# A Guide to *Writing* Proofs

**Slide 1**

**Propositions**

Britain is an island

Every island can be circumnavigated

If a set is non-empty it contains an element

All Martians like pepperoni on their pizza

The factorial of $6$ is 27

A *proposition* is a statement which is either true or false. We may not know which but it has to be one or the other, but not both! Some examples of propositions are given in Slide 1, while in Slide 2 we give some English phrases which can not be construed to be propositions.

In order to establish the truth of a proposition we use *reasoning*, which can be formal or informal. In fact there are many different kinds of reasoning, most of which are spurious. Some examples are given in Slide 3.

Here we will confine our attention to a particular form of reasoning called *deductive reasoning*. It will be informal but based on formal logical principles, called Natural Deduction.

One way to argue for the truth of a proposition is to give a *deductive argument*. An example is given in Slide 4. A deductive argument, or *proof*, consists of a sequence of propositions each of which is

- taken for granted, or self-evidently true; these are called *premises*
- implied logically by the truth of some previous propositions on the list.

Such an argument establishes the truth of the last proposition in the sequence. This proposition is said to be a *theorem* because it has a *proof*, namely this deductive argument.

So for example in Slide 4 we have a proof of the proposition

Britain can be circumnavigated

Slide 2

## Non-propositions

Could you please pass the salt?

Ready steady, go

Vote for Tom Cruise

Show your work clearly

Good luck to Sunderland

Slide 3

## False Reasoning Principles

**By superiority:** 298743 is a prime number because I say so.

**By similarity:** This proposition is true because it is very similar to one which I proved yesterday.

**By obviousness:** Obvious!

**By rumour:** I read somewhere on the Internet that this proposition was true.

**By intimidation:** This is so trivial.

**By plausibility:** It sounds reasonable.

**Slide 4**

**Deductive Argument**

Example:

S1: Britain is an island

S2: Every island can be circumnavigated

Therefore
S3: Britain can be circumnavigated

A sequence of propositions, each one of which is either a *premise*, which is taken for granted, or follows logically from the previous ones.

It uses two propositions, which are not justified, S1 and S2. Indeed logical principles can not help to establish their truth, and they are *premises* in the argument. But the third step, concluding S3 from S1 and S2, uses a valid logical principle. This principle has a fancy name in formal logic, called *instantiation*.

How do we come up with these deductive arguments, and how do we know a given method of argument is valid? In Slide 5 we give three different informal arguments. Which, if any, do you think is reasonable?

More generally, given a proposition how do we find a proof, along the lines described in Slide 4, which establishes its truth? This is a difficult, even impossible, problem in general. Large numbers of mathematicians are employed throughout the world to come up with proofs for theorems. This is an intrinsically creative process which can not be mechanised. But we can learn certain principles, which help in the exposition of proofs which you have found. Moreover these principles can be of some help when searching for proofs, but here we concentrate on their exposition. These principles will help you *structure* your proofs so that when you write them down other people will be able to understand them. Remember a proof is not a proof unless lots of people agree that it is!

To best way to consider these principles is to consider the *structure*, in particular the logical structure, of the proposition we are trying to establish. Some of these propositions are *elementary* or *atomic* in that they can not be broken down into lower level propositions and reasoning can not be used to establish their truth or falsity. For example

Britain is an island

is an elementary proposition. It can be broken down into the components *Britain* and *island*, and a relation between them, but none of these lower-level components are themselves propositions, which can be logically investigated. If you want to establish the truth of this proposition logic will be of little help. You will need a plane, a boat, or a chat with a man in a pub. However the proposition

**if** you are in Manchester **then** you are in the rain

does have a logical structure. It is constructed from two lower level propositions, *you are in Manchester* and *you are in the rain* using an **implication** connective. This is a particularly common structure for announcements, or propositions which people would like to be true. Another example is given in Slide 6, which uses the **and** connective.

**Slide 5**

## Valid Arguments?

If Abraham Lincoln was Ethiopian, then he was African. Abraham Lincoln was not African. Therefore he was not Ethiopian.

If astrology is a true science, then the economy is improving. The economy is improving. Therefore, astrology is a true science.

If it is cloudy, then it is going to rain. If it is going to rain, then I should take my raincoat with me.
Therefore if it is cloudy, I should take my raincoat with me.

