two consecutive terms.

Proving the statement "For all $n \in \mathbb{N}$, $P(n)$ is true," becomes:

- Base case(s): Prove that $P(0)$ is true. (Add more cases if needed.)
- Induction: Prove that $(P(0), P(1), \ldots, P(k)) \Rightarrow P(k+1)$ for all $k \in \mathbb{N}$.

Note that we do not have to use all the inductive hypotheses to show that $P(k+1)$ is true. It can often be sufficient to only require a subset, for example $P(k)$ and $P(k-1)$.

The general structure for a proof by strong induction of a statement "For all integers $n \geq n_0$, $P(n)$ is true" is:

> First, $P(n_0)$ is true because...
> Suppose $P(n_0), P(n_0+1), P(n_0+2), \ldots, P(k)$ are all true for some integer $k \geq n_0$.
> $\vdots$
> Then $P(k+1)$ is true.

Example 3 – Recurrence relation

Example. Prove that the sequence defined by $a_0 = 1, a_1 = 6$, and $a_n = 4(a_{n-1} - a_{n-2})$ for all $n \geq 2$, satisfies $a_n = 2^n(2n+1)$ for all $n \in \mathbb{N}$.

Proof. We proceed by mathematical induction on n. Let $P(n)$ be the statement "$a_n = 2^n(2n+1)$."

Base cases. $P(0)$ is true, because $a_0 = 2^0(2 \times 0 + 1) = 1$ as required. Also, $P(1)$ is true, because $a_1 = 2^1(2 \times 1 + 1) = 6$ as required.

Induction. Suppose that $P(k)$ and $P(k-1)$ are true for some $k \in \mathbb{Z}^+$. That is, suppose $a_k = 2^k(2k+1)$ and $a_{k-1} = 2^{k-1}(2(k-1)+1)$. Then we wish to show that $P(k+1)$ is true, that is, we want to show that a_{k+1} is equal to $2^{k+1}(2(k+1)+1)$.

We have that

$$\begin{aligned} a_{k+1} &= 4(a_k - a_{k-1}) \\ &= 4(2^k(2k+1) - 2^{k-1}(2k-1)) \quad \text{(by the inductive hypotheses)} \\ &= 2^{k+1}(2(2k+1) - (2k-1)) \\ &= 2^{k+1}(2(k+1)+1), \end{aligned}$$

as required. So $P(k+1)$ is true whenever $P(k)$ and $P(k-1)$ are true.

It follows by (strong) mathematical induction that $P(n)$ is true for all $n \in \mathbb{N}$.

Example 3 – Notes

- Here we wanted to use a form of strong induction, because the defining relation for a_n was based on the two terms preceding it (as opposed to just one). If we wanted to use induction on the expression for a_{k+1}, we would need to be able to assume the inductive hypothesis for both a_k and a_{k-1}. This is why we had two inductive hypotheses.
- In this example we also needed two base cases, since neither a_0 nor a_1 are defined by the general relation for a_n.

Example 4 – Fundamental Theorem of Arithmetic

Example. Prove that every integer greater than 1 can be written as a product of only prime numbers.

Proof. We proceed by mathematical induction on n. Let $P(n)$ be the statement "n can be written as a product of only prime numbers."

Base case. $P(2)$ is true, because 2 is a prime number itself.

Induction. Suppose that $P(2), P(3), P(4), \ldots, P(k)$ are all true for some $k \in \mathbb{Z}^+ - \{1\}$. That is, suppose $2, 3, 4, \ldots, k$ can each be written as a product of only prime numbers. Then we wish to show that $P(k+1)$ is true, that is, we want to show that $k+1$ can be written as a product of only prime numbers.

Notice that $k+1$ can be either prime or composite. If $k+1$ is prime, then it is trivially a product of only prime numbers. Otherwise, it is composite, and we may write $k+1 = ab$ for some integers a and b satisfying $1 < a < k+1$ and $1 < b < k+1$. So by the inductive hypothesis, we have that both a and b can be written as the product of only prime numbers, and therefore their product $ab = k+1$ can also be written as a product of only prime numbers.

It follows by (strong) mathematical induction that $P(n)$ is true for all integers n greater than 1.

Example 4 – Notes

- Here we wanted to use a form of strong induction, because the case where $k+1$ is composite calls for knowledge about two smaller integers a and b, but we can't specify their values. So it's useful to assume the claim holds for all values strictly between 1 and $k+1$.
- In this example of strong induction we only needed to check a single base case, namely $n = 2$.
- Notice this proof shows the existence part of the Fundamental Theorem of Arithmetic, but not the uniqueness part!

