MATH1081
DISCRETE MATHEMATICS

Section 3

Proof

The defining characteristic of modern mathematics is *proof*. In ancient times mathematics consisted of a collection of rules for calculation which "seemed to work"; it appears that the cultures of Egypt, Babylon and others did not demand any more than this.

Since the time of the Ancient Greeks mathematicians have become more picky! We now want to be *sure*, as far as possible, that our techniques work; we also want to understand *why* they work and to know how they are related to each other, how they fit into the broader picture.

In today's world there are various concepts of proof.

Mathematical proof consists of logical deduction on the basis of agreed premises. Apart from human error the results are certain.

Scientific proof is achieved by induction. The results, in principle, can never be certain, although some scientific conclusions have so much confirmation that they can be regarded as virtually certain.

Statistical inference says that on the basis of certain observations, some conclusion is "likely", and can also give an estimate of "how likely".

Legal proof: "beyond reasonable doubt".

How to study proofs. Practise!! We shall look at many useful techniques of proof, but *there are no foolproof "recipes"*!

Note. The *results* that we prove in this section will generally be of no particular relevance to the course. The actual subject matter consists of the *methods* of investigation and proof used.

Textbook: J. Franklin and A. Daoud, *Proof in Mathematics: an Introduction*.

Recommended reading: G. Pólya, *How to Solve It*.

Example. $\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1\,000\,000}$.

Proof. We have

$$\frac{1}{1000} - \frac{1}{1001} = \frac{1001-1000}{1000\times 1001} = \frac{1}{1\,001\,000}\ .$$

But $1\,001\,000 > 1\,000\,000$, and both are positive numbers, so

$$\frac{1}{1\,001\,000} < \frac{1}{1\,000\,000}\ .$$

Therefore

$$\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1\,000\,000}\ .$$

Things to learn from this proof.

- *Always* explain what you are doing, and your reasons for drawing your conclusions.
- Simplify!
- Keep the aim in mind.
- *Plan* a solution.
- Work on one side of an equation or inequation to relate it to the other.

Calculators in proofs. Consider the following attempt at proving the above result.

Proof by calculator. To ten decimal places, we have

$$\begin{aligned} \tfrac{1}{1000} - \tfrac{1}{1001} &= 0{\cdot}001 - 0{\cdot}0009990010 \\ &= 0{\cdot}0000009990 \\ &< 0{\cdot}000001 \ , \end{aligned}$$

that is,

$$\tfrac{1}{1000} - \tfrac{1}{1001} < \tfrac{1}{1\,000\,000} \ .$$

Reasons for using calculators.

- They are quick and easy to use, especially for one–off applications.
- They are generally accurate.

Reasons for not using calculators.

- They suppress understanding.
- They suppress generality. For example, what can you say about $\frac{1}{2000} - \frac{1}{2001}$?
- They are hardly ever absolutely correct. This is especially a problem if you wish to determine whether two expressions are or are not equal. For example:

  (i) Redo the above proof with an 8-figure calculator.

  (ii) Is 10^{100} equal to $10^{100} + 1$?

  (iii) Are $8 + 31\sqrt{15}$ and $20\sqrt{41}$ equal?

Example. $\sqrt[8]{8!} < \sqrt[9]{9!}$

Proof. Clearly $1 < 9$, $2 < 9$, $\ldots$ and $8 < 9$, so

$$1 \times 2 \times \cdots \times 8 < \underbrace{9 \times 9 \times \cdots \times 9}_{8 \text{ times}} ,$$

that is, $1 \times 2 \times \cdots \times 8 < 9^8$. Multiplying both sides by $(1 \times 2 \times \cdots \times 8)^8$ gives

$$(1 \times 2 \times \cdots \times 8)^9 < (1 \times 2 \times \cdots \times 8)^8 \times 9^8 .$$

Rearranging terms,

$$(1 \times 2 \times \cdots \times 8)^9 < (1 \times 2 \times \cdots \times 8 \times 9)^8 ,$$

or in factorial notation

$$(8!)^9 < (9!)^8 .$$

Taking the positive 72nd root of both sides,

$$\sqrt[8]{8!} < \sqrt[9]{9!} ,$$

which is the required result.

Things to learn from this proof.

- Go back to definitions (expand the definitions).
- Simplify!
- A proof is often *discovered* by working backwards; but it must be *written* forwards.
- Explain logical and technical steps *in words* (with punctuation!)

GENERALISATION

The results which we have just proved are of very little interest in themselves, mainly because they refer only to specific numbers. However, it seems clear that in proving

$$\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000^2}$$

we did not use any special properties of the numbers 1000 and 1001, other than that they are consecutive positive integers. Thus we should expect a similar result to hold if 1000 is replaced by *any* $n \in \mathbb{Z}^+$ and 1001 by $n+1$. This process of guessing (and if possible proving) a result more inclusive than one already known is called **generalisation**. A statement such as

$$\text{“for all } n \in \mathbb{Z}^+ \text{ we have } \frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}\text{”}$$

is called a **universal** statement, or an “**all**” statement.

Theorem. For all $n \in \mathbb{Z}^+$ we have $\dfrac{1}{n} - \dfrac{1}{n+1} < \dfrac{1}{n^2}$.

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

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

But $n(n+1) > n^2$, and both sides are positive, so

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

Thus

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

as claimed.

Things to learn from this proof.

- A common proof pattern for "for all $x \in A$, property B holds" is

  "Let $x \in A$.
  $\vdots$
  Therefore x has property B."

- An "all" statement cannot be proved by listing examples (unless it is actually possible to check *all* examples).

"All" statements can be rewritten in many ways:

- for all $x \in A$, property B holds;
- for each $x \in A$, $x \in B$;
- every A is a B;
- if x is an A, then x is a B;
- no A is not a B;
- $\forall x \in A \quad x \in B$;
- B is true if A is true;
- A is true only if B is true;
- property A is sufficient for property B to hold;
- property B is necessary for property A to hold.

Examples of "all" statements.

- For all $n \in \mathbb{Z}^+$ we have $\sqrt[n]{n!} < \sqrt[n+1]{(n+1)!}$.
- $A \subseteq B$.
- The function $f : \mathbb{R} \to \mathbb{R}$ is equal to the function $g : \mathbb{R} \to \mathbb{R}$.
- Every differentiable function is continuous.
  Any differentiable function is continuous.
- No mathematicians are millionaires.
- $\forall x \in \mathbb{R} \quad (x+1)^2 = x^2 + 2x + 1$.
- A mark of 200 in Maths Extension 2 is sufficient to be allowed to attempt Discrete Mathematics.

Proof by exhaustion of cases.

Example. For all $x \in \mathbb{R}$ we have

$$|x-3| \leq x^2 - 3x + 4 \ .$$

Proof. Let $x \in \mathbb{R}$. Then either $x \geq 3$ or $x < 3$.

Case 1, $x \geq 3$. Then $(x-2)^2 + 3 \geq 0$, that is, $x^2 - 4x + 7 \geq 0$. Adding $x - 3$ to both sides,

$$x - 3 \leq x^2 - 3x + 4 \ .$$

But $|x-3| = x - 3$ since $x - 3 \geq 0$; so

$$|x-3| \leq x^2 - 3x + 4 \ .$$

Case 2, $x < 3$. Here $(x-1)^2 \geq 0$, that is, $x^2 - 2x + 1 \geq 0$. Hence

$$3 - x \leq x^2 - 3x + 4 \ .$$

In this case $x - 3 < 0$, so

$$|x-3| \ = \ -(x-3) \ = \ 3 - x \ \leq \ x^2 - 3x + 4 \ .$$

Since the two cases exhaust all possibilities, we have shown that

$$|x-3| \leq x^2 - 3x + 4$$

for all $x \in \mathbb{R}$.

Example. For all $n \in \mathbb{Z}$ we have $n^3 \equiv n \pmod 6$.

Proof. Let $n \in \mathbb{Z}$. There are six possible cases:

$$n \equiv 0, 1, 2, 3, 4, 5 \pmod 6 .$$

In these cases we have, respectively,

$$n^3 \equiv 0, 1, 8, 27, 64, 125 \pmod 6 .$$

Simplifying,

$$n^3 \equiv 0, 1, 2, 3, 4, 5 \pmod 6$$

respectively. Clearly in every case $n^3 \equiv n \pmod 6$.

Things to learn from these proofs.

- Explain what you're doing!
- Since these are "all" statements, the outline of the proof is as before.
- On the previous page we have another example of finding a proof by working backwards.
- Proof by exhaustion of cases is often useful where there is a "natural" division of the problem into a small number of cases; for example, in questions involving absolute values, congruences or divisibility.
- Clearly state the separate cases, and *be sure all cases really are covered*!

Example. Let $f : \mathbb{R} \to \mathbb{R}$. If f is an odd function, then $f(0) = 0$.

Proof. Let $f : \mathbb{R} \to \mathbb{R}$ be an odd function. Then

$$f(-x) = -f(x)$$

for all $x \in \mathbb{R}$. In particular this is true when $x = 0$; therefore $f(-0) = -f(0)$, that is,

$$f(0) = -f(0) \ .$$

Hence $2f(0) = 0$, and so

$$f(0) = 0 \ .$$

Things to learn from this proof.

- A frequent proof pattern for "if A then B" is

  "Suppose that A is true.

  $\vdots$

  Therefore B is true."

- Expand the definition.
- Keep the aim in mind! Here we have information about general values of $f(x)$, and we want to know something in particular about $f(0)$. So it is a natural step to substitute $x = 0$ and see what we get.

WRITING PROOFS

Proving a given statement can be said to involve two stages: discovering the reasons why the statement is true, then presenting these reasons as a coherent, carefully written argument. The first part may well be "mathematically" more difficult; however, the second is not easy either and will require a good deal of practice.

In constructing a mathematical proof, always take the point of view that you are writing it for *someone else* to read! If you "know what you mean" that's good, but it's only half the job. You should explain in words what you are doing, and give reasons for your conclusions: an unconnected string of equations is not adequate because it does not explain *why* a certain step is taken, *why* a particular claim is true. As a general rule, *a proof with no words is a very poor proof!*

In the following exercise you are given a theorem, together with the basic ideas needed to prove it. You are asked to write up a detailed proof of the theorem.