**Slide 6**

## Logical structure of Propositions

Elementary or atomic:

Britain is an island

Can **not** be broken down further into propositions

Decomposition:

Cats and Dogs are here

Can be decomposed into:

Cats are here **and** Dogs are here

**Slide 7**

## The Logical Structure of Propositions

**Conjunction, and:** Jill is twelve **and** Jack is fourteen

**Disjunction, or:** I am going to the movies **or** I am going to the pub

**Negation, not:** I am **not** going to the movies

**Implication, implies:** x is fourteen **implies** y must be greater than 2

Initially we will consider four possible ways of structuring propositions, using the *connectives* given in Slide 7; these are called the *propositional* connectives. But beware; it is not always obvious how propositions written in English can be structured using these connectives. For example how would you write the following, using these connectives and atomic propositions?

> The moon's not a balloon only if I'm not the Queen of Sheba.

Also keep in mind that textbooks use a variety of symbols for these connectives. The most common are:

**and:** $A \wedge B$

**or:** $A \vee B$

**not:** $\neg A$

**implies:** $A \longrightarrow B$

Nevertheless it is the structure of propositions in terms of these connectives which determines both how we look for proofs and how we explain them. Even more crucially the validity of a logical argument never depends on the actual atomic propositions used; it is only the logical structure of propositions which count. For this reason when discussing proofs we will often use arbitrary uppercase letters to play the role of arbitrary propositions; in Slide 8 we explain how to abstract from a particular argument to a more general argument couched in terms of arbitrary propositions. In the following Slide 9 we introduce some general notation. Suppose we have a finite set of propositions $S_1,\ S_2,\ \ldots,\ S_n$, not necessarily atomic, which we are willing to take for granted; so in proofs we can use them as *premises*. When can we say that another proposition P follows logically from this set of premises? When this is the case we will write

$$S_1,\ S_2,\ \ldots,\ S_n \vdash P \tag{1}$$

For example, referring to Slide 8 the question is whether the judgement

$$A \ \textbf{implies}\ B,\ \textbf{not}\ B \vdash \textbf{not}\ A$$

Slide 8

## Propositional meta-variables

If Abraham Lincoln was Ethiopian, then he was African. Abraham Lincoln was not African.

Therefore he was not Ethiopian.

Atomic Propositions:

- A: Abraham Lincoln was Ethiopian
- B: Abraham Lincoln was African

Formal Argument:

Given premises

- A **implies** B
- **not** B

Is **not** A a logical consequence?

Slide 9

## Notation

$S_1, S_2, \ldots, S_n \vdash \mathrm{P}$

Means:

There is a valid logical argument, with which we can derive the proposition $P$ from the finite set of premises $S_1, \ldots S_n$

Question:

How can we develop valid logical arguments?

is valid.

We now look at a number of different ways of elaborating proofs of propositions from premises using valid logical arguments, thereby establishing instances of (1). As we have already mentioned these arguments are often, but not always, guided by the structure of the proposition we are trying to prove. But remember many statements written in English will have to be rearranged in order for their logical structure as propositions to become apparent. And many more statements will not really be amenable to any form of logical decomposition.

## Conjunction

The formal rules associated with the use of *conjunctive* propositions, P **and** Q, more or less coincide with the intuitive use of **and** in everyday conversation. Put another way, the manner in which we use this construct in every day reasoning can be justified by more formal logic reasons in a straightforward fashion. There is even a risk of introducing confusion by discussing their precise formulation; see Slide 10 and Slide 11. However rather than discussing these obvious rules let us see an example of their use, in Slide 12

**Slide 10**

**Establishing Conjunctive Propositions**

Rules for Introducing **and**

To establish $P$ **and** $Q$:

1. Establish $P$
2. Establish $Q$
3. Conclude ($P$ **and** $Q$)

Fancy name: Conjunction Introduction – **AndIntro**

Suppose we have two premises, the proposition P **and** Q, and the proposition R. From these can we derive the proposition Q **and** R ? Well the only possibility of establishing a conjunctive proposition is to use the rule **AndIntro**, which requires us to first establish the individual components Q, R. However one of these, R, is a premise, while the other can be established from the second premise using the rule **AndElim**. The formal proof is detailed in Slide 12, which establishes the judgement

P **and** Q, R $\vdash$ Q **and** R.

## Implication

Implications appear under various informal guises. See Slide 13 for examples of some ways in which they are expressed in English.