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.09 – Symbolic logic and truth tables

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Propositions

Definition. A proposition or statement is any sentence that is unambiguously true or false. For example:

- "1 is an integer" is a (true) proposition.
- "Today is Tuesday" is a proposition.
- "Tuesday is the best day" is not a proposition.
- "$1 + 1 = 2$" is a (true) proposition.
- "$1 + 1 = 3$" is a (false) proposition.
- "$1 + 1$" is not a proposition.
- "$x + 1 = 2$" is not a proposition.
- "$\exists x \in \mathbb{N} \quad x + 1 = 2$" is a (true) proposition.
- "$\forall x \in \mathbb{N} \quad x + 1 = 2$" is a (false) proposition.

Typically a proposition is denoted by a lowercase letter, for example p or q.

Definition. A compound proposition is a sentence made up of one or more propositions. Whether a compound proposition is true or false is dependent on whether its component propositions are true or false.

Usually a compound proposition is denoted by an uppercase letter, for example P or Q.

Truth tables

A truth table is a useful way of tabulating information about compound propositions. We write **T** for "true" and **F** for "false", and evaluate all possible outcomes based on the possible values of the component simple propositions.

For example:

It's cloudy	It's raining	The weather is sensible
T	**T**	**T**
T	**F**	**T**
F	**T**	**F**
F	**F**	**T**

In the above example, to decide whether "the weather is sensible" was true or false, we needed to consider the four possible ways "it's cloudy" and "it's raining" could be true or false in combination.

To better describe compound propositions, we'll need to introduce some new notation...

Negation (logical "not")

Definition. The negation of a proposition is a proposition that is true precisely when the original proposition is false.

Notation. The negation of the proposition p is written as $\sim p$ (or sometimes as $\neg p$), and can be read as "not p", "never p", etc.

The truth table for $\sim p$ is as follows:

p	$\sim p$
T	**F**
F	**T**

Conjunction (logical "and")

Definition. The conjunction of two propositions is a compound proposition that is true precisely when both the component propositions are true.

Notation. The conjunction of the propositions p and q is written as $p \wedge q$, and can be read as "p and q", "p as well as q", "p but q", "p despite q", etc.

The truth table for $p \wedge q$ is as follows:

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

Disjunction (logical "or")

Definition. The disjunction of two propositions is a compound proposition that is true precisely when either (or both) of the two component propositions are true.

Notation. The disjunction of the propositions p and q is written as $p \vee q$, and can be read as "p or q", "either p or q", "p and/or q", etc.

The truth table for $p \vee q$ is as follows:

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

Notice that "or" is always treated as the "inclusive or" here (even when used with "either" in English).

Notice that "neither p nor q" is interpreted as "not (either p or q)", that is, $\sim(p \vee q)$.

Examples of compound propositions

Exercise. Write the following sentences as compound propositions, using s for the proposition "There's a spy in our midst" and e for the proposition "The engineer is a spy".

- There isn't a spy in our midst.
  $\sim s$.
- There's a spy in our midst and it's the engineer.
  $s \wedge e$.
- Either there's a spy in our midst or the engineer is a spy.
  $s \vee e$.
- There's a spy in our midst, but it's not the engineer.
  $s \wedge \sim e$.
- There is neither a spy in our midst nor is the engineer a spy.
  $\sim(s \vee e)$.
- Either there's a spy in our midst or the engineer is a spy, but not both.
  $(s \vee e) \wedge \sim(s \wedge e)$.

Example 1 – Truth table

Example. Construct a truth table for the compound proposition $\sim p \vee (p \wedge q)$.

Solution. We break the expression into manageable parts per column:

p	q	$\sim p$	$p \wedge q$	$\sim p \vee (p \wedge q)$
T	**T**	**F**	**T**	**T**
T	**F**	**F**	**F**	**F**
F	**T**	**T**	**F**	**T**
F	**F**	**T**	**F**	**T**

The final column shows the values of the compound proposition.

Example 2 – Larger truth table

Example. Construct a truth table for the compound proposition $(p \vee q) \wedge (q \vee r)$.

Solution. We break the expression into manageable parts per column:

p	q	r	$p \vee q$	$q \vee r$	$(p \vee q) \wedge (q \vee r)$
T	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**T**	**T**
T	**F**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**
F	**T**	**T**	**T**	**T**	**T**
F	**T**	**F**	**T**	**T**	**T**
F	**F**	**T**	**F**	**T**	**F**
F	**F**	**F**	**F**	**F**	**F**

The final column shows the values of the compound proposition.

Notice that for a compound proposition in three variables, we need $2^3 = 8$ rows in the truth table.

Tautologies and contradictions

Definition. A (compound) proposition is called a tautology if it is always true (regardless of the values of its component propositions). In a truth table, a tautology would correspond with a column containing only **T**s.

