Proof and Logic

Robert Brignall

April 27, 2006

1 Introduction

The first question we want to answer is "what is a proof?". We can define it formally as follows.

Definition 1.1. A *proof* is a logical argument that establishes a conclusion.

However, this doesn't really help us to work out what can form a proof, unless we know what constitutes a "logical argument". We introduce logical statements:

Definition 1.2. A *logical statement* is an expression saying things like "*if* A *then* B", where A is known as the *hypothesis*, and B is known as the *conclusion*. We sometimes say "A implies B", and we can write "$A \Rightarrow B$".

A statement is either going to be true or false. Here are some examples of true statements:

- If I am not inside a building, then I am outside.
- If it is raining and I am outside, then I will get wet.
- If x is even, then x is divisible by 2.

And here are some which are false:

- If it is not raining, then the sun is shining [*it could be cloudy...*].
- If x is not a prime number, then x is a square number [$x = 6$ *is neither prime nor square*].

The false statements above are clearly not true, and we can demonstrate that they are false by giving a *counter-example* to the statement. In the second statement above, the counter-example is when $x = 6$, and so we only need one counter-example to *disprove* a statement.

A proof is therefore a sequence of logical statements (all of which we know to be true), which can be used to establish the conclusion of another logical statement. So, for a silly example:

Theorem 1.3. *If it is raining and I am not inside a building, then I am going to get wet.*

Proof. I am not inside a building $\Rightarrow$ I am outside.
I am outside and it is raining $\Rightarrow$ I am going to get wet. □

1.1 Contrapositive Logic

Definition 1.4. We form the *contrapositive* statement by negating both the hypothesis and conclusion, and then by interchanging the resulting negations. So "if A then B" becomes "if B is not true, then A is not true".

Here are some of the examples from the previous section:

- If I am not outside, then I am inside a building.
- If I am not wet, then either I am inside a building or it is not raining. [*Note how we negate "A and B" to "not A OR not B".*]
- If x is not divisible by 2, then x is odd.

Note that the contrapositive statement has the same truth value as the original statement, so the above examples are all true.

Warning: Simple negation is not necessarily true. If $A \Rightarrow B$, then it is *not*, in general, true that if A is not true then B is not true. For example, the statement "maths is fun" (which is true) cannot be negated to "everything that isn't maths is not fun" — we don't know whether this is true or false.

1.2 Bi-directional statements and equivalence

Sometimes we have a statement which has a *2-way implication.* This is a statement like "*A if and only if B*", and is really two statements:

- If A then B [*The "only if" part.*]
- If B then A [*The "if" part – this is NOT the contrapositive!*]

If both statements are true, then we say that A and B are *equivalent.* We can write "$A \Leftrightarrow B$", or sometimes even "A iff B".

For example, we know that if x is even then x is divisble by 2, but also if x is divisble by 2, then x is even, and so

$$x \text{ even} \iff x \text{ divisible by } 2.$$

Note that if we are trying to prove two properties, A and B, are equivalent, then we will need to prove it in *both* directions.

1.3 Examples of proofs and non-proofs

In this section we will look at two "proofs": one of which is correct, and one of which is wrong. You may find it difficult to find all the separate "statements" in the proof.

Proposition 1.5. *If n is a positive integer, then $n^3 - n$ is a multiple of 3.*

Proof. Write $n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$. Now $n-1, n, n+1$ are three consecutive numbers, and so one of them must be a multiple of 3. Thus $n^3 - n$ is divisble by 3. □

Proposition 1.6. *For any positive integer n, if n^2 is even then n is even.*

Proof. Take n to be even, so $n = 2k$. Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, and so n^2 is even. □

But this proof is rubbish — we haven't "proved" the proposition at all! We have proved "n even $\Rightarrow n^2$ even". Instead, let us use the contrapositive to give a correct proof:

Proof. We show that the contrapositive statement "if n is odd then n^2 is odd" is true.
Take n to be odd, so $n = 2k+1$. Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd. □

2 Methods of Proof

2.1 Proof by Contradiction

Proof by contradiction relies on the fact that the contrapositive of a statement has the same truth value as the original statement. Suppose we want to prove the statement "A implies B". Proof by contradiction will go as follows:

- Suppose A.
- Suppose B is false.
- Since B is false, use logical statements to establish that A is false.
- We assumed A was true, so it cannot be false, and this is a *contradiction.*

So for example:

Proposition 2.1. *If n^2 is a multiple of 3, then n is a multiple of 3.*

Proof. Suppose n^2 is a multiple of 3, but n is not. Therefore $n = 3k + 1$ or $n = 3k + 2$.