Slide 11

## How do use Conjunctions? - and

How do we make use of (P **and** Q) ? :

| | |
|---|---|
| From | (P **and** Q) we can conclude P |
| From | (P **and** Q) we can conclude Q |

Fancy name: Conjunction Elimination: **AndElim**

All very obvious

Slide 12

## An example proof

P **and** Q, R $\vdash$ Q **and** R

A proof:

| | |
|---|---|
| 1. P **and** Q | premise |
| 2. R | premise |
| 3. Q | **AndElim** to 1 |
| 4. Q **and** R | **AndIntro** to 2,3 |

**Slide 13**

### Implicative Propositions

Examples:

| |
|---|
| *if* the sun is up it is daytime |
| $n$ is prime *implies* $n$ is odd |
| for even integer $n$, $n^2$ is also an even integer |
| $B$ only if $A$ |

Each has a *premise* and a *conclusion*

Decomposition:

| |
|---|
| *Premise:* the sun is up |
| *Conclusion:* it is daytime |

It is important to realise that the truth of an implication does not in general depend on the truth of its components, the *premise* or the *conclusion*. It merely says that **if** the premise is true then so is the conclusion. More concretely it means:

if you give me a proof of the *premise* I will be able to construct a proof of the *conclusion*.

For example the proposition

if 7 is even then so is 9

is true. If somebody ever gave me a proof that 7 is even I would be able to construct a proof that 9 is even.

**Establishing Implications:** The general form of the proof of an implication is given in Slide 14. To prove the proposition

$$P \text{ implies } Q$$

it is sufficient to prove the conclusion $Q$ under the assumption that $P$, the premise, holds. Let us look at an example proof, of the mathematical proposition

If $n$ is even then so is $n^2$

This proof is laid out in Slide 15, where the lines are numbered for reference. Here the premise is

$n$ is an even number

and so the first line of the proof starts with this as an assumption. To derive the conclusion, that $n^2$ is even, we must find a number $w$ such that $n^2$ is equal to $2w$; this is what it means for $n^2$ to be even. To find this $w$ we must, of course, use the information in the assumption. The second line analyses the assumption to obtain some information from it, namely the existence of the number $k$. We can now use $k$ to find the required $w$, namely $2k^2$, in line 4. So lines 1 to 4 consist of a *hypothetical* proof of the fact that $n^2$ is even, using the proposition $n$ *is an even number* as an assumption, or temporary premise. Therefore we can apply the rule **ImpIntro**, in the final line of the proof, to establish the implicative proposition.

Slide 14

## Proving Implications

Every proof of $\boxed{P \text{ implies } Q}$ has the form:

1. Assume the proposition $P$ to be true
2. Using this assumption establish $Q$
3. Conclude: $\boxed{P \text{ implies } Q}$ is true

All the work is in the Part 2.

Fancy name: Implication Introduction - **ImpIntro**

Slide 15

## An example proof

$\boxed{\text{If } n \text{ is even then so is } n^2}$

1. Assume $n$ is an even number
2. So there is some $k$ such that $n = 2k$ (Definition of even)
3. Therefore, using 2, $n^2 = 2(2k^2)$
4. Therefore $n^2$ is even (Definition of even)
5. Therefore, by **ImpIntro** from 1 and 4,

if $n$ is even then so is $n^2$

Note that every line in the proof has a justification. It either follows from previous lines, by an elementary mathematical fact or the application of a definition, or is an application of one of our methods of reasoning; here we have used the method **ImpIntro**, which in fact requires the existence of a *sub-proof* before it can be applied. Note also that the proof is *not* a record of how I found or constructed the proof. Instead I first found a proof, then laid it out in a manner which can be followed by the proverbial *intelligent reader*.

**Slide 16**

**Using Implications: Modus Ponens**

Modus Ponens:

From

- $P$ implies $Q$

- and $P$

We can conclude

$Q$ is true

Should be called Implication Elimination - **ImpElim**
but Greeks got there first

**Using Implications:** Implicative propositions are very useful, particularly if somebody has already shown them to be true. The general schema for using them, known for at least 2,500 years, is given in Slide 16. One way to establish a proposition, say $Q$, is to find an implication of the form

$$P \text{ implies } Q$$

which is already known to be true, and then prove the premise $P$. In other words a proof of $P$ *implies* $Q$, together with a proof of $P$ is sufficient to establish $Q$. We use this all the time informally in every day discourse. In Slide 17 we see it's use in establishing a useful judgement, which underpins a very common form of informal argument; if we know C **implies** R, and we know R **implies** S, then we can conclude C **implies** S. In other words the judgement

C **implies** R, R **implies** S $\vdash$ C **implies** S

represents a valid form of logical reasoning. Moreover any instantiation of C, R and S with propositions will also represent a valid form of logical reasoning. An instance is given in Slide 18, which justifies an informal argument we first discussed in Slide 5.