Notation. A proposition that is known to be a tautology is usually denoted by T.

In some texts, the notation might instead be a lowercase t or the character $\top$, and/or might be written in boldface.

Definition. A (compound) proposition is called a contradiction if it is always false (regardless of the values of its component propositions). In a truth table, a contradiction would correspond with a column containing only **F**s.

Notation. A proposition that is known to be a contradiction is usually denoted by F.

In some texts, the notation might instead be a lowercase c or the character $\bot$, and/or might be written in boldface.

Definition. A (compound) proposition that is neither a tautology nor a contradiction is called a contingency. In a truth table, a contingency would correspond with a column containing both **T**s and **F**s.

Example 3 – Tautology

Example. Show that the compound proposition $q \vee \sim(p \wedge q)$ is a tautology.

Solution. Writing up a truth table gives:

p	q	$p \wedge q$	$\sim(p \wedge q)$	$q \vee \sim(p \wedge q)$
T	**T**	**T**	**F**	**T**
T	**F**	**F**	**T**	**T**
F	**T**	**F**	**T**	**T**
F	**F**	**F**	**T**	**T**

Since the final column contains only **T**s, we can conclude that the compound proposition is a tautology.

Example 4 – Contradiction

Example. Show that the compound proposition $q \wedge \sim(p \vee q)$ is a contradiction.

Solution. Writing up a truth table gives:

p	q	$p \vee q$	$\sim(p \vee q)$	$q \wedge \sim(p \vee q)$
T	**T**	**T**	**F**	**F**
T	**F**	**T**	**F**	**F**
F	**T**	**T**	**F**	**F**
F	**F**	**F**	**T**	**F**

Since the final column contains only **F**s, we can conclude that the compound proposition is a contradiction.

Logical equivalence

Definition. Two (compound) propositions are called logically equivalent if their truth values match for all possible component proposition values – that is, if their corresponding columns in a truth table are identical.

Notation. If two compound propositions P and Q are logically equivalent, we write $P \Leftrightarrow Q$. Some texts might instead use the notation $P \equiv Q$.

To show two compound propositions are equivalent, we can check that they have identical columns in a truth table.

To show two compound propositions are not equivalent, we only need to find a single row where their values are not the same.

Example 5 – Equivalence

Example. Show that $\sim(p \wedge q) \Leftrightarrow \sim p \vee \sim q$.

Solution. Writing up a truth table gives:

p	q	$p \wedge q$	$\sim(p \wedge q)$	$\sim p$	$\sim q$	$\sim p \vee \sim q$
T	**T**	**T**	**F**	**F**	**F**	**F**
T	**F**	**F**	**T**	**F**	**T**	**T**
F	**T**	**F**	**T**	**T**	**F**	**T**
F	**F**	**F**	**T**	**T**	**T**	**T**

Since the 4th and final columns' values are identical, we can conclude that the corresponding compound propositions are logically equivalent. That is, $\sim(p \wedge q) \Leftrightarrow \sim p \vee \sim q$.

Exclusive disjunction ("exclusive or")

Definition. The exclusive disjunction of two propositions is a compound proposition that is true precisely when exactly one of the two component propositions are true.

Notation. The exclusive disjunction of the propositions p and q is written as $p \oplus q$, and can be read as "p or q, but not both", "p or q exclusively", "p xor q", etc.

The truth table for $p \oplus q$ is as follows:

p	q	$p \oplus q$
T	**T**	**F**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

Fact. The exclusive disjunction can be rewritten in terms of earlier operators:

$$p \oplus q \Leftrightarrow (p \vee q) \wedge \sim(p \wedge q).$$

Example 6 – Exclusive disjunction

Example. Show that $p \oplus q \Leftrightarrow (p \vee q) \wedge \sim(p \wedge q)$.

Solution. Writing up a truth table gives:

p	q	$p \oplus q$	$p \vee q$	$p \wedge q$	$\sim(p \wedge q)$	$(p \vee q) \wedge \sim(p \wedge q)$
T	**T**	**F**	**T**	**T**	**F**	**F**
T	**F**	**T**	**T**	**F**	**T**	**T**
F	**T**	**T**	**T**	**F**	**T**	**T**
F	**F**	**F**	**F**	**F**	**T**	**F**

Since the 3rd and final columns' values are identical, we can conclude that the corresponding compound propositions are logically equivalent. That is, $p \oplus q \Leftrightarrow (p \vee q) \wedge \sim(p \wedge q)$.

Logical conditional

Notation. The conditional compound proposition $p \to q$ can be read as "p implies q", "if p then q", "q if p", "q whenever p", "p only if q", etc.

The compound proposition $p \to q$ is false precisely when p is true but q is false.