Theorem. Let n be an integer. If n is even then n^2 is even.

Basic ideas: $n = 2k$, so $n^2 = 4k^2$.

Theorem. Let n be an integer. If n is even then n^2 is even.

Proof. Let n be an integer. Suppose that n is even. Then by definition $n = 2k$ for some integer k. Squaring both sides,

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2) \ .$$

But since k is an integer $2k^2$ is also an integer. Therefore n^2 is even. This completes the proof.

Things to learn from this proof.

Clarity of expression.

- A proof must be written in complete sentences, with correct spelling and grammar! Among other things, each sentence must begin with a capital letter and end with a full stop.
- A sentence should begin with a *word!* It is usually regarded as poor style to begin a sentence with mathematical notation, as in, for example,

  "$n = 2k$ because n is even".

  This can be avoided by inserting some introductory words:

  "We can write $n = 2k$ because n is even",

  or by reordering the sentence:

  "Because n is even we have $n = 2k$".
- In text, writing equations consecutively with no words between them can make the proof unclear. Instead of

  "Let $n = 2k$, $k \in \mathbb{Z}$"

  write

  "Let $n = 2k$, where $k \in \mathbb{Z}$".

. . . continued

Things to learn from this proof.

Structure of a proof.

- Begin with a clear statement of the result you are proving. In a test or exam this will probably only mean copying out the question – all the same, it's important!
- Write the word "Proof"; then begin your argument.
- Any notation you use, any variables, must be introduced properly. If n is to be an integer you should say so: don't just start straight in with "$n = 2k$".
- It is vital that the *logic* of the proof be clear. In this case we are to show that if n is even then n^2 is even; as we have seen on page 15, a possible proof pattern for this is

  "Suppose that n is even... therefore n^2 is even".

  Both of these sentences appear in our proof.
- Include a conclusion which clearly indicates the end of the proof. You can write "QED" if you like but nowadays this is often regarded as a bit old–fashioned.

  QED stands for the Latin expression *quod erat demonstrandum*, "which was to be proved".

. . . continued

Things to learn from this proof.

Helping the reader.

- Give reasons for all your conclusions. If the reason is brief it is often good to give it before the conclusion: in the preceding proof "by definition" and "since k is an integer" are examples of this.
- It is also helpful to explain technical and algebraic steps ("squaring both sides"). Remember, you know what you are about to do – your readers don't! You should do all you can to help them.
- Often in this kind of exercise the ideas we give you will require amplification: with "$n = 2k$" you need to make the comment that k is an integer. (If it isn't, then n isn't even!) We shall also expect you to fill in algebraic steps where necessary.
- Try to get the level of argument right. *This is not easy!* Here, for example, it would not be good to say "n^2 is even because even times even is even", as this is more or less what you are asked to prove. The proof of any statement must be based upon simpler statements. Nevertheless, as a general rule in MATH1081 you may take as known anything you have done in school: this could include basic arithmetic, algebra, calculus, geometry and trigonometry.

Note. In MATH1081 proper presentation is regarded as essential for **all** proofs, not only those specifically tagged as writing exercises!

CONVERSES; IF AND ONLY IF

The **converse** of the statement

"if A then B"

is the statement

"if B then A".

Similarly, the converse of "every A is a B" is "every B is an A", the converse of "for all $x \in A$, $x \in B$" is "for all $x \in B$, $x \in A$", and so on.

Important. The converse of a true statement may or may not be true. So if you wish to prove some statement, it is **completely useless** to prove its converse instead. To do so is called the converse fallacy.

Examples.

- The statement

  "if you live in NSW then you live in Australia"

  is true; its converse,

  "if you live in Australia then you live in NSW",

  is false.
- The converse of the true statement

  "if a triangle has three equal sides then it has three equal angles"

  is

  "if a triangle has three equal angles then it has three equal sides",

  which is also true.
- The statement

  "all squares are quadrilaterals"

  is true; its converse,

  "all quadrilaterals are squares",

  is false.

Example. Let $f : \mathbb{R} \to \mathbb{R}$. Write the converse of

"if f is an odd function, then $f(0) = 0$".

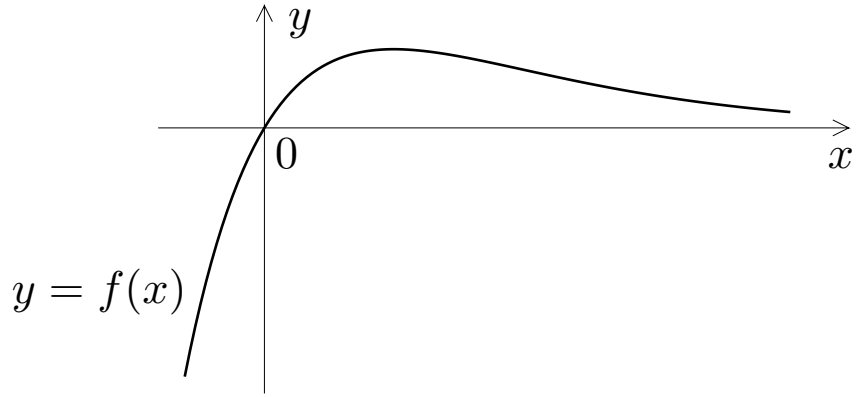
Is the converse true or false?

Solution. The converse is

"if $f(0) = 0$ then f is an odd function",

which is false.

Proof. If f has graph as shown, then $f(0) = 0$, but f is not an odd function.



Things to learn from this proof

- To disprove an "all" statement only one example is needed. Likewise, to disprove "if A then B" we need only produce one example where A is true but B is false.

Exercise. Which of the following statements say the same thing?

1. All Hamiltonian graphs are Eulerian.
2. All Eulerian graphs are Hamiltonian.
3. If a graph is Hamiltonian, then it is Eulerian.
4. A graph is Eulerian if it is Hamiltonian.
5. A graph is Eulerian only if it is Hamiltonian.
6. A graph is Hamiltonian only if it is Eulerian.
7. All graphs are Hamiltonian and Eulerian.
8. Every Eulerian graph is Hamiltonian.

If and only if. When a statement "if A then B" and its converse "if B then A" are both true we often combine the two statements and write

"A if and only if B",

sometimes abbreviated to

"A iff B".

This statement can be rephrased

- if A then B, and conversely;
- every A is a B, and every B is an A;
- A is a necessary and sufficient condition for B;
- $A \quad \Leftrightarrow \quad B$.

Examples.

- A triangle has three equal sides if and only if it has three equal angles.
- The real number x has a real square root if and only if $x \geq 0$.
- The set A equals the set B.
- An integer is divisible by 6 if and only if it is divisible both by 2 and by 3.

Note. An "if and only if" statement really consists of two statements, and its proof should therefore consist of two parts. Occasionally these can be combined, but this is not recommended. For "x is an A if and only if x is a B", a common proof pattern is:

"Firstly, let x be an A.

$\vdots$

Therefore x is a B.

Conversely, let x be a B.

$\vdots$

Therefore x is an A."

Theorem. Let n be an integer. Then $6 \mid n$ if and only if both $2 \mid n$ and $3 \mid n$.

Proof. Let $n \in \mathbb{Z}$. Firstly suppose that $6 \mid n$. That is, $n = 6k$ for some $k \in \mathbb{Z}$. Therefore

$$n = 2 \times 3k \ ,$$

and $3k \in \mathbb{Z}$, so $2 \mid n$. Similarly $3 \mid n$.

Conversely, let $2 \mid n$ and $3 \mid n$. Since $3 \mid n$ we have $n = 3l$ for some integer l. Now $2 \mid 3l$, so $3l$ is even; and obviously $2l$ is even; so $3l - 2l$ is even. That is, l is even. Therefore $l = 2m$ for some $m \in \mathbb{Z}$ and we have

$$n = 6m$$

with $m \in \mathbb{Z}$. Hence $6 \mid n$.

Both parts of the theorem have been proved.

Things to learn from this proof.

- Expand definitions!!
- Keep the goal in mind!!
- Make the logical subdivision clear by writing "Firstly ..." and "Conversely ...".
- Each part follows the normal format for an "if ... then" proof.
- "Similarly" saves work for the reader, not the writer!
- The two parts of an "if and only if" proof may require quite different ideas.

"SOME" STATEMENTS

An existential generalisation, or "**some**" statement, asserts that there exists something which satisfies a certain condition.

Note. "There exists something such that ..." means that there is *one object or more* with the given property. For example,

"there exists $x \in \mathbb{R}$ such that $x^2 = 2$"

is true; the fact that there are two different such x is irrelevant. Likewise,

"there exists an integer greater than π"

is true.

Examples of "some" statements.

- Some integers are positive.
- Some primes are even.
- There exists a function $f : \mathbb{R} \to \mathbb{R}$ which is both odd and even.
- Some students think Discrete Mathematics is easy.
- $S \neq \varnothing$.
- $6 \mid n$.
- a is odd.
- The vector $\mathbf{b}$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$.

A "some" statement can be written

- some A is a B;
- some As are Bs;
- there exists an A which is (also) a B;
- for some $x \in A$ we have $x \in B$;
- property B holds for some $x \in A$;
- $\exists x \in A \quad x \in B$.

To prove a "some" statement, the most concise method is to produce a specific object having the desired property.

Theorem. There exists a function $f : \mathbb{R} \to \mathbb{R}$ which equals its own derivative.

Proof. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = e^x$. Then for each $x \in \mathbb{R}$ we have

$$f'(x) = e^x = f(x) \ .$$

Thus $f' = f$.

Theorem. The vector $(6, -1, 5)$ is a linear combination of $(1, 1, 2)$ and $(1, 2, 3)$.

Note. By definition of a linear combination, we must prove that

$$(6, -1, 5) = \alpha(1, 1, 2) + \beta(1, 2, 3)$$

for some $\alpha, \beta \in \mathbb{R}$.

