Proof by Induction

§**1. The most common version.** This supplement gives a brief description of a very useful and long established method of proof. In addition, you can find many discussions of the method on the web (but beware that some go into very exotic versions which we do not need for this course).

We often want to prove a statement about the natural numbers, examples include:

(1) $n < 2^n$ for all $n \geq 0$.

(2) $0 + 1 + \cdots + n = n(n+1)/2$ for all $n \geq 0$.

(3) If the function $f : \mathbb{N} \to \mathbb{N}$ is defined by

$$f(n) = \begin{cases} 0 & \text{for } n = 0; \\ 2f(n-1) + 1 & \text{for } n > 0, \end{cases}$$

then $f(n) = 2^n - 1$ for all $n \geq 0$.

In each case we have a statement that is parametrised by a natural number n and we often use a notation such as $P(n)$ to stand for the statement being made (this is just a matter of convenience so we don't have to write the whole thing out every time). Claiming that such a statement $P(n)$ is true is claiming that infinitely many things are true:

- $P(0)$ is true and
- $P(1)$ is true and
- $P(2)$ is true and . . .

Sometimes we make our claim for all natural numbers starting from some number n_0 onwards rather than 0. Wherever we start our claim, we call it the *base case*.

How can we prove our claim (assuming it is indeed true)? Clearly it is no good checking that $P(0)$ holds, then that $P(1)$ holds etc. Of course if any of these fail to hold then the claim is false (and typically we do a few checks) but if it is indeed true then we have infinitely many cases to check!

The task becomes possible by means of a simple and very powerful idea.

(1) Show that the base is true.

(2) Show that if the claim holds for n (where n is *not* fixed, it stands for any number whatever that is at least as large as the base case) then it necessarily holds for $n + 1$.

These can be summarised as: (i) show that $P(0)$ holds (or $P(n_0)$ if we are not starting at 0) and (ii) show that $P(n) \Rightarrow P(n+1)$. The first task is referred to the *base case* and the second as *the induction step*. Note that in the induction step we assume that $P(n)$ holds and prove that under this assumption $P(n+1)$ must also hold. The assumption referred to is called the *induction hypothesis*.

Establishing the induction step gives us the following guarantee. Let m be a fixed natural number that is at least as large as the base case. The induction step now tells us: "if you can prove (by whatever means) that the claim is true for $n = m$ then I guarantee that it is also true for $n = m + 1$." So buy one get one free; in fact we get *much* more. Let's assume we have established both the base case and the induction step. Then we have the following sequence of facts:

- The claim holds for $n = 0$, this is the base case that we proved.
- Since the claim holds for $n = 0$ the induction step now shows us that the claim is also true for $n = 1$ (take $n = 0$ in the induction step proof).
- Since the claim holds for $n = 1$ the induction step now shows us that the claim is also true for $n = 2$ (take $n = 1$ in the induction step proof).
- Since the claim holds for $n = 2$ the induction step now shows us that the claim is also true for $n = 3$ (take $n = 2$ in the induction step proof).
- . . .

In other words the claim holds for *all* natural numbers (from the base case onwards).

Let us now return to the three examples above and see induction at work.

(1) $n < 2^n$ for all $n \geq 0$ (this claim is what we referred to above as $P(n)$).

Our base case is $n = 0$ and so we must check that $0 < 2^0 = 1$ which is clearly true. Now for the induction step: we must show that if the claim holds for n then it also holds for $n + 1$. So suppose $n < 2^n$; this is the induction hypothesis. We must show that from this assumption it follows that $n + 1 < 2^{n+1}$; this is the induction step. Now if $n = 0$ then we must prove that $1 < 2$ which is clearly true (we don't need the induction hypothesis for this special case). If $n > 1$ then we have $n + 1 \leq 2n$ (just subtract n form both sides). By the induction hypothesis we have that $n < 2^n$ and so $2n < 2 \cdot 2^n = 2^{n+1}$ and we have established that $n < 2^{n+1}$.