The truth table for $p \to q$ is as follows:

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

Fact. The conditional can be rewritten in terms of earlier operators:

$$p \to q \Leftrightarrow \sim p \vee q.$$

Notice that "p unless q" is interpreted as "p if not q", that is, $\sim q \to p$.

Example 7 – Conditional proposition

Example. Show that $p \to q \Leftrightarrow \sim p \vee q$.

Solution. Writing up a truth table gives:

p	q	$p \to q$	$\sim p$	$\sim p \vee q$
T	**T**	**T**	**F**	**T**
T	**F**	**F**	**F**	**F**
F	**T**	**T**	**T**	**T**
F	**F**	**T**	**T**	**T**

Since the 3rd and final columns' values are identical, we can conclude that the corresponding compound propositions are logically equivalent. That is, $p \to q \Leftrightarrow \sim p \vee q$.

Logical biconditional

Notation. The biconditional compound proposition $p \leftrightarrow q$ can be read as "p if and only if q", "p iff q", "p if q and q if p", "p implies q and q implies p", etc.

The compound proposition $p \leftrightarrow q$ is true precisely when p and q have the same value.

The truth table for $p \leftrightarrow q$ is as follows:

p	q	$p \leftrightarrow q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**T**

Fact. The biconditional can be rewritten in terms of earlier operators:

$$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p).$$

Example 8 – Biconditional proposition

Example. Show that $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$.

Solution. Writing up a truth table gives:

p	q	$p \leftrightarrow q$	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$
T	**T**	**T**	**T**	**T**	**T**
T	**F**	**F**	**F**	**T**	**F**
F	**T**	**F**	**T**	**F**	**F**
F	**F**	**T**	**T**	**T**	**T**

Since the 3rd and final columns' values are identical, we can conclude that the corresponding compound propositions are logically equivalent. That is, $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$.

Logical conditionals versus implications

Notice that $P \to Q$ is a compound proposition that may or may not be true, while $P \Rightarrow Q$ is a statement that claims to be true. The statement "$P \Rightarrow Q$" means the same as "$P \to Q$ is a tautology".

In order to prove that $P \Rightarrow Q$, we can show that the column corresponding to $P \to Q$ in a truth table contains only **T**s.

Similarly, $P \leftrightarrow Q$ is a compound proposition that may or may not be true, while $P \Leftrightarrow Q$ is a statement that claims to be true. The statement "$P \Leftrightarrow Q$" means the same as "$P \leftrightarrow Q$ is a tautology".

In order to prove that $P \Leftrightarrow Q$, we can show that the column corresponding to $P \leftrightarrow Q$ in a truth table contains only **T**s.

More examples of compound propositions

Exercise. Write the following sentences as compound propositions, using s for the proposition "There's a spy in our midst" and e for the proposition "The engineer is a spy".

- Either there's a spy in our midst or the engineer is a spy, but not both.
  $s \oplus e$.
- If there's a spy in our midst, it's the engineer.
  $s \to e$.
- There's a spy in our midst if the engineer is a spy, and conversely.
  $s \leftrightarrow e$.
- There isn't a spy in our midst unless the engineer is a spy.
  $\sim e \to \sim s$.
- If there's a spy in our midst or the engineer is a spy, then both statements are true.
  $(s \vee e) \to (s \wedge e)$.

Example 9 – Negation of conditionals

Example. Show that the negation of $p \to q$ is $p \wedge \sim q$.

Solution. We write up a truth table for $\sim(p \to q)$ and $p \wedge \sim q$:

p	q	$p \to q$	$\sim(p \to q)$	$\sim q$	$p \wedge \sim q$
T	**T**	**T**	**F**	**F**	**F**
T	**F**	**F**	**T**	**T**	**T**
F	**T**	**T**	**F**	**F**	**F**
F	**F**	**T**	**F**	**T**	**F**

Since the 4th and final columns' values are identical, we can conclude that the corresponding compound propositions are logically equivalent. That is, $\sim(p \to q) \Leftrightarrow p \wedge \sim q$.

Example 10 – Converse fallacy

Example. Show that the converse of $p \to q$ is not equivalent to $p \to q$.

Solution. We write up a truth table for $p \to q$ and its converse, $q \to p$:

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

Since the 3rd and final columns' values are not identical, we can conclude that the corresponding compound propositions are not logically equivalent equivalent.

Example 11 – Contrapositive

Example. Show that the contrapositive of $p \to q$ is equivalent to $p \to q$.