Proof. Choose $\alpha = 13$, $\beta = -7$. Then

$$\text{RHS} = (13, 13, 26) - (7, 14, 21) = \text{LHS} \ .$$

Things to learn from these proofs.

- As in many previous examples, we *discover* the proof by working backwards; but as always we must *write* the proof in the correct order.

  Note in particular that for the "linear combination" problem, if we start with the vector equation and find values of α and β but don't check that they work, then our proof is *not correct*.

- The real work here is all "behind the scenes", and it requires much more knowledge of calculus and algebra than the actual proof.

- The previous page gives an example of a "some" statement with an "all" statement embedded in the proof.

What is wrong with the following?

"**Theorem**". There exists $x \in \mathbb{R}$ such that

$$x^{18} + x^{16} + \cdots + x^4 + x^2 + 1 = 0 \ .$$

"**Proof**". Multiplying both sides by $x^2 - 1$ gives

$$(x^2 - 1)(x^{18} + x^{16} + \cdots + x^4 + x^2 + 1) = 0 \ ,$$

that is,

$$x^{20} - 1 = 0 \ .$$

So in fact there exist two solutions, $x = 1$ and $x = -1$.

Sometimes it is possible to prove a "some" statement without producing any particular object. This is often called a *non–constructive* existence proof, by contrast with our previous *constructive* proofs in which we gave a specific example of the required object.

Theorem. Let $f(x) = x^5 + 2x - 2$. Then $f(x) = 0$ for some $x \in [\,0, 1\,]$.

Proof. Let $f(x) = x^5 + 2x - 2$. Then $f(0) = -2$, which is negative, while $f(1) = 1$, which is positive. So the graph of f, being a continuous curve, must cross the x–axis somewhere between 0 and 1; and at this crossing point we have $f(x) = 0$. This completes the proof.

Theorem. There exist $x, y \in \mathbb{R}$ such that

$$\begin{cases} 209x - 432y = -172 \\ 168x + 746y = 331\ . \end{cases}$$

Proof. The determinant of the system is

$$(209 \times 746) + (432 \times 168)$$

which is clearly not zero. Therefore the system has a solution.

Things to learn from these proofs.

- For both of these results we assume a lot of background knowledge: (1) continuity and the Intermediate Value Theorem; (2) linear equations and determinants.
- It would be tedious to find actual values of x and y to prove (2), and in a sense impossible to find the actual solution in (1).
- "Clearly" does not mean you don't have to check the following statement!

Existence and uniqueness. A statement of the form

"there exists a unique $x \in S$ such that ..."

asserts that there is *one and only one* object having the given property.

The proof of such a statement will normally consist of two parts:

- show that there exists an object with the property;
- show that there cannot be two different objects with the property. A common proof pattern for this part is

  "Suppose that x_1 and x_2 both have the property.

  $\vdots$

  Therefore $x_1 = x_2$."

Theorem. *The division algorithm.* Let a and b be positive integers. Then there exists a unique pair of integers q, r such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < b \ .$$

Proof. *Existence.* Let a and b be positive integers; take $q = \lfloor a/b \rfloor$ and $r = a - qb$. Then clearly $a = qb + r$; also

$$q \leq \frac{a}{b} < q + 1 \quad \Rightarrow \quad 0 \leq \frac{a}{b} - q < 1 \quad \Rightarrow \quad 0 \leq r < b \ .$$

Uniqueness. Suppose that $a = q_1 b + r_1$, $0 \leq r_1 < b$ and also $a = q_2 b + r_2$, $0 \leq r_2 < b$. Then we have

$$0 = b(q_1 - q_2) + (r_1 - r_2)$$

and hence

$$q_1 - q_2 = \frac{r_2 - r_1}{b} \ .$$

Now $r_2 < b$, $r_1 \geq 0$, so $r_2 - r_1 < b$; similarly $r_2 - r_1 > -b$; so $-1 < q_1 - q_2 < 1$; but $q_1 - q_2$ is an integer and therefore must be zero. Thus $q_1 = q_2$ and consequently $r_1 = r_2$. Hence there is a unique pair of integers with the required properties.

Things to learn from this proof.

- Clearly distinguish the "existence" and "uniqueness" parts of the proof.
- Pattern of the uniqueness proof.

MULTIPLE QUANTIFIERS

The words "all" and "some" are called **quantifiers**. A statement may contain more than one quantifier.

Examples.

- For every $x \in \mathbb{Z}$, there exists $y \in \mathbb{Z}$ such that $y > x$.
- There exists $y \in \mathbb{Z}$ such that for every $x \in \mathbb{Z}$, $y > x$.
- $2^{29} - 1$ is composite.
- For any prime there is a larger prime.
- $(6, -1, 5)$ is a linear combination of $(1, 1, 2)$ and $(1, 2, 3)$.
- There is a function $f : \mathbb{R} \to \mathbb{R}$ which is equal to its own derivative.
- Every positive real number has a real square root.
- For all $A, B, C \subseteq \mathcal{U}$ we have $A \cup (B \cup C) = (A \cup B) \cup C$.
- The function $f : X \to Y$ is onto.

Theorem. Any composite positive integer has a factor greater than 1 and less than or equal to its square root.

Note. Making the quantifiers explicit, the statement is

> "for every composite integer n there exists c, a factor of n, such that $c > 1$ and $c \leq \sqrt{n}$".

Proof. Let n be a positive composite number. Then $n = ab$ for some integers $a, b > 1$. Now either $a \leq \sqrt{n}$ or $a > \sqrt{n}$.

Case 1, $a \leq \sqrt{n}$. Then choose $c = a$, which has the required properties.

Case 2, $a > \sqrt{n}$. Choose $c = b$. Then c is a factor of n. Also $c > 1$, and

$$c = b = \frac{n}{a} < \frac{n}{\sqrt{n}} = \sqrt{n}\,.$$

So in either case we have found a factor c of n such that $1 < c \leq \sqrt{n}\,$.

Things to learn from this proof.

- Rewrite the given statement if necessary to make the quantifiers clear.
- Pattern of "all" proof; within this, pattern of existence proof.
- Another example of proof by exhaustion of cases.
- Expand the definition!!

Theorem: $\lim_{x\to\infty} \dfrac{4x^2+7x+19}{2x^2+3} = 2.$

Note. According to the definition of a limit, we must show that for every $\varepsilon > 0$ there exists a real number M such that

$$\text{if} \quad x > M \quad \text{then} \quad \left|\frac{4x^2+7x+19}{2x^2+3} - 2\right| < \varepsilon \ .$$

Proof. Let $\varepsilon > 0$.

Choose $M = \max\left(1, \dfrac{10}{\varepsilon}\right)$.

Let $x > M$. Then

$$x > 1 \quad \text{and} \quad x > \frac{10}{\varepsilon} \ ,$$

. . . continued

(*continued*) so

$$\begin{aligned}
\left|\frac{4x^2+7x+19}{2x^2+3}-2\right| &= \left|\frac{7x+13}{2x^2+3}\right| \\
&= \frac{7x+13}{2x^2+3} \\
&< \frac{7x+13x}{2x^2} && \text{because } x>1 \\
&= \frac{10}{x} \\
&< \frac{10}{10/\varepsilon} \\
&= \varepsilon\ .
\end{aligned}$$

Therefore $\lim\limits_{x\to\infty} \dfrac{4x^2+7x+19}{2x^2+3} = 2.$

Things to learn from this proof.

- Expand the definition!!
- The logical structure of the statement to be proved is

  "for all ... there exists ... such that if ... then ...",

  and the proof follows this structure *precisely*. It is often helpful to write down the logical skeleton first and fill in the gaps later, probably after having done some rough working.
- Working backwards seems to be even more important here than usual – how could you possibly guess a suitable choice for M otherwise?
- Simplification, especially getting rid of "insignificant" terms in the fraction. The helpful trick

  $$x > 1 \ , \quad \text{so} \quad 13 < 13x$$

  is also worth remembering.
- There are many other suitable choices for M, for example

  $$M = \max\left(3, \frac{6}{\varepsilon}\right) \ .$$

Exercise. Prove one of the following from the definition (that is, by using ε and M). Be extremely careful with the logic and setting out of your proof.

1. (*easier*) $\lim_{x\to\infty} \dfrac{3x^2}{x^2+1} = 3.$

2. (*harder*) $\lim_{x\to -2} x^2 + 5x + 3 = -3.$

   Recall that by definition, $\lim_{x\to a} f(x) = L$ means

   "for each $\varepsilon > 0$ there exists $\delta > 0$ such that if $0 < |x - a| < \delta$, then $|f(x) - L| < \varepsilon$"

One of these will be proved next lecture.

Change of order of quantifiers. Two adjacent quantifiers *of the same kind* can be interchanged. For example

$$\exists\alpha \in \mathbb{R} \quad \exists\beta \in \mathbb{R} \quad (6,-1,5) = \alpha(1,1,2) + \beta(1,2,3)$$

means the same as

$$\exists\beta \in \mathbb{R} \quad \exists\alpha \in \mathbb{R} \quad (6,-1,5) = \alpha(1,1,2) + \beta(1,2,3)$$

since both statements assert that there exist two real numbers satisfying the equation. Likewise,

$$\forall A \subseteq \mathcal{U} \quad \forall B \subseteq \mathcal{U} \quad A \cap B = B \cap A$$

and

$$\forall B \subseteq \mathcal{U} \quad \forall A \subseteq \mathcal{U} \quad A \cap B = B \cap A$$

both say that the equation is true for any two subsets of $\mathcal{U}$.

However, . . .

. . . an “all” and a “some” quantifier **may not** be interchanged.

Example. The statement

$$\forall x \in \mathbb{Z} \quad \exists y \in \mathbb{Z} \quad y > x$$

says that for every integer there is a larger integer, which is true. But

$$\exists y \in \mathbb{Z} \quad \forall x \in \mathbb{Z} \quad y > x$$

says that there exists an integer which is greater than *every* integer, which is false. So clearly these two statements are not the same.