## Negation

Negation is a nightmare; it has caused problems for logicians for hundreds of years, and even today they still argue about how it should be handled. For the moment let us take a minimalist approach, and use

**Slide 17**

## An example proof

$\boxed{\text{C } \textbf{implies} \text{ R},\ \text{R } \textbf{implies} \text{ S} \vdash \text{C } \textbf{implies} \text{ S}}$

1. C **implies** R — premise
2. R **implies** S — premise
3. Assume C
4. R — using **Modus Ponens** with 1, 3
5. S — using **Modus Ponens** with 2, 4
6. Therefore C **implies** S — by **ImpIntro** applied to 3 – 5

**Slide 18**

## A Valid Argument

If it is cloudy, then it is going to rain. If it is going to rain, then I should take my raincoat with me.
Therefore if it is cloudy, I should take my raincoat with me.

C: It is cloudy

R: it is going to rain

S: I should take my raincoat

$\boxed{\text{C } \textbf{implies} \text{ R},\ \text{R } \textbf{implies} \text{ S} \vdash \text{C } \textbf{implies} \text{ S}}$

Slide 19

## Handling Negation

How to establish the proposition **not** P:

1. Assume proposition P to be true
2. Derive a contradiction, say **false**
3. Conclude $\boxed{\textbf{not}\ \text{P is true}}$

Fancy rule: Negation Introduction, **NotIntro**

Using Contradictions:

If we have established a contradiction **false**, we can conclude *any* proposition.

Fancy rule: False Elimination, **falseElim**

rules which are not controversial. Negation is closely associated with *contradictions*. These are propositions which are obviously false, such as (*n is even* ***and*** *n is odd*). We will use the special symbol **false** to denote some arbitrary contradiction. The important point about contradictions is that if we have derived one then something terrible has gone wrong. Of course we should never really derive a contradiction; this will only occur in hypothetical sub-proofs, such as those used to establish implications P **implies** Q. But in such proofs if we have derived a contradiction, then we are able to extend this contradictory proof by being able to conclude *any* proposition; this rule is called **falseElim**; see Slide 19

So how do we establish the proposition **not** P? Intuitively **not** P is true, if whenever we assume P itself to be true we arrive at some contradiction. The formal rule in Slide 19 implements this intuition. To derive **not** P formally, we assume P to be true. If from this assumption we can use the other rules to derive **false**, then we can conclude **not** P to be true.

If we have established the negative proposition **not** P how can we make use of it in a proof? It turns out we can only use it indirectly, typically in hypothetical sub-proofs, to establish a contradiction. The rule **NotElim** in Slide 20 says: if in addition we have established the corresponding positive proposition P, then we know that there is a contradiction; so we can conclude **false**.

To see an application of these rules consider the judgement

$$\text{P}\ \textbf{implies}\ \text{Q},\ \ \textbf{not}\ \text{Q} \vdash \textbf{not}\ \text{P}$$

This is a form of argument known to the Greeks as *Modus Tollens*. We can justify this method of argument by giving a proof of it using our rules; see Slide 21 for the details. It is important to realise here that the lines 3 to 5 are actually a sub-proof, a hypothetical sub-proof, necessary for the application of **notElim** on line 6, which establishes the negative proposition **not** P.

# Disjunction

Let us now look at the final connective used in Propositional Logic. The rules associated with *disjunctions* such as P **or** Q correspond very much to the intuitive meaning of **or** in everyday language. The proposition P **or** Q is true if either of its components P, Q are true. Therefore there are two possible ways to establish

Slide 20

## Handling Negation: Elimination

How do we use proposition **not** P:

| |
|---|
| Only indirectly, to establish contradictions |

The rule **NotElim** :

If we have established

(a) P

(b) **not** P

Then we can conclude **false**

Slide 21

## An example: Modus Tollens

P **implies** Q, **not** Q $\vdash$ **not** P

A proof:

| | |
|---|---|
| 1. P **implies** Q | premise |
| 2. **not** Q | premise |
| 3. Suppose P is true | |
| 4. Then Q is true | **MP** to 1 |
| 5. Then **false** | **NotElim** to 2,4 |
| 6. Therefore **not** P | **NotIntro** to 3–5 |

P **or** Q; the first is to establish P, the second is to establish Q. In Slide 22 this principle is dignified with the name **OrIntro**.