Solution. We write up a truth table for $p \to q$ and its contrapositive, $\sim q \to \sim p$:

p	q	$p \to q$	$\sim p$	$\sim q$	$\sim q \to \sim p$
T	**T**	**T**	**F**	**F**	**T**
T	**F**	**F**	**F**	**T**	**F**
F	**T**	**T**	**T**	**F**	**T**
F	**F**	**T**	**T**	**T**	**T**

Since the 3rd and final columns' values are identical, we can conclude that the corresponding compound propositions are logically equivalent. That is, $p \to q \Leftrightarrow \sim q \to \sim p$.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 3 – Proofs and logic
Lecture 3.10 – Laws of logical equivalence and inference

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Laws of logical equivalence

For any propositions p, q, r with tautology T and contradiction F, we have the following laws of logical equivalence:

Commutativity:

$$p \wedge q \Leftrightarrow q \wedge p,$$
$$p \vee q \Leftrightarrow q \vee p.$$

Associativity:

$$p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r,$$
$$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r.$$

Distributivity:

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r),$$
$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r).$$

Absorption:

$$p \wedge (p \vee q) \Leftrightarrow p,$$
$$p \vee (p \wedge q) \Leftrightarrow p.$$

Idempotence:

$$p \wedge p \Leftrightarrow p,$$
$$p \vee p \Leftrightarrow p.$$

Identity:

$$p \wedge T \Leftrightarrow p,$$
$$p \vee F \Leftrightarrow p.$$

Domination:

$$p \wedge F \Leftrightarrow F,$$
$$p \vee T \Leftrightarrow T.$$

Negation law:

$$p \wedge \sim p \Leftrightarrow F,$$
$$p \vee \sim p \Leftrightarrow T.$$

Double negation law:

$$\sim(\sim p) \Leftrightarrow p.$$

De Morgan's law:

$$\sim(p \wedge q) \Leftrightarrow \sim p \vee \sim q,$$
$$\sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q.$$

We also have the following definitions:

Logical implication:

$$p \to q \Leftrightarrow \sim p \vee q.$$

Exclusive disjunction:

$$p \oplus q \Leftrightarrow (p \vee q) \wedge \sim(p \wedge q).$$

Laws of set algebra (for comparison)

For any sets A, B, C with universal set $\mathcal{U}$ and empty set $\varnothing$, we have the following laws of set algebra:

Commutativity:

$$A \cap B = B \cap A,$$
$$A \cup B = B \cup A.$$

Associativity:

$$A \cap (B \cap C) = (A \cap B) \cap C,$$
$$A \cup (B \cup C) = (A \cup B) \cup C.$$

Distributivity:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Absorption:

$$A \cap (A \cup B) = A,$$
$$A \cup (A \cap B) = A.$$

Idempotence:

$$A \cap A = A,$$
$$A \cup A = A.$$

Identity:

$$A \cap \mathcal{U} = A,$$
$$A \cup \varnothing = A.$$

Domination:

$$A \cap \varnothing = \varnothing,$$
$$A \cup \mathcal{U} = \mathcal{U}.$$

Complement law:

$$A \cap A^c = \varnothing,$$
$$A \cup A^c = \mathcal{U}.$$

Double complement law:

$$(A^c)^c = A.$$

De Morgan's law:

$$(A \cap B)^c = A^c \cup B^c,$$
$$(A \cup B)^c = A^c \cap B^c.$$

We also have the following (variations of) definitions:

Complement of difference:

$$(A - B)^c = A^c \cup B.$$

Symmetric difference:

$$A \ominus B = (A \cup B) \cap (A \cap B)^c.$$

Comments on the laws of logical equivalence

The laws of logical equivalence completely describe the behaviour of propositions under the basic logic operations. It is possible to verify any statements involving logical expressions by using only these laws.

We can map all the set algebra laws to logical equivalence laws by replacing sets with propositions, $\cap$ with $\wedge$, $\cup$ with $\vee$, complement with negation, $\mathcal{U}$ with T, and $\varnothing$ with F. The definitions of $p \to q$ and $p \oplus q$ also correspond with the definitions for $(A - B)^c$ and $A \ominus B$ respectively.

When simplifying expressions or proving statements using the laws of logical equivalence, we should always state which laws are being used at each step. If you do not remember the name of a particular law, you may instead describe it in words and/or provide its general definition.

Definition. The dual of a compound proposition is the proposition obtained by replacing every instance of $\wedge$ with $\vee$, $\vee$ with $\wedge$, T with F, and F with T.

Theorem. (Duality principle)
Any statement involving only simple propositions and the conjunction, disjunction, and negation operations is true if and only if its dual statement is true.

Example 1 – Negation of conditionals (revisited)

Example. Show that the negation of $p \to q$ is $p \wedge \sim q$.