A puzzle. Sometimes in ordinary English the order of quantifiers is unclear. For example,

“you can fool some of the people all of the time”

could be written

$$\exists P \quad \forall t \quad \text{person } P \text{ can be fooled at time } t$$

or

$$\forall t \quad \exists P \quad \text{person } P \text{ can be fooled at time } t \ ,$$

but which of these did the original speaker (Abraham Lincoln, 1809–1865) mean?

Exercise. If ... denotes an expression containing no quantifiers, rewrite the statement

$$\forall w\ \exists x\ \forall y\ \forall z\ \ \ldots$$

in as many ways as possible with the order of quantifiers changed.

Answer. There is only one possibility,

$$\forall w\ \exists x\ \forall z\ \forall y\ \ \ldots\ .$$

Note that $\forall w$ and $\forall y$ cannot be interchanged as they are not adjacent, $\exists x$ gets in the way.

Theorem. Let $f, g : \mathbb{R} \to \mathbb{R}$ and let a, b be real numbers. If

$$\lim_{x\to\infty} f(x) = a \quad \text{and} \quad \lim_{x\to\infty} g(x) = b$$

then

$$\lim_{x\to\infty} (f(x) + g(x)) = a + b \ .$$

Proof. Suppose that

$$\lim_{x\to\infty} f(x) = a \quad \text{and} \quad \lim_{x\to\infty} g(x) = b \ ,$$

and let $\varepsilon > 0$. Then there exist real numbers M_1, M_2 such that

$$\text{if} \quad x > M_1 \quad \text{then} \quad |f(x) - a| < \frac{\varepsilon}{2} \qquad \text{and} \qquad \text{if} \quad x > M_2 \quad \text{then} \quad |g(x) - b| < \frac{\varepsilon}{2} \ .$$

Choose $M = \max(M_1, M_2)$, and suppose that $x > M$. Then $x > M_1$ and $x > M_2$, so

$$|f(x) - a| < \frac{\varepsilon}{2} \qquad \text{and} \qquad |g(x) - b| < \frac{\varepsilon}{2} \ ;$$

. . . continued

therefore

$$\begin{aligned} |(f(x)+g(x))-(a+b)| &= |(f(x)-a)+(g(x)-b)| \\ &\leq |f(x)-a|+|g(x)-b| \\ &< \frac{\varepsilon}{2}+\frac{\varepsilon}{2} \\ &= \varepsilon\ . \end{aligned}$$

Thus $\lim_{x\to\infty}(f(x)+g(x))=a+b$, as claimed.

Things to learn from this proof.

- Clearly distinguish between what is given (in this problem, two limits) and what you have to prove (another limit).
- The main "imaginative" step in the proof is to come up with two positive numbers which add up to ε. We chose $\varepsilon/2$ and $\varepsilon/2$, but many other choices would have been possible.
- Once again we see the importance of working backwards in a complicated problem.
- As so often happens, going back to definitions is a profitable idea.

"NOT" and CONTRADICTION

The **negation** of a statement is the assertion that the statement is false. We often write

$$\sim A \quad \text{or} \quad \sim (A)$$

for the negation of A.

Examples.

- The negation of

  $$2 + 2 = 5$$

  is "it is false that $2 + 2 = 5$", or more simply

  $$2 + 2 \neq 5 \ .$$

- The negation of

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

  is

  $$\frac{1}{n} - \frac{1}{n+1} \geq \frac{1}{n^2} \ ,$$

  but...

- ...*beware*! The negation of "$A \subset B$" is *not* "$A \supseteq B$". It is "$A \not\subset B$", which cannot in general be simplified further.

Example. Is the statement

$$8 + 31\sqrt{15} = 20\sqrt{41}$$

true or false? Prove your answer.

Answer. The statement is false.

Proof. Suppose that the statement is true. Squaring both sides,

$$14479 + 496\sqrt{15} = 16400 \ ,$$

so

$$496\sqrt{15} = 1921 \ .$$

Squaring both sides again,

$$3690240 = 3690241 \ .$$

But this is false. Hence our original supposition was false; that is,

$$8 + 31\sqrt{15} \neq 20\sqrt{41} \ .$$

Things to learn from this proof.

- This is called **proof by contradiction** or *reductio ad absurdum*.
- To decide whether a statement is true or false, work out the consequences until you find something which is known to be true or false. If it is false you have a proof by contradiction. If it is true **and all the steps are reversible** you have a direct proof.
- Be very careful to distinguish between the following formats:

"Suppose A is true. ⋮ Therefore B. But B is false. Therefore A is false."
VALID

"Suppose A is true. ⋮ Therefore B. But B is true. Therefore A is true."
INVALID

. . . continued

- A proof by contradiction of a statement A will look like this:

  "Suppose that A is false.
  $\vdots$
  Therefore ...
  But this is false.
  So the initial assumption was false.
  That is, A is true."

  Similarly, a statement "if A then B" may be proved using the pattern

  "Suppose that A is true but B is false.
  $\vdots$
  Therefore ...
  But this is a contradiction.
  So, if A is true then B is true."

Theorem. There are infinitely many primes.

Proof by contradiction. Suppose that there are only finitely many primes. Let $p_1, p_2, \ldots, p_n$ be a complete list of primes. Consider the number

$$N = p_1 p_2 \cdots p_n + 1 \ .$$

Now N is an integer, $N > 1$, and therefore has a prime factor p. However $p \neq p_1$, for otherwise we would have

$$p \mid N \quad \text{and} \quad p \mid p_1 p_2 \cdots p_n \ ,$$

so $p \mid 1$, which is impossible; and similarly $p \neq p_2, \ldots, p_n$. Therefore our initial set of primes was not a complete list after all. This contradiction completes the proof.

Things to learn from this proof.

- A proof by contradiction begins by assuming the negation of the statement to be proved.
- Be extremely careful with the logic and setting out of a proof by contradiction.
- Make the proof easier to read by introducing suitable notation. (Euclid couldn't do this!!)
- Here we have a "sub–proof" by contradiction within the main proof by contradiction.
- Justifiable use of "similarly".
- See Martin Aigler and Günter M. Ziegler, *Proofs from THE BOOK*, for six different proofs of this result!

The **contrapositive** of a statement

"if A then B"

is the statement

"if not B then not A".

Similarly, the contrapositive of "every A is a B" is "every 'non–B' is a 'non–A'", or, in better English, "anything which is not a B is not an A".

Unlike the converse, the contrapositive of a statement **is logically equivalent** to the original. So if you wish to prove a statement, it is permissible (and may well be easier) to prove the contrapositive instead. Therefore another possible proof pattern for "if A then B" is

"Suppose that B is false.

$\vdots$

Therefore, A is false."

Examples.

- Let $f : X \to Y$. The contrapositive of

  "if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$"

  is

  "if $f(x_1) = f(x_2)$, then $x_1 = x_2$".

- The contrapositive of

  "all horses are animals"

  is

  "anything which is not an animal cannot be a horse".

- Let $n \in \mathbb{Z}$. The contrapositive of

  "if n^2 is even, then n is even"

  is

  "if n is not even, then n^2 is not even",

  or more simply

  "if n is odd, then n^2 is odd".

Theorem. Let $n \in \mathbb{Z}$. If n^2 is even, then n is even.

Proof. Let n be an integer. We shall prove the contrapositive of the required statement,

"if n is odd, then n^2 is odd".

So, suppose that n is odd. Then by definition

$$n = 2k + 1$$

for some $k \in \mathbb{Z}$. Squaring both sides,

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

and since k is an integer $2k^2 + 2k$ is also an integer. Thus n^2 is odd. The proof is finished.

Things to learn from this proof.

- The contrapositive is valuable here since "n is odd" gives more direct information about n than "n^2 is even".
- If you're going to use the contrapositive, it's a good idea to say so at the beginning.
- Standard "if ... then" proof.
- Definitions!!
- Remember the goal!!

Theorem: $\sqrt{2}$ is irrational.

Proof by contradiction. Suppose that $\sqrt{2}$ is not irrational. Then we can write

$$\sqrt{2} = \frac{m}{n} \ ,$$

where m and n are integers with no common factor. Squaring both sides leads to

$$m^2 = 2n^2 \ .$$

Hence m^2 is even, so m is even and we can write $m = 2k$. Substituting into the previous equation, $4k^2 = 2n^2$, and so

$$n^2 = 2k^2 \ .$$

Therefore n^2 is even; hence, n is even. So m and n have a common factor, namely, 2. But this is false. Therefore our original assumption (that $\sqrt{2}$ is not irrational) must be false; that is, $\sqrt{2}$ is irrational.

Things to learn from this proof.

- As always for a *reductio ad absurdum*, the proof begins by assuming that the given statement is false.
- Proving that a number is irrational will nearly always involve proof by contradiction.
- Do not attempt this proof while on a cruise with a group of Ancient Greek mathematicians.

More examples of negation.

- The negation of

  "all first–year maths is easy"

  is

  "not all first–year maths is easy",

  in other words,

  "some first–year maths is hard".

- The negation of

  "there exists $x \in \mathbb{R}$ such that $x^2 = -1$"

  is

  "there does not exist $x \in \mathbb{R}$ such that $x^2 = -1$",

  which can be restated

  "for all $x \in \mathbb{R}$ we have $x^2 \neq -1$".

The last two examples illustrate the following.

- The negation of

  "for all $x \in \mathcal{U}$, ..."

  is

  "for some $x \in \mathcal{U}$, not (...)".

- The negation of

  "for some $x \in \mathcal{U}$, ..."

  is

  "for all $x \in \mathcal{U}$, not (...)".

Hence to disprove an "all" statement we must prove a "some" statement, which may be done by producing *one* example: this is often referred to as a *counterexample*.

Likewise, to disprove a "some" statement, we prove an "all" statement. In practice, it is often easier to prove the "some" statement false using proof by contradiction than to directly prove the "all" statement true.

Example. Prove or disprove: no prime is congruent to 14 modulo 25.

Answer. The statement is false.

Note. To disprove this "all" statement, we prove the negation

"there exists a prime congruent to 14 modulo 25"

by producing one example.

Proof. Take $p = 89$. Then p is a prime; furthermore, since $89 = 3 \times 25 + 14$, we have $p \equiv 14 \pmod{25}$.