We did this example in the lectures but with the base case $n = 1$, i.e., we left out the claim for $n = 0$ (because we were applying it to deduce the inequality $\lg(n) < n$ and $\lg(0)$ is not defined).

(2) $0 + 1 + \cdots + n = n(n+1)/2$ for all $n \geq 0$.

For the base case we must check that $0 = 0(0+1)/2$ which is clearly true. so suppose the claim is true for n, we must show that it is then necessarily true for $n+1$. Now

$$\begin{aligned} 0+1+\cdots+n+(n+1) &= (0+1+\cdots+n)+(n+1) \\ &= n(n+1)/2+(n+1), \quad \text{by the induction hypothesis} \\ &= (n+1)(n/2+1) \\ &= (n+1)(n+2)/2. \end{aligned}$$

So if the summation formula holds for n then it also holds for $n+1$, which completes the proof of the induction step.

(3) If the function $f : \mathbb{N} \to \mathbb{N}$ is defined by

$$f(n) = \begin{cases} 0 & \text{for } n = 0; \\ 2f(n-1)+1 & \text{for } n > 0, \end{cases}$$

then $f(n) = 2^n - 1$ for all $n \geq 0$.

Here the base case is $f(0) = 2^0 - 1 = 1 - 1 = 0$ which is true from the definition of f. For the induction step we assume that $f(n) = 2^n - 1$ and show that then $f(n+1) = 2^{n+1} - 1$. From the definition of f we have $f(n+1) = 2f(n)+1$. By the induction hypothesis, $f(n) = 2^n - 1$ and so we have

$$\begin{aligned} f(n+1) &= 2f(n)+1 \\ &= 2(2^n-1)+1 \\ &= (2^{n+1}-2)+1 \\ &= 2^{n+1}-1. \end{aligned}$$

This completes the proof of the induction step.

Warning: The base case is usually easy to prove (often amounting to a simple check). Sometimes people new to induction overlook it altogether and focus on the more difficult induction step. However unless the base case does indeed hold then we cannot deduce anything about the truth of the claim. This should be clear from the discussion above. It is perfectly possible for the induction step to be true (i.e., as a logical implication $P(n) \Rightarrow P(n+1)$) even though the base is false and the claim is in fact false for all natural numbers. As an example consider the function f defined above and suppose we make the (false) claim that $f(n) = 2^{n+1} - 1$. The induction step assumes the claim for n and then for $n+1$ we have $f(n+1) = 2f(n)+1 = 2(2^{n+1}-1)+1 = 2^{n+2}-1$ which is the formula for $n+1$. Of course there is no foundation form which to deduce any actual fact about the values of $f(n)$, all we have established is that *if* $f(n) = 2^{n+1} - 1$ *then* $f(n+1) = 2^{n+2} - 1$ but the premise is just false!

A different pitfall is to establish the base case but make a subtle error in the induction step, such as using the induction hypothesis for a case to which it does not apply. For the uses of induction in this course you are unlikely to come across such pitfalls but be aware of them, the moral is that it is necessary to be careful about justifying the various steps.

§**2. Variants.** Sometimes we need to use more than one base case. In this situation we check all the base cases before going on to the induction step. In other

situations, in establishing the induction step we need to use the assumption that the claim not only holds for n but for some (or possibly all) values up to n. This happens if, e.g., the truth of $P(n+1)$ depends not only on that of $P(n)$ but on $P(n-1)$ as well. This version is called *strong induction* but a little thought should convince you that it is really the same idea as that discussed above.

Finally sometimes our claim is not made for all natural numbers but for some infinite sequence, say $n_0, n_1, n_2, \ldots$, which we will call the relevant values (to the claim). We can, if we like, say that $P(0)$ is the claim for n_0, $P(1)$ is the claim for n_1 etc. In fact we can circumvent this by an induction step of the form: suppose the claim is true for some relevant value n then it is necessarily true for the next relevant value. The “strong” version assumes the claim is true for all relevant values up to n then it is shown to be necessarily true for the next relevant value.