Solution. We proceed using laws of logical equivalence:

$$\begin{aligned} \sim(p \to q) &\Leftrightarrow \sim(\sim p \vee q) && \text{(definition of conditional)} \\ &\Leftrightarrow \sim(\sim p) \wedge \sim q && \text{(De Morgan's law)} \\ &\Leftrightarrow p \wedge \sim q && \text{(double negation).} \end{aligned}$$

We have now proven this equivalence using truth tables and using equivalence laws. In this case, the latter method is arguably the easier one to write up.

Example 2 – Negation of exclusive disjunction

Example. Show that the negation of $p \oplus q$ is $p \leftrightarrow q$.

Solution. We proceed using laws of logical equivalence:

$$
\begin{aligned}
\sim(p \oplus q) &\Leftrightarrow \sim((p \vee q) \wedge \sim(p \wedge q)) && \text{(definition of } \oplus\text{)} \\
&\Leftrightarrow \sim(p \vee q) \vee \sim(\sim(p \wedge q)) && \text{(De Morgan's law)} \\
&\Leftrightarrow \sim(p \vee q) \vee (p \wedge q) && \text{(double negation)} \\
&\Leftrightarrow (\sim p \wedge \sim q) \vee (p \wedge q) && \text{(De Morgan's law)} \\
&\Leftrightarrow (\sim p \vee p) \wedge (\sim p \vee q) \wedge (\sim q \vee p) \wedge (\sim q \vee q) \\
& && \text{(distributivity, associativity)} \\
&\Leftrightarrow T \wedge (\sim p \vee q) \wedge (\sim q \vee p) \wedge T && \text{(negation)} \\
&\Leftrightarrow (\sim p \vee q) \wedge (\sim q \vee p) && \text{(identity)} \\
&\Leftrightarrow (p \to q) \wedge (q \to p) && \text{(def'n of conditional)} \\
&\Leftrightarrow p \leftrightarrow q && \text{(def'n of biconditional).}
\end{aligned}
$$

Notice that this equivalence would have been much easier to prove using a truth table!

Inferential statements

A typical logical argument will take the form of several hypotheses (or premises) which, when they are considered all together, imply a new proposition (the conclusion).

Symbolically, an argument with hypotheses $P_1, P_2, P_3, \ldots, P_n$ and conclusion Q can be written as $P_1 \wedge P_2 \wedge P_3 \wedge \cdots \wedge P_n \to Q$.

A logical argument is valid if it is a tautology, that is, if when all the hypotheses are taken to be true, the conclusion must also be true.

Symbolically, an argument with hypotheses $P_1, P_2, P_3, \ldots, P_n$ and conclusion Q is valid if $P_1 \wedge P_2 \wedge P_3 \wedge \cdots \wedge P_n \Rightarrow Q$.

Some texts might represent a logical argument this way:

$$\begin{array}{l} P_1 \\ P_2 \\ \vdots \\ P_n \\ \hline \therefore\ Q\,. \end{array}$$

If neither Q nor $\sim Q$ are valid conclusions, then we say Q is inconclusive.

To check the validity of a logical argument, we can use some further laws, known as rules of inference...

Rules of logical inference

For propositions p, q, and r, we have the following rules of inference:

Modus ponens:	$(p \to q) \wedge (p) \Rightarrow q$
Modus tollens:	$(p \to q) \wedge (\sim q) \Rightarrow \sim p$
Generalisation:	$(p) \Rightarrow p \vee q$
Specialisation:	$(p \wedge q) \Rightarrow p$
Elimination:	$(p \vee q) \wedge (\sim p) \Rightarrow q$
Transitivity:	$(p \to q) \wedge (q \to r) \Rightarrow p \to r$
Case exhaustion:	$(p \vee q) \wedge (p \to r) \wedge (q \to r) \Rightarrow r$

Remember that this means that if every bracketed proposition is known to be true, then the rightmost proposition is also true.

Notice that *modus ponens* ("method of affirming") describes the method of direct proof, while *modus tollens* ("method of denying") describes the method of proof by contraposition.

The *modus tollens* rule of inference with p replaced by $\sim p$ describes the method of proof by contradiction: $(\sim p \to q) \wedge (\sim q) \Rightarrow p$.

Example 3 – Word argument

Example. Given the hypotheses "if you battle Cynthia, you will lose", "you cannot face the champion unless you battle Cynthia", and "you faced the champion", is it possible to conclude whether or not you will lose?