Things to learn from this proof.

- Since it is not obvious whether the statement is true or false, and since there is no obvious way of "working backwards", try a few examples. This might reveal a counterexample, or it might suggest a pattern which could be used to prove the statement true.
- In looking at examples, remember that (initially) primes are more numerous than numbers congruent to 14 modulo 25.

Negation of multiple quantifiers. The above equivalences can be used repeatedly to simplify the negation of statements containing multiple quantifiers.

Example. Simplify the negation of

$$\forall x \quad \forall y \quad \exists z \quad \dots \ .$$

Solution. The negation is

$$\sim \big(\forall x \quad \forall y \quad \exists z \quad \dots \big) \ ,$$

that is,

$$\exists x \quad \sim \big(\forall y \quad \exists z \quad \dots \big) \ ,$$

or

$$\exists x \quad \exists y \quad \sim \big(\exists z \quad \dots \big) \ ,$$

or finally

$$\exists x \quad \exists y \quad \forall z \quad \sim \big(\dots \big) \ .$$

Definition. A set $S \subseteq \mathbb{R}$ is called **open** if

$$\forall x \in S \quad \exists \varepsilon > 0 \quad \forall y \in \mathbb{R} \quad \text{if} \quad |x - y| < \varepsilon \quad \text{then} \quad y \in S \ .$$

Example. Is $[\,1, 2\,)$ open? Prove your answer.

Answer. $[\,1, 2\,)$ is not open. We shall prove

$$\exists x \in [\,1, 2\,) \quad \forall \varepsilon > 0 \quad \exists y \in \mathbb{R} \quad |x - y| < \varepsilon \quad \text{and} \quad y \notin [\,1, 2\,) \ .$$

Proof. Choose $x = 1$.
Let $\varepsilon > 0$.
Choose $y = 1 - \frac{1}{2}\varepsilon$.
Then

$$|x - y| = |\,\tfrac{1}{2}\varepsilon\,| < \varepsilon \ ;$$

but $y < 1$, so clearly $y \notin [\,1, 2\,)$.

Things to learn from this proof.

- Draw pictures to assist your intuition.
- The negation of "if A then B" can be expressed "A and not B".
- The first three lines of the proof deal (in the correct order!) with the three quantifiers in the statement to be proved.
- After we have done the background work, this proof is short and not very difficult. This is typical of existence proofs.
- Roughly, a set is open if it contains no part of its "boundary".

MATHEMATICAL INDUCTION

Mathematical induction is a very useful method of proving statements about all the natural numbers. The proof by mathematical induction of a statement

"for all $n \in \mathbb{N}$, ..."

consists of two parts:

(i) prove ... for $n = 0$;

(ii) prove that **if** ... is true for some particular value of $n \in \mathbb{N}$, **then** ... is true for $n + 1$.

Likewise,

"for all $n \geq n_0$, ..."

can be proved by mathematical induction:

(i) prove ... for $n = n_0$;

(ii) prove that if ... is true for some particular value of $n \geq n_0$, then it is true for $n + 1$.

Step (i) is called the **basis** of the proof, and step (ii) the **inductive step**.

Theorem. For all integers $n \geq 1$ we have $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$.

Proof. For $n = 1$ we have

$$\text{RHS} = \tfrac{1}{6} \times 1 \times 2 \times 3 = 1 = \text{LHS} \ .$$

So the equation is true when $n = 1$.

Now assume the equation true for *some particular* value of $n \geq 1$, that is,

$$1^2 + 2^2 + \cdots + n^2 = \tfrac{1}{6}n(n+1)(2n+1) \ .$$

We must prove that

$$1^2 + 2^2 + \cdots + (n+1)^2 = \tfrac{1}{6}(n+1)((n+1)+1)(2(n+1)+1) \ .$$

But we have

$$\text{LHS} \ = \ (1^2 + 2^2 + \cdots + n^2) + (n+1)^2 \ = \ \tfrac{1}{6}n(n+1)(2n+1) + (n+1)^2 \ ,$$

using the inductive assumption. Simplifying,

$$\begin{aligned} \text{LHS} &= \tfrac{1}{6}(n+1)\big[n(2n+1) + 6(n+1)\big] \\ &= \tfrac{1}{6}(n+1)[\,2n^2 + 7n + 6\,] \\ &= \tfrac{1}{6}(n+1)(n+2)(2n+3) = \text{RHS} \ . \end{aligned}$$

We have shown that the equation is true for $n = 1$; and that if it is true for some particular n, then it is true for $n+1$. Therefore, by induction, the equation is true for all integers $n \geq 1$.

Things to learn from this proof.

- An induction proof will generally look something like this:

  "Let $n = 1$.
  $\vdots$
  Therefore the statement is true for $n = 1$.
  Now assume that the statement is true for some particular n.
  We must prove that. . .
  $\vdots$
  Therefore, the statement is true for $n + 1$.
  By induction, the statement is true for all $n \geq 1$."

  The line "We must prove that. . . " is strongly recommended but not absolutely essential.

- To make the method of induction work we need some (fairly) simple relation between the statement for n and that for $n + 1$.

Theorem. For all real numbers x with $0 < x < 1$, and for all integers $n \geq 0$, we have

$$(1-x)^n \geq 1 - nx \ .$$

Proof. Let $0 < x < 1$.

For $n = 0$ the statement is $1 \geq 1$, which is clearly true.

Now let k be a specific non–negative integer and assume the result true when $n = k$, that is,

$$(1-x)^k \geq 1 - kx \ . \qquad (*)$$

We must show that the result is true when $n = k + 1$, that is,

$$(1-x)^{k+1} \geq 1 - (k+1)x \ .$$

Now $1 - x$ is a positive number, so multiplying both sides of the inequality $(*)$ by $1 - x$ gives

$$(1-x)^{k+1} \geq (1-x)(1-kx) \ ;$$

expanding the right hand side and noting that $kx^2 \geq 0$, we have

$$\begin{aligned}(1-x)^{k+1} &\geq 1 - (k+1)x + kx^2 \\ &\geq 1 - (k+1)x \ .\end{aligned}$$

We have shown that the inequality is true for $n = 0$; and that if it is true for $n = k$, then it is true for $n = k + 1$. By induction, the inequality is true for all integers $n \geq 0$.

Things to learn from this proof.

- Here we have proved by induction a doubly quantified statement of the form "for all x, for all n, . . . ". We have handled the "for all x" as in earlier proofs by beginning with "let x be . . . ", and we have handled the "for all n" by induction.
- In this case the connection between the property for k and for $k + 1$ is that we need to multiply one more term into the left hand side.
- *Never* multiply an inequality by anything unless you know for sure whether the "anything" is positive or negative!

Exercise. Alternatively, as a calculus exercise, this result can be proved by using the Mean Value Theorem. Try it!

Strong induction or **extended induction**.

Suppose that a certain statement is true for $n = 0$ and $n = 1$; and that if it is true for two consecutive integers n and $n + 1$, then it is true for the next integer $n + 2$. Here again we may conclude that the statement is true for all $n \geq 0$.

Theorem. Suppose the sequence $\{ u_n \}$ has the properties

$$u_0 = 2 \ , \quad u_1 = 6 \ ,$$
$$u_{n+2} = 6u_{n+1} - 8u_n \quad \text{for all } n \geq 0 \ .$$

Then for all $n \geq 0$ we have $u_n = 4^n + 2^n$.

Proof. For $n = 0$ and $n = 1$ the result becomes

$$2 = 1 + 1 \quad \text{and} \quad 6 = 4 + 2$$

respectively; both of these are true.

Assume the formula is true for some particular $n \geq 0$, and also for $n + 1$; that is,

$$u_n = 4^n + 2^n \quad \text{and} \quad u_{n+1} = 4^{n+1} + 2^{n+1} \ .$$

We must prove that

$$u_{n+2} = 4^{n+2} + 2^{n+2} \ .$$

Now

$$\text{LHS} = u_{n+2} = 6u_{n+1} - 8u_n \qquad (*)$$

(given), and substituting the assumed equalities for u_n and u_{n+1}, we have

$$\begin{aligned} \text{LHS} &= 6 \times \left(4^{n+1} + 2^{n+1}\right) - 8 \times \left(4^n + 2^n\right) \\ &= (6 \times 4 - 8)\, 4^n + (6 \times 2 - 8)\, 2^n \\ &= 4^2 \times 4^n + 2^2 \times 2^n \\ &= \text{RHS} \ . \end{aligned}$$

By induction, the formula is true for all $n \geq 0$.

Things to learn from this proof.

- Here, the proof of the equation for any particular value (say, $n+2$) depends on knowing it to be true for *two* previous values ($n+1$ and n). So the proof will start out by checking the equation for the first *two* values, namely, 0 and 1.
- Keep the aim in mind!!
- Each case is related to the previous cases by the *recurrence relation*

$$u_{n+2} = 6u_{n+1} - 8u_n \ .$$

- In a case like this make sure you are absolutely clear on what is given and what you are required to prove. In particular, the recurrence relation $u_{n+2} = 6u_{n+1} - 8u_n$ is given to be true for all n, and so it is correct to use this equation in line $(*)$.

We can extend the method of mathematical induction even further: suppose

(i) a certain statement is true for $n = 1$;

(ii) for any particular $n \geq 1$, **if** the statement is true for $1, 2, 3, \ldots, n$, **then** it is true for $n + 1$.

Then the statement is true for all $n \geq 1$.

Theorem. Let $\pi = 3{\cdot}14159\cdots = d_0{\cdot}d_1d_2d_3\cdots$; define a sequence $\{\, u_n \,\}$ by $u_0 = 1$ and

$$u_{n+1} = d_0u_n + d_1u_{n-1} + \cdots + d_nu_0$$

for $n \geq 0$. Then for $n \geq 1$ we have

$$u_n \leq 9 \times 10^{n-1} \ .$$

Proof. For $n = 1$ the result says $u_1 \leq 9$, which is true since $u_1 = 3$.