**Slide 22**

### Establishing Disjunctive Propositions

Two ways to establish $P$ **or** $Q$:

| | |
|---|---|
| 1. Establish $P$ | 1. Establish $Q$ |
| 2. Conclude ($P$ **or** $Q$) | 2. Conclude ($P$ **or** $Q$) |

It is sufficient to establish *one* of $P$, $Q$

Fancy rule: Or Introduction, **OrIntro**

Having established a disjunctive proposition P **or** Q, or having it as a premise, or do we use it? The difficulty is that we know one of P, Q are true but we don't know which. So if we are going to establish a proposition R using the fact that P **or** Q is true we are going to have to do *two* separate proofs:

(1) establish R, assuming P to be true

(2) establish R, assuming Q to be true.

This is what the rule **OrElim** in Slide 23 says. This is actually a well-known proof principle, called reasoning by *Case Analysis*. Suppose you know one of a number of facts are true, but you don't know which one. To establish a consequence, you have to prove that it follows from each of the facts separately.

Let us see an example of the use of these rules for handling **or**. You might know form Boolean Algebra or Circuit Theory, that disjunctions distribute over conjunctions. What this means is that

$$\text{P } \textbf{and} \text{ (Q } \textbf{or} \text{ R)} \vdash \text{(P } \textbf{and} \text{ Q) } \textbf{or} \text{ (P } \textbf{and} \text{ R)}$$

is a valid argument; it can be established using our proof rules. An example proof is given in Slide 24. It first decomposes the premise to obtain the proposition P and the proposition (Q **or** R). In order to use the latter we need to do a Case Analysis. First we suppose Q is true; lines 4 to 6 establish that the required conclusion, (P **and** Q) **or** (P **and** R), follows from this assumption. Next we suppose R is true, and lines 7 to 9 establish that the conclusion also follows from this assumption. Since on line 3 we have the disjunct Q **or** R, Case Analysis, in other words the rule **OrElim**, enables us to actually conclude (P **and** Q) **or** (P **and** R), in line 10.

It is important to realise here that the proof given in Slide 24 is not really linear; it has a structure, containing two hypothetical sub-proofs. The first is in the lines 4 to 6, and the second in lines 7 to 10. If we were being more formal then we would emphasise this structure.

Slide 23

## Using Disjunctive propositions - or

Rules for Eliminating **or**: Case Analysis

To prove $R$ from $P$ **or** $Q$ :

| | |
|---|---|
| 1a. Assume $P$ | 1b. Assume $Q$ |
| 2a. Use assumption to prove $R$ | 2b. Use assumption to prove $R$ |
| 3. Conclude $R$ | |

Two separate cases:

Proof of $R$, assuming $P$ to be true

Proof of $R$, assuming $Q$ to be true

Fancy name: **OrElim**

Slide 24

## and distributes over or

| | | |
|---|---|---|
| 1. | P **and** (Q **or** R) | premise |
| 2. | P | **AndElim** to 1 |
| 3. | Q **or** R | **AndElim** to 1 |
| 4. | Assume Q | |
| 5. | P **and** Q | **AndIntro** to 2,4 |
| 6. | (P **and** Q) **or** (P **and** R) | **OrIntro** to 5 |
| 7. | Assume R | |
| 8. | P **and** R | **AndIntro** to 2,4 |
| 9. | (P **and** Q) **or** (P **and** R) | **OrIntro** to 8 |
| 10. | (P **and** Q) **or** (P **and** R) | **OrElim** to 3,4–6, 7–9 |

Slide 25

## A Valid Argument?

If the train arrives late and there are no taxis at the station then John is late for his meeting. John is not late for his meeting. The train did arrive late. *Therefore*, there were taxis at the station.