If $n = 3k + 1$, then $n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$, which is not divisible by 3, a contradiction.

If $n = 3k+2$, then $n^2 = (3k+2)^2 = 9k^2+12k+4 = 3(3k^2+4k+1)+1$, which is not divisible by 3, a contradiction. □

Notice that in this example, we get two "cases": $n = 2k+1$ or $n = 2k+2$, and we must get a contradiction for BOTH cases.

What is wrong with the following proof?

Proposition 2.2. *Every positive real number is greater than or equal to 1.*

Proof. Let x be the smallest possible positive real number. We want to show that $x = 1$. Suppose, for a contradiction, that x is not 1:

1. If $x < 1$ then $x^2 < x$, and so x was not the smallest possible real number, a contradiction.

2. If $x > 1$ then $\sqrt{x} < x$, again a contradiction.

Therefore $x = 1$. □

The proposition is clearly not true. The error is in the first line: there is no smallest positive real number.

2.2 Proof by Induction

Proof by induction is a very powerful tool that we can use to prove statements about the integers. Suppose we have a statement $P(n)$, that has a truth value for each positive integer n, for example:

- $P(n) =$ "n is a prime number". Then $P(2) = P(3) = P(5) =$ true, but $P(4)$ is false.

- $P(n) =$ "$n \geq 1$". Then $P(n)$ is true for every $n \in \mathbb{N}$.

Then we can use induction to prove a proposition like "$P(n)$ is true for every $n > N$" (where we specify N). We then can prove this by proving two different statements:

(i) $P(N)$ is true. [This is known as the *base case*.]

(ii) $P(n) \Rightarrow P(n + 1)$ for any $n \geq N$. [We "assume" $P(n)$, and deduce $P(n + 1)$: this is called the *inductive hypothesis*.]

Here is a first simple example:

Proposition 2.3. *$n^2 \geq 1$ for all $n \geq 1$.*

Proof. Here, $P(n)$ says "$n^2 \geq 1$". We prove $P(n)$ is true in two steps:

- The base case is $P(1)$ = "$1^2 \geq 1$", which is obviously true.
- We now assume, for $n \geq 1$, that $P(n)$ is true, so $n^2 \geq 1$. Now look at $P(n+1)$: it says "$(n+1)^2 \geq 1$". But $(n+1)^2 = n^2 + 2n + 1$, and then *by the inductive hypothesis* we know $n^2 + 2n + 1 \geq 1 + 2n + 1$, so $(n+1)^2 \geq 2 + 2n \geq 1$, and hence $P(n+1)$ is true.

□

How does it work? In the above example, we know $P(1)$ is true. Now $P(1) \Rightarrow P(2)$, so $P(2)$ is true. Then $P(2) \Rightarrow P(3)$ so $P(3)$ is true, and so on.

Here's a more complicated example:

Proposition 2.4. *For every integer $n \geq 1$, $3^{2n} - 2^n$ is divisible by 7.*

Proof. $P(n)$ is the statement "$7 \mid 3^{2n} - 2^n$". The base case is $P(1)$, and $3^2 - 2^1 = 9 - 2 = 7$ which is clearly divisible by 7.

Now assume $P(n)$ is true, so for some integer n, there exists an integer a so that

$$3^{2n} - 2^n = 7a.$$

We now look at $P(n+1)$:

$$\begin{aligned} 3^{2(n+1)} - 2^{n+1} &= 9 \cdot 3^{2n} - 2 \cdot 2^n - 9 \cdot 2^n + 9 \cdot 2^n \\ &= 9(3^{2n} - 2^n) + 9 \cdot 2^n - 2 \cdot 2^n \\ &= 9 \cdot 7a + 7 \cdot 2^n = 7(9a + 2^n) \end{aligned}$$

and so $P(n+1)$ is true. □

One final example of induction:

Proposition 2.5. *Let $x > -1$. Then for every integer $n \geq 1$, $(1+x)^n \geq 1 + nx$.*

Proof. This is done by induction on n [do not be misled by the existence of x]. The base case, $n = 1$ is clear:$(1+x)^1 = 1 + x = 1 + 1 \cdot x$.

So now assume the statement is true for some $n \geq 1$, and look at $n+1$:

$$\begin{aligned} (1+x)^{n+1} &= (1+x)^n(1+x) \\ &\geq (1+nx)(1+x) \text{ by the inductive hypothesis} \\ &= 1 + nx + x + nx^2 \\ &\geq 1 + nx + x \text{ since } nx^2 \geq 0 \\ &= 1 + (n+1)x \end{aligned}$$

and hence the statement is true for $n+1$. □