Assume that the result is true for $1, \ldots, k$, where k is some particular integer, $k \geq 1$. We shall show

$$u_{k+1} \leq 9 \times 10^k \ .$$

Now

$$\begin{aligned} \text{LHS} &= d_0u_k + d_1u_{k-1} + \cdots + d_{k-1}u_1 + d_ku_0 \\ &\leq 9 \times (u_k + u_{k-1} + \cdots + u_1 + u_0) \\ &\leq 9 \times (9 \times 10^{k-1} + 9 \times 10^{k-2} + \cdots + 9 + 1) \end{aligned}$$

by the induction hypothesis. Hence

$$\text{LHS} \leq 9 \times \big(\underbrace{99\cdots99}_{k \text{ digits}} + 1\big) = 9 \times 10^k \ ,$$

which is what we had to show.

By strong induction the result is true for all $n \geq 1$.

Theorem. Every positive rational number less than 1 can be written as a sum of distinct unit fractions.

Note. Making this more explicit, we seek to prove that for every positive integer m the following is true: for each integer $n > m$, there exist positive integers $d_1, d_2, \ldots, d_s$, all different, such that

$$\frac{m}{n} = \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_s} \ .$$

Proof by induction on m. Let $m = 1$ and $n > 1$; choose $s = 1$ and $d_1 = n$. Then

$$\frac{m}{n} = \frac{1}{d_1} \ ,$$

so the statement is true. This proves the basis of the induction.

Now let m be a specific positive integer, $m \geq 2$, and suppose that the result is true for fractions with numerators $1, 2, \ldots, m-1$. We must deduce that it is true for numerator m. Let $n > m$; since $0 < \frac{m}{n} < 1$, there is an integer $q \geq 2$ such that

$$\frac{1}{q} \leq \frac{m}{n} < \frac{1}{q-1} \ . \qquad (*)$$

We write $\frac{m}{n}$ as the largest possible unit fraction, plus a remainder:

$$\frac{m}{n} = \frac{1}{q} + \frac{qm-n}{nq} \ .$$

. . . continued

Now $(*)$ implies that $0 \leq qm - n < m$, and we consider two cases.

If $qm - n = 0$ then $\frac{m}{n} = \frac{1}{q}$, and the desired conclusion holds with $s = 1$ and $d_1 = q$.

If $qm - n$ is not zero, it is one of the integers $1, 2, \ldots, m-1$, and we may apply the inductive hypothesis. Since $qm - n < m < n < nq$, there exist positive integers $d_1, d_2, \ldots, d_s$, all of them different, such that

$$\frac{qm-n}{nq} = \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_s} \ .$$

Because

$$\frac{qm-n}{nq} < \frac{n}{nq} = \frac{1}{q} \ ,$$

every one of the denominators on the right hand side satisfies $d_k > q$; therefore all the denominators on the right hand side of

$$\frac{m}{n} = \frac{1}{q} + \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_s}$$

are different, and the result is true for fractions with numerator m. By extended induction, the theorem is proved.

Comment. Actually, rational numbers greater than 1 can also be written as sums of distinct unit fractions. This is a bit harder to prove (try it!).

Theorem. Any integer greater than or equal to 2 can be written as a product of primes.

Note. Stated more explicitly, the theorem is

"for all $n \geq 2$, there exist primes $p_1, p_2, \ldots, p_s$ such that $n = p_1 p_2 \cdots p_s$".

Proof. The statement is true for $n = 2$, since 2 is a product of *just one* prime, namely, itself.

Consider a specific integer $n \geq 2$, and suppose the statement true for $2, 3, \ldots, n$. We shall show that $n+1$ can be written as a product of primes. Now $n+1$ is either prime or composite.

Case 1, $n + 1$ is prime. Then $n + 1$ is a product of just one prime.

Case 2, $n + 1$ is composite. Then

$$n + 1 = ab$$

for some integers $a, b > 1$. Here $2 \leq a \leq n$ and $2 \leq b \leq n$, so by the inductive assumption

$$a = p_1 p_2 \cdots p_s \quad \text{and} \quad b = q_1 q_2 \cdots q_t$$

for some primes $p_1, p_2, \ldots, p_s$ and $q_1, q_2, \ldots, q_t$. Hence

$$n + 1 = p_1 p_2 \cdots p_s \, q_1 q_2 \cdots q_t \ ,$$

and $n + 1$ is again a product of primes.

In both cases the result is true for $n + 1$; hence, by induction, the result is true for all $n \geq 2$.

Things to learn from these proofs.

- The inequality for u_n is not valid for $n = 0$; therefore the basis of the proof is the case $n = 1$. Similarly, prime factorisation holds only for $n \geq 2$.
- Structure of an extended induction proof: "For $n = 2$ the statement is . . . , which is true. Assume the statement is true for $2, 3, \ldots, n$ . . . so it is true for $n + 1$.
- In both the unit fractions result and the factorisation result we have used the method of exhaustion of cases for part of the proof.
- In the sequence proof we use the truth of the formula for *all* previous cases, that is, for $1, 2, \ldots, n$. However in Case 2 of the factorisation proof, we use only *two* previous cases – and we don't actually know which two!! Likewise with the unit fractions proof – we assume the result is true for all of the numerators $1, 2, \ldots, m$, because we don't know which one we are going to need.
- Use definitions!

LOGIC and TRUTH TABLES

Logic is the study of how the truth or falsity of a given statement follows (or not!) from the truth of other statements. For example, given the statements

"if G is an Eulerian graph, then no vertex of G has odd degree"

and

"G is an Eulerian graph",

we may deduce that

"no vertex of G has odd degree".

Note. The logic we have used here says nothing about whether the first two statements are actually true or not, but only that **if** they are true, **then** the third is also.

Of course, we could ask whether the first two statements are true (on the basis of other, presumably simpler, statements), and this inquiry would again involve the use of logic.

Definition. A **proposition** is a statement which is unambiguously true or false.

Examples.

- $1 + 1 = 2$;
- $2 + 2 = 3$;
- my birthday is on 29 February;
- there exist infinitely many primes p for which $2^p - 1$ is also prime.

These are **not** propositions:

- $2 + 2$;
- $x^2 + x - 12 = 0$;
- mathematics is more interesting than football;
- do you agree with the previous statement?;
- this sentence is false;
- "yields a false statement when preceded by its own quotation" yields a false statement when preceded by its own quotation.

More complicated expressions can be built up from other propositions by using **logical operators**. The most useful of these are

- "not", symbolised by $\sim$;
- "and", symbolised by $\wedge$;
- "or", symbolised by $\vee$;
- "exclusive or", symbolised by $\oplus$;
- "if ... then", symbolised by $\rightarrow$;
- "if and only if", symbolised by $\leftrightarrow$.

Examples. If p and q are propositions then

- $p \wedge (\sim q)$ means "p and not q";
- $(\sim q) \rightarrow (\sim p)$ is the *contrapositive* of $p \rightarrow q$;
- $q \rightarrow p$ is the *converse* of $p \rightarrow q$.

The above propositions, made up of simpler propositions by the use of logical operators, are called *compound propositions*.

If we think of p, q as being not specific propositions but variables which may represent any propositions, then we call the combined statements **propositional forms**.

Example. If

$$p = \text{“I will study tonight”},$$
$$q = \text{“I will go to the pub tonight”},$$
$$r = \text{“I will submit my assignment on time tomorrow”},$$

write the following statements in logical notation.

(i) I will go to the pub tonight, but I will submit my assignment on time tomorrow.

(ii) I will not both study and go to the pub tonight.

(iii) I will submit my assignment late tomorrow unless I avoid the pub and study instead tonight.

(iv) I will only submit my assignment on time tomorrow if I study tonight.

Answers.

(i) $q \wedge r$.

Note that “but” is logically the same as “and”.

(ii) $\sim(p \wedge q)$.

(iii) $\sim((\sim q) \wedge p) \rightarrow (\sim r)$.

Note that “A unless B” means “A if not B”.

The word “instead” has no logical function and can be ignored.

(iv) $r \rightarrow p$.

Note that $p \rightarrow r$ may well be true, but it is **not** what the given expression says!

With the same meanings for p, q, r, write the following in ordinary English.

(i) $(\sim p) \wedge (\sim q)$.

(ii) $(p \to r) \wedge (q \to \sim r)$.

Answers.

(i) "I will not study tonight, and I will not go to the pub tonight".

More concisely, "I will neither study nor go to the pub tonight".

"Neither ... nor ..." means "not ..., and not ...".

(ii) "If I study tonight then I will submit my assignment on time tomorrow; while if I go to the pub tonight then I will submit my assignment late".

Here "while" is just another way of expressing "but" or "and".

Observe that the truth or falsity of a compound proposition such as $p \vee q$ does not depend on what the propositions p and q *actually are*, but only on whether they are true or false.

The main task of the logic of propositions, therefore, is this: given **truth values** T or F for propositions $p, q, r, \ldots$, determine the truth value of a certain compound proposition. This can be done step by step once we know the truth values of the basic combinations $\sim p$, $p \wedge q$, and so on.

Negation. The truth value of $\sim p$ is the opposite of the truth value of p. We can express this by giving the **truth table** for $\sim p$.

p	$\sim p$
T	F
F	T

"**And**". The conjunction $p \wedge q$ is true when both p and q are true, and false otherwise. Its truth table is

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

Problem. Is the above definition circular? If so, how can we fix it?

"**Or**". The disjunction $p \vee q$ is true when either p or q, or both, is true, and false otherwise. It has the following truth table.

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

Note. This is the *inclusive* meaning of "or".

"**Exclusive or**". The exclusive or $p \oplus q$ is true when either p or q is true, but not both, and is false otherwise. Its truth table is as shown.

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

We can use these results to find the truth tables of further compound propositions.

Example. Construct truth tables for $\sim(p \vee q)$ and for $(\sim p) \wedge (\sim q)$.

Solution.

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

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

Definition. Two propositional forms are **logically equivalent** if they have the same truth values for each possible allocation of truth values to the variables in them. We denote the logical equivalence of P and Q by writing $P \Leftrightarrow Q$.