Solution. Let b be the proposition "you battle Cynthia", ℓ be the proposition "you will lose", and c be the proposition "you faced the champion". Then we have the following hypotheses:

$$\begin{aligned} P_1 &\Leftrightarrow b \to \ell, \\ P_2 &\Leftrightarrow \sim b \to \sim c, \\ P_3 &\Leftrightarrow c. \end{aligned}$$

Using the laws of logical equivalence and inference, we can show that

$$\begin{aligned} P_1 \wedge P_2 \wedge P_3 &\Leftrightarrow (b \to \ell) \wedge (\sim b \to \sim c) \wedge (c) \\ &\Leftrightarrow (b \to \ell) \wedge (\sim b \to \sim c) \wedge \sim(\sim c) && \text{(double negation)} \\ &\Rightarrow (b \to \ell) \wedge \sim(\sim b) && \text{(\textit{modus tollens})} \\ &\Leftrightarrow (b \to \ell) \wedge b && \text{(double negation)} \\ &\Rightarrow \ell && \text{(\textit{modus ponens}).} \end{aligned}$$

This shows that $P_1 \wedge P_2 \wedge P_3 \Rightarrow \ell$, and so "you will lose" is a valid conclusion (that is, it is true that you will lose).

Example 3 – Word argument

Example. Given the hypotheses "if you battle Cynthia, you will lose", "you cannot face the champion unless you battle Cynthia", and "you faced the champion", is it possible to conclude whether or not you will lose?

Alternate solution. Using the same propositions and hypotheses as before, we have:

$$\begin{aligned} P_1 \wedge P_2 \wedge P_3 &\Leftrightarrow (b \to \ell) \wedge (\sim b \to \sim c) \wedge (c) \\ &\Leftrightarrow (b \to \ell) \wedge (c \to b) \wedge (c) && \text{(contrapositive)} \\ &\Rightarrow (c \to \ell) \wedge (c) && \text{(transitivity)} \\ &\Rightarrow \ell && (\textit{modus ponens}). \end{aligned}$$

This again shows that "you will lose" is a valid conclusion.

Notice that we can use logical equivalences and inferences together in these arguments, since we are only interested in showing the logical implication carries in one direction.

However, notice also that when applying a logical inference rule, we can lose information about the complete system. For example, the last line in the above solution loses information about the truth value of c.

Example 4 – Another word argument

Example. Given the hypotheses "if you battle Cynthia, you will lose", "you cannot face the champion unless you battle Cynthia", and "you lost", is it possible to conclude whether or not you faced the champion?

Working. Let b be the proposition "you battle Cynthia", ℓ be the proposition "you will lose", and c be the proposition "you faced the champion". Then we have the following hypotheses:

$$\begin{aligned} P_1 &\Leftrightarrow b \to \ell, \\ P_2 &\Leftrightarrow \sim b \to \sim c, \\ P_3 &\Leftrightarrow \ell. \end{aligned}$$

We can show that

$$\begin{aligned} P_1 \wedge P_2 \wedge P_3 &\Leftrightarrow (b \to \ell) \wedge (\sim b \to \sim c) \wedge (\ell) \\ &\Leftrightarrow (b \to \ell) \wedge (c \to b) \wedge (\ell) && \text{(contrapositive)} \\ &\Rightarrow (c \to \ell) \wedge (\ell) && \text{(transitivity).} \end{aligned}$$

This expression does not seem to simplify any further, and the proposition $(c \to \ell) \wedge (\ell)$ can be true regardless of whether c is true or false. So we suspect that it is not possible to make any conclusion about c alone (that is, c is inconclusive).

Example 4 – Another word argument

Example. Given the hypotheses "if you battle Cynthia, you will lose", "you cannot face the champion unless you battle Cynthia", and "you lost", is it possible to conclude whether or not you faced the champion?

Solution. Let b be the proposition "you battle Cynthia", ℓ be the proposition "you will lose", and c be the proposition "you faced the champion". Then we have the following hypotheses:

$$\begin{aligned} P_1 &\Leftrightarrow b \to \ell, \\ P_2 &\Leftrightarrow \sim b \to \sim c, \\ P_3 &\Leftrightarrow \ell. \end{aligned}$$

We claim that the proposition c is inconclusive. To show this, we find cases where c is not a valid conclusion and where $\sim c$ is not a valid conclusion.

Case 1. Suppose that $\ell \Leftrightarrow T$, $b \Leftrightarrow T$, and $c \Leftrightarrow T$. Then each of P_1, P_2, and P_3 is true, as is c. So $P_1 \wedge P_2 \wedge P_3 \to \sim c$ is not a valid argument.

Case 2. Suppose that $\ell \Leftrightarrow T$, $b \Leftrightarrow F$, and $c \Leftrightarrow F$. Then each of P_1, P_2, and P_3 is true, while c is false. So $P_1 \wedge P_2 \wedge P_3 \to c$ is not a valid argument.

So c is inconclusive, and it is impossible conclude whether or not you faced the champion.