Propositions:

L: the train arrives late

T: there are taxis at the station

J: John arrives late for his meeting

Slide 26

## An extra rule required

(L **and not** T) **implies** J, **not** J, L $\vdash$ T

| | | |
|---|---|---|
| 1. | (L **and not** T) **implies** J | premise |
| 2. | **not** J | premise |
| 3. | L | premise |
| 4. | Assume **not** T | |
| 5. | L **and not** T | **AndIntro** to 3,4 |
| 6. | J | **MP** to 1,5 |
| 7. | **false** | **NotElim** to 2,6 |
| 8. | **not** ( **not** T) | **NotIntro** to 4–7 |
| 9. | Can we now conclude T ? | |

Slide 27

**Double Negation**

Introducing double negations:

P $\vdash$ **not** ( **not** P)

Can NOT be derived from our existing rules

Using double negations:

From **not** ( **not** P) we can conclude P

Fancy rule: Double negation Elimination, **NotnotElim**

## Proof by Contradiction

Consider the argument outlined in Slide 25. It seems reasonable. Since John did not arrive late for his meeting there must have been taxis at the station. But if we analyse the argument formally, by breaking it down into it's constituent propositions, it turns out that we cannot justify the argument using our rules. We need to establish

(L **and** **not** T) **implies** J, **not** J, L $\vdash$ T

where the propositions L, T, J are given in Slide 25. But the best we can do, outlined in Slide 26 is to establish **not** ( **not** T) from the premises; in other words that

it is **not** true that there were **no** taxis at the station.

Does this allow us to conclude that there were taxis at the station?

This is a very controversial point with logicians. In order for us to justify formally the conclusion that there were taxis we need to add a new rule for establishing arguments. This is given in Slide 27, and is called **NotnotElim**. It enables us to conclude P from **not** ( **not** P). With this extra rule we can obviously finish the proof in Slide 26, and thereby justify the informal argument in Slide 25.

But many logicians object to the use of this rule. The main reason being that its use can lead to some questionable results. For example it can be used to show that for any proposition P,

$\vdash$ P **or** **not** P

is derivable; to see how this is done consult [1]. In other words it is allowable, at any time in a proof to assume the proposition (P **or** **not** P) for any P. This somehow flies in the face of the intuitive idea that the only way to establish a disjunctive proposition (Q **or** R) is to either establish Q or to establish R.

Nevertheless the double negation rule is very useful. For example it justifies the well-known proof strategy, known to the Greeks as *Reductio ad Absurdum*; these days it is known as *Proof by contradiction*. A famous example, due to Euclid, is outlined in Slide 28. The proposition to be derived is:

There are an infinite number of primes

Slide 28

**Proof by contradiction**

1. Suppose there are only a finite number, say $p_1, \ldots p_n$.
2. Consider the number $(P+1)$ where $P = (p_1 \times p_2 \times \ldots \times p_n)$
3. It is not a prime as it is different from each $p_i$
4. So $(P+1)$ must be divisible by some $p_r$
5. So $(P+1) = (p_r \times S) + 1$ where $S = p_1 \times p_{r-1} \times p_{r+1} \times \ldots$
6. Contradiction in 4, 5
7. Therefore from 6, 1 must be false
8. Therefore there are an infinite number of primes.

The proof proceeds by assuming the contrary, namely *there are only a finite number of primes*, and from this deducing a contradiction. Since a contradiction can not hold the assumption is incorrect, and therefore there are an infinite number of primes. The contradiction achieved is coming up with a number $(P+1)$ which is both

- divisible by some $p_r$, in line 4
- not divisible by the same $p_r$, in line 5.

In conclusion, if we want to continue to use *proof by contradiction* we need to accept the double negation rule **NotnotElim**.

## Summing up

In this brief note we have introduced ten *propositional deduction rules*, ways of deriving new propositions from exisiting ones; for convenience they are collected together in Figure 2. We end with two remarks about these rules.

(a) How do we know the rules are sound?

All the rules look “reasonable”, but can we be sure that using them will never get us into trouble? By this I mean, for example, that could they ever be used to derive something which is blatantly false, starting from facts which we know are obviously true?

To understand this point consider the rule **Silly** described in Slide29; it is obviously suspicious, saying that if we have established the proposition (P **implies Q**) and we have established the proposition Q, then we can conclude the proposition P. We can justify our suspicions by demonstrating that if we allow **Silly** into our set of deductive rules then we will be able to proof propositions which are obviously false.

One such proposition is

*black is white*

**Slide 29**

## An unsound rule

A **Silly** rule:

From
- (P **implies** Q)
- Q
1. Conclude P

Using **Silly**:

We can derive contradictions:

If *the moon is in the sky* then *black is white*

*the moon is in the sky* - obviously true

*black is white* - obviously false

This is obviously false, but using **Silly** we can derive it, starting from a proposition which everybody takes to be obviously true, say

*the moon is in the sky*

For a derivation see Slide 30. What this means is that the rule **Silly** is *unsound*; it can be used to derive contradictions.