Example. From the above truth tables,

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

This is one of **De Morgan's** laws.

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

Proof. We find the truth tables as shown.

p	q	r	$q \vee r$	$p \wedge q$	$p \wedge r$	LHS	RHS
T	T	T	T	T	T	T	T
T	T	F	T	T	F	T	T
T	F	T	T	F	T	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

Since the left hand side and the right hand side have the same truth values in all cases, $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$. This is one of the **distributive** laws.

Two propositional forms can be shown *not* to be equivalent by constructing tables as above and observing that the resulting truth values are *not* always the same, or by producing specific interpretations of the variables in such a way that one of the forms is true and the other false.

Example. Show that $p \wedge q$ and p are not logically equivalent.

Solution. Choose the propositions

$$p = \text{“}2 + 3 = 5\text{”} \quad \text{and} \quad q = \text{“}2 \times 3 = 5\text{”} \ .$$

Then p is true, while $p \wedge q$ is false. Thus the two propositional forms are not logically equivalent.

Definition. A propositional form that is always true, no matter what the truth values of the propositional variables that occur in it, is called a **tautology**. A propositional form that is always false is called a **contradiction**. A form that is neither a tautology nor a contradiction is called a **contingency**.

Examples.

- $p \vee (\sim p)$ is a tautology.
- $p \wedge (\sim p)$ is a contradiction.
- $p \wedge q$ is a contingency.

To check these assertions, either consider what the propositions mean, or construct their truth tables.

Note.

- Any two tautologies are logically equivalent, since they have the same truth value in all cases. Likewise all contradictions are logically equivalent.
- Conversely, if a proposition is equivalent to a tautology, then the proposition is itself a tautology.

Laws of logical equivalence. Let p, q, r be propositional variables, let $\mathbf{T}$ be a tautology and $\mathbf{F}$ a contradiction. We have already seen the following equivalences:

$$\begin{aligned} \sim(p \vee q) &\Leftrightarrow (\sim p) \wedge (\sim q) \\ p \wedge (q \vee r) &\Leftrightarrow (p \wedge q) \vee (p \wedge r) \\ p \vee (\sim p) &\Leftrightarrow \mathbf{T} \\ p \wedge (\sim p) &\Leftrightarrow \mathbf{F} \ . \end{aligned}$$

There are many more. *Apart from the different notation they are identical with the laws of set algebra!* Compare, for example,

$$\begin{aligned} \sim(p \vee q) \Leftrightarrow (\sim p) \wedge (\sim q) \quad &\text{and} \quad (A \cup B)^c = A^c \cap B^c \\ p \vee (\sim p) \Leftrightarrow \mathbf{T} \quad &\text{and} \quad A \cup A^c = \mathcal{U} \\ p \wedge (\sim p) \Leftrightarrow \mathbf{F} \quad &\text{and} \quad A \cap A^c = \varnothing \ . \end{aligned}$$

As with laws of set algebra, logical equivalences come in dual pairs, for example,

$$p \vee (\sim p) \Leftrightarrow \mathbf{T} \quad \text{and} \quad p \wedge (\sim p) \Leftrightarrow \mathbf{F} \ .$$

Here are some of the most useful logical equivalences.

- Commutative laws:

$$p \wedge q \;\Leftrightarrow\; q \wedge p \qquad \text{and} \qquad p \vee q \;\Leftrightarrow\; q \vee p \;.$$

- Associative laws:

$$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r) \qquad \text{and} \qquad (p \vee q) \vee r \Leftrightarrow p \vee (q \vee r) \;.$$

- Distributive laws:

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r) \qquad \text{and} \qquad p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r) \;.$$

- Idempotent laws:

$$p \wedge p \;\Leftrightarrow\; p \qquad \text{and} \qquad p \vee p \;\Leftrightarrow\; p \;.$$

- Double negation law:

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

. . . continued

- De Morgan's laws:

$$\sim(p \wedge q) \Leftrightarrow (\sim p) \vee (\sim q) \qquad \text{and} \qquad \sim(p \vee q) \Leftrightarrow (\sim p) \wedge (\sim q) \ .$$

- Identity laws:

$$p \wedge \mathbf{T} \ \Leftrightarrow \ p \qquad \text{and} \qquad p \vee \mathbf{F} \ \Leftrightarrow \ p \ .$$

- Domination laws:

$$p \vee \mathbf{T} \ \Leftrightarrow \ \mathbf{T} \qquad \text{and} \qquad p \wedge \mathbf{F} \ \Leftrightarrow \ \mathbf{F} \ .$$

- Laws of negation:

$$p \vee (\sim p) \ \Leftrightarrow \ \mathbf{T} \qquad \text{and} \qquad p \wedge (\sim p) \ \Leftrightarrow \ \mathbf{F} \ .$$

Example. Use the laws of logical equivalence to simplify

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

Solution. We have

$$\begin{aligned}
(p \wedge (\sim q)) \vee (\sim(p \vee q)) &\Leftrightarrow (p \wedge (\sim q)) \vee ((\sim p) \wedge (\sim q)) && \text{(De Morgan's law)} \\
&\Leftrightarrow (p \vee (\sim p)) \wedge (\sim q) && \text{(distributive law)} \\
&\Leftrightarrow \mathbf{T} \wedge (\sim q) && \text{(law of negation)} \\
&\Leftrightarrow \sim q \ . && \text{(commutative law, and identity law)}
\end{aligned}$$

"**If ... then**". The truth table for the *conditional proposition* or *implication* $p \to q$ (which we usually read as "if p then q" or "p implies q") is

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

That is, $p \to q$ is always true except in the case p true, q false.

Logical equivalences involving $\rightarrow$.

First we show that $p \rightarrow q \Leftrightarrow (\sim p) \vee q$.

p	q	$\sim p$	$p \rightarrow q$	$(\sim p) \vee q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

This is useful since we can now replace $p \rightarrow q$ by $(\sim p) \vee q$ and then apply the 17 logical equivalences that we already know.

Example. We can re–express the negation of $p \to q$ as

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

So to disprove "if p then q" we have to find a case where p is true and q is false – as we have seen before!!

Example. Also,

$$\begin{aligned} (\sim q) \to (\sim p) &\Leftrightarrow (\sim(\sim q)) \vee (\sim p) && \text{(equivalence for } \to) \\ &\Leftrightarrow q \vee (\sim p) && \text{(double negation law)} \\ &\Leftrightarrow (\sim p) \vee q && \text{(commutative law)} \\ &\Leftrightarrow p \to q\ . \end{aligned}$$

This shows that a statement "if p then q" is true when its contrapositive is true, and false when its contrapositive is false.

Example. Are $p \to q$ and $q \to p$ logically equivalent?

Answer. No. We construct the truth table.

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

We might as well stop here: the truth values will not always be the same, so $p \to q$ is not logically equivalent to $q \to p$. This shows that the truth values of a proposition and its converse are not always the same.

Note that the *non–equivalence* of two propositional forms would normally be very difficult to prove by "algebraic" methods.

Example. An example involving $\rightarrow$ and tautologies:

$$(p \wedge q) \rightarrow p$$

is a tautology.

Proof by truth table:

p	q	$p \wedge q$	$(p \wedge q) \rightarrow p$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

Exercise. Prove this by using logical equivalences to show

$$(p \wedge q) \rightarrow p \;\Leftrightarrow\; \cdots \;\Leftrightarrow\; \mathbf{T}\ .$$

"**If and only if**". The *biconditional* proposition $p \leftrightarrow q$ is true when p and q are both true or both false, and is false otherwise. Its truth table is

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

We can check by a truth table that

$$p \leftrightarrow q \;\Leftrightarrow\; (p \rightarrow q) \wedge (q \rightarrow p) \;,$$

which corresponds with our previous "informal" definition of "if and only if".

Note carefully the difference between the symbols $\Leftrightarrow$ and $\leftrightarrow$. If P and Q are two propositional forms, then

$$P \Leftrightarrow Q$$

is a statement which tells you something about these two forms, whereas

$$P \leftrightarrow Q$$

is a combination of the two propositional forms into a single form.

There is, however, a close relationship between logical equivalence and the biconditional proposition.

Theorem. Two propositional forms P and Q are logically equivalent if and only if $P \leftrightarrow Q$ is a tautology.

Proof. Suppose that $P \leftrightarrow Q$ is a tautology. Then for all truth values of the constituent variables, the truth value of $P \leftrightarrow Q$ is T. Thus for all truth values of the variables, P and Q have the same truth value. So by definition, $P \Leftrightarrow Q$.

Conversely, if $P \Leftrightarrow Q$ then in all cases P and Q have the same truth values; so in all cases $P \leftrightarrow Q$ is true. That is, $P \leftrightarrow Q$ is a tautology.

Example. We know that

$$\sim(p \vee q) \;\Leftrightarrow\; (\sim p) \wedge (\sim q)\ ;$$

therefore

$$(\sim(p \vee q)) \leftrightarrow ((\sim p) \wedge (\sim q))$$

is a tautology. Check this by algebra or by a truth table.

Definition. Let P and Q be propositional forms. Suppose that in any case where P is true, Q is also true. Then we say that P **logically implies** Q and write $P \Rightarrow Q$.

Example. Consider the propositional forms P and Q, defined to be

$$(p \to q) \wedge r \quad \text{and} \quad p \to (q \wedge r) \ .$$

respectively. Does P logically imply Q? Does Q logically imply P?

Solution. We draw up a truth table for both propositional forms.

p	q	r	$p \to q$	$q \wedge r$	$(p \to q) \wedge r$	$p \to (q \wedge r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	T	T	T	T
F	T	F	T	F	F	T
F	F	T	T	F	T	T
F	F	F	T	F	F	T

The cases where P is true occur in rows $1, 5$ and 7; in these cases Q is always true. That is, if P is true then Q is also true. Therefore P logically implies Q.

On the other hand, when Q is true, P is not always true, for example in row 8. Therefore Q does not logically imply P.