Examples 3 and 4 – Notes

- To show a logical argument is valid, we can use both the laws of equivalence and of inference.
- To show a logical argument is invalid, we just have to find a particular case where specific truth values for the component simple propositions leads to a false implication.
- To show that a proposition Q is inconclusive, we must show that both Q and $\sim Q$ are invalid conclusions.
- We could also try proving the validity of the argument in Example 3 in the following alternative (arguably less efficient) ways:
  - Show that $P_1 \wedge P_2 \wedge P_3 \rightarrow \ell$ is a tautology using truth tables.
  - Show that $P_1 \wedge P_2 \wedge P_3 \rightarrow \ell \Leftrightarrow T$ using only the equivalence laws.
- While generally less succinct, we might also prefer to provide an explanation incorporating aspects of equivalence laws, inference rules, and truth tables altogether. For example, instead of citing *modus ponens* when showing $(p \rightarrow q) \wedge (p) \Rightarrow q$, we could draw up a truth table for $p \rightarrow q$ and demonstrate that the rows in which both p and $p \rightarrow q$ are **T** only ever correspond with q also being **T**.

Example 3 Revisited – Using laws of logical equivalence

Example (revisited). Recall we wanted to show that

$$(b \to \ell) \wedge (\sim b \to \sim c) \wedge (c) \Rightarrow \ell.$$

Alternative solution. We proceed by simplifying the following expression, labelled P:

$$((b \to \ell) \wedge (\sim b \to \sim c) \wedge (c)) \to \ell.$$

$$\begin{array}{lll}
P & \Leftrightarrow & \sim((\sim b \vee \ell) \wedge (\sim(\sim b) \vee \sim c) \wedge c) \vee \ell & \text{(conditional)} \\
& \Leftrightarrow & \sim((\sim b \vee \ell) \wedge (b \vee \sim c) \wedge c) \vee \ell & \text{(double neg.)} \\
& \Leftrightarrow & (\sim(\sim b \vee \ell) \vee \sim(b \vee \sim c) \vee \sim c) \vee \ell & \text{(De Morgan's)} \\
& \Leftrightarrow & ((\sim(\sim b) \wedge \sim \ell) \vee (\sim b \wedge \sim(\sim c)) \vee \sim c) \vee \ell & \text{(De Morgan's)} \\
& \Leftrightarrow & ((b \wedge \sim \ell) \vee (\sim b \wedge c) \vee \sim c) \vee \ell & \text{(double neg.)} \\
& \Leftrightarrow & ((b \wedge \sim \ell) \vee \ell) \vee ((\sim b \wedge c) \vee \sim c) & \text{(assoc., comm.)} \\
& \Leftrightarrow & ((b \vee \ell) \wedge (\sim \ell \vee \ell)) \vee ((\sim b \vee \sim c) \wedge (c \vee \sim c)) & \text{(distributivity)} \\
& \Leftrightarrow & ((b \vee \ell) \wedge T) \vee ((\sim b \vee \sim c) \wedge T) & \text{(negation)} \\
& \Leftrightarrow & (b \vee \ell) \vee (\sim b \vee \sim c) & \text{(identity)} \\
& \Leftrightarrow & (b \vee \sim b) \vee \ell \vee \sim c & \text{(assoc., comm.)} \\
& \Leftrightarrow & T \vee \ell \vee \sim c & \text{(negation)} \\
& \Leftrightarrow & T & \text{(domination).}
\end{array}$$

Since P is a tautology, we can thus conclude that

$$(b \to \ell) \wedge (\sim b \to \sim c) \wedge (c) \Rightarrow \ell.$$

Example 3 Revisited – Using truth tables

Example (revisited). Recall we wanted to show that

$$(b \to \ell) \wedge (\sim b \to \sim c) \wedge (c) \Rightarrow \ell.$$

Alternative solution. We proceed by creating a truth table for the following statement, labelled P:

$$((b \to \ell) \wedge (\sim b \to \sim c) \wedge (c)) \to \ell.$$

b	ℓ	c	$b \to \ell$	$\sim b \to \sim c$	$(b \to \ell) \wedge (\sim b \to \sim c) \wedge (c)$	P
T	**T**	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**T**	**F**	**T**
T	**F**	**T**	**F**	**T**	**F**	**T**
T	**F**	**F**	**F**	**T**	**F**	**T**
F	**T**	**T**	**T**	**F**	**F**	**T**
F	**T**	**F**	**T**	**T**	**F**	**T**
F	**F**	**T**	**T**	**F**	**F**	**T**
F	**F**	**F**	**T**	**T**	**F**	**T**

Thus P is a tautology, so we can conclude that

$$(b \to \ell) \wedge (\sim b \to \sim c) \wedge (c) \Rightarrow \ell.$$