How do we know that the rules in Figure 2 do not suffer from the same problem? At this point we don't, but with further effort it can be shown that they are all indeed *sound*; using them will never give rise to contradictions. The interested reader should study Section 1.4 of [1].

(b) How do we know we have enough rules?

By this I mean is, will it ever necessary to come up with new rules, ones which are not in Figure 2, in order to carry our "reasonable" deductions? The answer is no; the rules in Figure 2 will always be sufficient to carry out any propositional deduction which is in some sense true. Again we do not have time to go into justifying this assertion, but again this point is discussed at length in Section 1.4 of [1].

# Formal versus informal proofs

Very formal proofs are very boring to read, and therefore many proofs in textbooks are written down relatively informally, in English. A good proof is not only well laid out, but also has adequate explanations. Not only does it engage the reader, but it is structured in such a way that the reader can themselves, if they so wish, call upon formal logical rules to justify each individual step. Good proofs maintain the correct balance between readability and conciseness, while at the same time giving sufficient hints to the reader about the formal logical rules underlying the reasoning used.

A proof of the set theoretic identity

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$$

**Slide 30**

## An unsound deduction

*the moon is in the sky* ⊢ *black is white*

| | |
|---|---|
| 1. *the moon is in the sky* | premise |
| 2. Assume *black is white* | |
| 3. *the moon is in the sky* | **falseElim** to 2 |
| 4. *black is white* **implies** *the moon is in the sky* | **ImpIntro** to 2,3 |
| 5. *black is white* | **Silly** to 4,1 |

**Slide 31**

## Formal versus Informal Proofs

In an informal proof:

- many steps are omitted

- co-operation of reader is required

- some (obvious) justifications omitted

Reader can construct formal proof if necessary

Informal proof contains sufficient material to construct formal proof.

A proof of $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

1. Let $x$ be an arbitrary element.
We must show $x \in A \cap (B \cup C)$ implies $x \in (A \cap B) \cup (A \cap C)$ (def of $\subseteq$)
2. Assume $x \in A \cap (B \cup C)$
3. Then $x \in A$ and $x \in B \cup C$ (def of $\cap$)
4. Then $x \in A$ and $x \in B$ or $x \in C$ (def of $\cup$)
5. Case Analysis on $x \in B$ or $x \in C$
5a. Case a: $x \in A$ and $x \in B$
6a. So $x \in A \cap B$ (def of $\cap$)
7a. Therefore $x \in (A \cap B) \cup (A \cap C)$ (def of $\cup$)
5b. Case b: $x \in A$ and $x \in C$
6b. So $x \in A \cap C$ (def of $\cap$)
7b. Therefore $x \in (A \cap B) \cup (A \cap C)$ (def of $\cup$)
8. Therefore, in all cases, $x \in (A \cap B) \cup (A \cap C)$
9. Therefore $x \in A \cap (B \cup C) \in$ implies $x \in (A \cap B) \cup (A \cap C)$.
10. Therefore for every element $x$, $x \in A \cap (B \cup C) \in$ implies $x \in (A \cap B) \cup (A \cap C)$.
11. Therefore $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ (def of $\subseteq$)

Figure 1: A formal proof

is given in Figure 1, where each line is numbered for reference. The proof requires knowledge of the set theoretic operators $\cap$ and $\cup$ and their definitions are used to justify a large number of the steps. But some steps also have their basis in the formal rules of logic. In other words they are an informal application of certain formal rules. Examples are given in Slide 32. The important point is that in a proof each step must be justified, and in principle be backed up by some formal rule. The example proof is precise but perhaps too boring. It would be better to use more English phrases, so that it reads more easily. But in these more reader-friendly proofs it should still always be clear to the reader the formal basis for each step.

There are many more ways to logically structure propositions which can be found in standard logic books. We look at one final one, which students often find confusing, *logical equivalence*. Examples are given in Slide 33. This is simply notation which makes it easier to write down two related but independent implication propositions. So such propositions require two proofs, one for each implication. You will see, in some books, attempts to present these two proofs in one go but this just leads to confusion. When confronted with a *logical equivalence* to prove **always** give the two independent proofs.