As with logical equivalence (compare page 104), be sure you understand the difference between $\Rightarrow$ and $\rightarrow$. If P and Q are propositional forms then

$$P \Rightarrow Q$$

is a statement which tells you something about these two propositions (namely, that if P is true then Q must also be true), while

$$P \rightarrow Q$$

is a single propositional form built up from these two. Once again, however, though the two symbols are not identical, there is a close relationship between them.

Theorem. Let P and Q be propositional forms. Then P logically implies Q if and only if $P \rightarrow Q$ is a tautology.

Proof. Suppose that $P \rightarrow Q$ is a tautology. Then it is never false; so there is no case where P is true and Q is false. That is, in every case where P is true, Q is also true. But this is exactly what is meant by $P \Rightarrow Q$.

Conversely, suppose that $P \Rightarrow Q$ and consider the truth values of $P \rightarrow Q$.

- *Case 1*, P is true. Since $P \Rightarrow Q$ we see that Q is also true. Therefore $P \rightarrow Q$ is true.
- *Case 2*, P is false. Then $P \rightarrow Q$ is true, regardless of the truth value of Q.

Thus $P \rightarrow Q$ is true in every case, that is, it is a tautology.

Example. Show that

$$((p \to q) \wedge p) \;\Rightarrow\; q \;.$$

Solution. We draw up a truth table for LHS $\to$ RHS.

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

Since the final result is always T we see that

$$((p \to q) \wedge p) \to q$$

is a tautology. That is,

$$((p \to q) \wedge p) \;\Rightarrow\; q \;.$$

Exercise. Repeat this problem using the method of page 106. (The working is almost identical.)

Theorem. Let P and Q be propositional forms. Then $P \Leftrightarrow Q$ if and only if both $P \Rightarrow Q$ and $Q \Rightarrow P$.

Proof. Exercise.

VALID AND INVALID ARGUMENTS

Recall the argument we saw before:

> "If G is an Eulerian graph, then no vertex of G has odd degree.
> G is an Eulerian graph.
> Therefore, no vertex of G has odd degree."

The deduction made here uses the **rule of inference**

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore\ q\ . \end{array}$$

Such an argument is **valid** because the **conclusion** (the last statement) *must always be true*, provided that the **hypotheses** (earlier statements) are true.

This particular rule of inference is commonly known as *modus ponens*.

The following supposed rule of inference is **invalid**,

$$\begin{array}{l} p \to q \\ q \\ \hline \therefore\ p\ , \end{array}$$

since in some cases the hypotheses will be true and the conclusion false. For example, take

$$p = \text{“I live in Queensland”}$$
$$q = \text{“I live in Australia”}\ .$$

In fact the above (invalid) argument is simply the converse fallacy.

Note carefully that the conclusion of a valid argument is *not always true*! For example,

> “If my pet Fluffy drinks milk, then she is a dinosaur.
> My pet Fluffy drinks milk.
> Therefore, my pet Fluffy is a dinosaur.”

To be sure of reaching a true conclusion we need a valid argument **and** true hypotheses.

Another rule of inference, known as *modus tollens*, is

$$\begin{array}{l} p \to q \\ \sim q \\ \hline \therefore \sim p \ . \end{array}$$

For example,

> "If you kick this goal, then we will win the match.
> We did not win the match.
> Therefore, you did not kick the goal."

Essentially, this is proof by use of the contrapositive.

The *hypothetical syllogism* is the rule of inference

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore\ p \to r\ . \end{array}$$

For example,

> "If I study hard, then I will earn a degree.
> If I earn a degree, then I will get a good job.
> Therefore, if I study hard, then I will get a good job."

So far, we have been agreeing on the validity of rules of inference in a very informal manner; now we would like to approach the question more carefully. For a start, we use truth tables to check that the rule of inference *modus ponens*

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore\ q \end{array}$$

is a valid method of argument. First we construct a truth table showing truth values of the hypotheses and the conclusion.

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

The only case in which both the hypotheses are true occurs in the first row; and here the conclusion is also true. Hence, the argument is valid.

To confirm that the converse fallacy

$$\begin{array}{l} p \to q \\ q \\ \hline \therefore\ p \end{array}$$

does *not* constitute a valid argument, we again construct a truth table.

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

Here the hypotheses are true in the first and third rows; but in these rows the conclusion is *not always true*. In particular, the third row exhibits a case where the hypotheses may be true and the conclusion false. Thus, this is not a valid argument.

Valid arguments and tautologies. Observe that the truth table we used on page 113 to confirm that *modus ponens* is valid is very similar to that used on page 108, showing that $(p \to q) \wedge p$ logically implies q.

Theorem. An argument

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

is valid if and only if $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \Rightarrow Q$, that is, if and only if the proposition

$$(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \to Q \qquad \otimes$$

is a tautology.

. . . continued

Proof. Suppose the given argument is valid. Now the proposition $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ is either true or false.

Case 1, $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ is false. Then $\otimes$ is true (regardless of the truth value of Q).

Case 2, $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ is true. Then Q is true, so $\otimes$ has the form $a \to b$, with a, b both true; and this is a true statement.

Thus $\otimes$ has the truth value T in all cases, and is therefore a tautology.

Conversely, suppose that the argument is invalid. Then there exists a case in which all of $P_1, P_2, \ldots, P_n$ are true yet Q is false. In this case $\otimes$ is of the form $a \to b$ with a true, b false; so $\otimes$ is false. Since $\otimes$ is not always true, it is not a tautology.

Things to learn from this proof.

- Structure of an "if and only if" proof.
- Proof by division into cases.
- Proof by contrapositive.

Another valid argument form is

$$\begin{array}{l} p \vee q \\ p \to r \\ q \to r \\ \hline \therefore\ r\ . \end{array}$$

We prove this by showing that

$$((p \vee q) \wedge (p \to r) \wedge (q \to r)) \to r$$

is a tautology. For brevity we write it as $P \to r$.

p	q	r	$p \vee q$	$p \to r$	$q \to r$	P	$P \to r$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	T	T	T	T	T
T	F	F	T	F	T	F	T
F	T	T	T	T	T	T	T
F	T	F	T	T	F	F	T
F	F	T	F	T	T	F	T
F	F	F	F	T	T	F	T

Thus $P \to r$ is a tautology, and the argument form is valid.

In fact this argument form is simply proof by **division into cases**!

Theorem. The rule of inference

$$\frac{(\sim p) \to \mathbf{F}}{\therefore\ p}$$

is valid.

Proof. By the laws of logical equivalence,

$$\begin{aligned}
((\sim p) \to \mathbf{F}) \to p &\Leftrightarrow (\sim(\sim p) \vee \mathbf{F}) \to p && \text{(equivalence for } \to) \\
&\Leftrightarrow (p \vee \mathbf{F}) \to p && \text{(double negation)} \\
&\Leftrightarrow p \to p && \text{(identity law)} \\
&\Leftrightarrow (\sim p) \vee p && \text{(equivalence for } \to) \\
&\Leftrightarrow \mathbf{T}\ . && \text{(law of negation)}
\end{aligned}$$

This is a formal verification of the method of **proof by contradiction**.

Problem. Suppose it is known that

"If I don't leave home early I will miss the bus.
If I run fast I will catch the bus.
I caught the bus."

Did I leave home early?

Solution. Let's see if we can prove that I left home early. First we write the argument in symbolic form. Define the propositions

$h =$ "I left home early"
$c =$ "I caught the bus"
$r =$ "I ran fast".

We need to decide whether or not the argument form

$$\begin{array}{l} (\sim h) \to (\sim c) \\ r \to c \\ c \\ \hline \therefore\ h \end{array}$$

is valid.

Method 1, rules of inference. The first statement is logically equivalent to its contrapositive $c \to h$. But we also know from the third statement that c is true. Therefore by *modus ponens* h is also true. Hence the argument is valid and **yes**, I did leave home early.

. . . continued

Method 2, truth table. We show that

$$((\sim h) \to (\sim c)) \wedge (r \to c) \wedge c$$

logically implies h. Denote the above statement by H.

h	c	r	$(\sim h) \to (\sim c)$	$r \to c$	c	H	h
T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	T
T	F	T	T	F	F	F	T
T	F	F	T	T	F	F	T
F	T	T	F	T	T	F	F
F	T	F	F	T	T	F	F
F	F	T	T	F	F	F	F
F	F	F	T	T	F	F	F

Now H is true in the first two rows; and in these cases h is true too. Therefore

$$(((\sim h) \to (\sim c)) \wedge (r \to c) \wedge c) \;\; \Rightarrow \;\; h \;;$$

this proves that the argument is valid and I must have left home early.

Method 3, logical equivalences. Use the laws of logical equivalence to prove that

$$(((\sim h) \to (\sim c)) \wedge (r \to c) \wedge c) \to h$$

is a tautology.

Problem. Suppose again that

> "If I don't leave home early I will miss the bus.
> If I run fast I will catch the bus.
> I caught the bus."

Did I run fast?

Solution. Defining the propositions h, c and r as above, we now have to consider the argument form

$$\begin{array}{l} (\sim h) \to (\sim c) \\ r \to c \\ c \\ \hline \therefore\ r\ . \end{array}$$

If we try to deduce r from the given statements we don't seem to have any success. This leads us to suspect that the argument form is **invalid**. We can check this by using a truth table to show that there is a case where the three hypotheses are true but the conclusion is false. Since we only need one case there is no need to work out the whole truth table; a bit of trial and error shows that if we take

$$h \text{ true}, \quad c \text{ true} \quad \text{and} \quad r \text{ false}$$

then the assumptions are true but r is false. Thus the argument is invalid and we **cannot** conclude that I ran fast.

. . . continued

Does this mean that I didn't run fast? Consider the argument form

$$\begin{array}{l} (\sim h) \rightarrow (\sim c) \\ r \rightarrow c \\ c \\ \hline \therefore \sim r \ . \end{array}$$

In the same way (*exercise!*) we can show that this argument is not valid either. So, given the three facts we started with, did I run fast? The answer is that **we cannot tell** because insufficient information is given.

Exercise. Discuss the validity of the following argument.

"Any argument which obeys all the laws of logic is valid.

This argument does not obey all the laws of logic.

Therefore, this argument is not valid."