## Finding versus Writing proofs

So far we have discussed how proofs are to be written; how they are to be laid out in such a way that a reader is convinced of your argument. An all together different activity is to find the proof in the first place. In general this is a *creative* activity in that there are no general rules which can be applied which will always succeed in finding the proof you require. Mathematicians often spend years of their life searching for a proof!

Nevertheless there is a general strategy which, when followed, will help structure your search for a proof. This is called *Goal-Oriented Reasoning*; the idea is outlined in Slide 35.

- First you have to lay out the proposition which needs to be proved as a goal, *which you can understand*. You are never going to verify a proposition about differential equations if you do not know anything about differential equations.

Slide 32

## Proof of $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

Each line

- boring but has clear justification

- can (if necessary) be justified *formally*

Hidden formal rules:

**Generalisation**: Lines 1,10 (from predicate logic)

**ImpIntro**: Lines 1,2,9

**OrElim** (Case Analysis): Lines 5,8

Slide 33

## Very Confusing: iff

Examples:

The sun is up *if and only if* it is day time

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

$P \vee (Q \wedge P)$ *logically equivalent* to $P$

These are **abbreviations** for two independent propositions, which need two independent proofs.

**Slide 34**

## Proving *iff* Propositions

There are **NO** shortcuts

To prove $P$ *if and only if* $Q$:

1. Prove implication: $P$ implies $Q$
2. Prove implication: $Q$ implies $P$

To prove $(A \cup B) \cap A = A$:

1. Prove $x \in (A \cup B) \cap A$ implies $x \in A$
2. Prove $x \in A$ implies $x \in (A \cup B) \cap A$

**Slide 35**

## Goal-Oriented Reasoning

- Set up a Goal
  assumptions
- Understand both
- Ransack assumptions for relevant information
- Reduce Goal to simpler subGoals
- Arrive at Trivial Goals
- Write up proof using Deductive Reasoning Rules

- Then you must be clear about the assumptions under which you are working. Again these you must be able to understand.

- Now you must bridge the gap between the assumptions and the goal.
How ?

- By searching, analysing, de-constructing both the goals and the assumptions until some relevant information emerges. This information should at least help you to break the current goal down into simpler subgoals, or at least subgoals which look like they might be easier to prove.

- Now there are new subgoals which require to be established. At this stage you may also have inherited further assumptions. Use the same method of decomposition until you arrive at goals, which are true for general reasons, or which are immediately implied by the assumptions.

- The last step is to write up the proof you think you have as a precise sequence of propositions, each of which follows logically from some previous ones. That is write up the proof using the rules of deductive reasoning.

This strategy is best learned by example and practice. The course Worksheets will provide material to work on.

## References

[1] Huth, M., and Ryan, M. *Logic in Computer Science*. Cambridge University Press, 2004.

[2] Garnier, R., and Taylor, J. *100% Proof*. Wiley, 1996.

Conjunction Introduction **AndIntro**:

| |
|---|
| 1. Establish P |
| 2. Establish Q |
| 3. Conclude (P **and** Q) |

Conjunction Elimination **AndElim**:

| | |
|---|---|
| From (P **and** Q) | From (P **and** Q) |
| 1. Conclude P | 1. Conclude Q |

Disjunction Introduction **OrIntro**:

| | |
|---|---|
| 1. Establish P | 1. Establish Q |
| 2. Conclude (P **or** Q) | 2. Conclude (P **or** Q) |

Disjunction Elimination **OrElim**:

| | |
|---|---|
| From (P **or** Q) | |
| 1a. Assume P | 1b.Assume Q |
| 2a. Derive R | 2b. Derive R |
| 3. Conclude R | |

Implication Introduction **ImpIntro**:

| |
|---|
| 1. Assume P |
| 2. Derive Q |
| 3. Conclude P **implies** Q |

Implication Elimination **Modus Ponens**:

| |
|---|
| From (P **implies** Q) |
| P |
| 1. Conclude Q |

Negation Introduction **NotIntro**:

| |
|---|
| 1. Assume P |
| 2. Derive contradiction |
| 3. Conclude **not** P |

Negation Elimination **NotElim**:

| |
|---|
| From **not** P |
| P |
| 1. Conclude **false** |

Double Negation **NotnotElim**:

| |
|---|
| From **not** ( **not** P) |
| 1. Conclude P |

False Elimination **falseElim**:

| |
|---|
| From **false** |
| 1. Conclude *any* proposition |

Figure 2: Formal Rules of Natural Deduction