Main Steps

There are five main steps for an induction proof.

Step 1: State what you're trying to prove. State what you are trying to prove, which should depend somehow on the size n of whatever you're trying to analyze.

Step 2: State the variable you'll be inducting on. What will be the variable that increases in the inductive step? This tells the reader what to expect.

Step 3: State your base case. State for which n your base case is true, and prove it. Typically, this will be the smallest n for which you are trying to prove your claim for, but occasionally you'll need more than one base case.

Step 4: State your inductive hypothesis. State your inductive hypothesis. Here you are usually just hypothetically asserting the property you're trying to prove for some fixed $k \geq \langle$base case$\rangle$.

Step 5: Prove the inductive step. Now consider $n = k + 1$. Here is where you actually do the proof that your claim for this new value of n is true, and thus this is where the creativity comes in. This proof is going to be different for each induction proof; sometimes it will use algebra, number theory, common sense, etc. It will *always* need to use the inductive hypothesis, and you should *clearly label* when and where you use this assumption. If you haven't used your inductive hypothesis, then you aren't doing a proof by induction (and you should be worried!)

(Optional Step 6: Conclusion.) Summarize the steps above. Best when the proof is long.

Comments

- Sometimes, there will be many candidates for the variable n. For example, in a graph problem, n could be the number of vertices, the number of edges, the number of connected components, or some other crazy thing. In these cases, Step 2 is especially important.

- Check that the claim you want to prove mentions n in it somewhere.

- Be careful with the base case—sometimes you will need more than one, as with some recurrence relations.

- You must use your inductive hypothesis somewhere in the proof of the inductive step, otherwise you are not doing a proof by induction. Check to be sure.

- If you're stuck in your inductive step, take a step back for a moment. What are you trying to prove? Keep this in mind when you work on proving your claim for $n = k + 1$. Since you have to use your inductive hypothesis somewhere, you may want to think about how you can manipulate what you've got into something that resembles your inductive hypothesis. Also, you may want to check any algebra you've done as that can often be the source of problems!

- When trying to prove some equation holds, that is, if you are trying to prove that

$$\text{left-hand-side} = \text{right-hand-side}$$

for some left-hand-side and right-hand-side, please do not start with assuming they are equal and then modifying both sides of the equations until you get an equation that is actually true. For example:

$$
\begin{aligned}
\text{left-hand-side} &= \text{right-hand-side} \\
0 \times \text{left-hand-side} &= 0 \times \text{right-hand-side} \\
0 &= 0 \ .
\end{aligned}
$$

Therefore they are equal.

Obviously I can 'prove' that left-hand-side $=$ right-hand-side using this method for any left-hand-side and right-hand-side, regardless of whether or not they are actually equal! What is better is to start with left-hand-side, make modifications to left-hand-side through a string of equalities that somehow ends with right-hand-side. That is,

$$\text{left-hand-side} = \cdots$$
$$= \cdots$$
$$= \text{right-hand-side}.$$

This will guarantee that you don't prove something that isn't true.

- Recall the difference between strong and weak induction. They're equivalent, but sometimes using one is easier than using the other.

Example 1: Sum of Squares

Suppose we are trying to come up with a formula for the sum of the first n squares, for $n \geq 0$. We may try a few numbers out to see if we can find a pattern:

$$0^2 = 0 \qquad\qquad\qquad 0^2 + 1^2 + 2^2 = 5$$
$$0^2 + 1^2 = 1 \qquad\qquad\qquad 0^2 + 1^2 + 2^2 + 3^2 = 14$$

It looks like the sum of the first n squares may be $n(n+1)(2n+1)/6$. It certainly works for the few examples above, but I'd like to prove that the formula works for *every single* $n \geq 0$, that is, I want to prove an infinite number of equalities. Let's see how to do this with induction:

Step 1. We seek to show that for any $n \geq 0$, $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$...

Step 2. We will argue by induction on n.

Step 3. As a base case, consider when $n = 0$. We need to show that
$0^2 + \cdots + 0^2 = 0(0+1)(2 \cdot 0 + 1)/6$. Fortunately,

$$\text{left-hand side} = 0^2 + \cdots + 0^2 = 0 = 0(0+1)(0+1)/6 = \text{right-hand side}.$$

Step 4. For the inductive hypothesis, suppose (hypothetically) that our claim held for some fixed $k \geq 0$. That is, suppose that

$$0^2 + 1^2 + 2^2 + \cdots + (k-1)^2 + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Step 5. Now we prove that the claim hold for $n = k + 1$, using the (hypothetical) induction assumption that it holds for $n = k$. That is, we prove that

$$0^2 + 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2(k+1)+1)}{6}.$$

The proof that that the claim holds for $n = k + 1$ is as follows:

$$
\begin{aligned}
\text{left-hand side} &= 0^2 + 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 \\
&= (0^2 + 1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{by the inductive hypothesis } P(k) \\
&= \frac{(k+1)(2k^2 + 7k + 6)}{6} && \text{by algebra} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} && \text{by algebra} \\
&= \text{right-hand side.}
\end{aligned}
$$

Therefore we have shown that *if* the claim holds for $n = k$, then it holds for $n = k + 1$ as well, for any $k \geq 0$.

Example 2: Towers of Hanoi

There are n disks of different diameters stacked from largest to smallest on a start tower. The goal is to move all disks to an end tower, such that they are stacked in same order. You have one extra tower, and you are restricted to moving one disk at a time, such that you never place a larger disk on top of a smaller disk. We propose the following algorithm:

```
tower( n disks, start tower, end tower, extra tower)
    if n == 0, do nothing and return.
    recursively move top n-1 disks from start to extra, using end as third tower
        (that is, call tower(n-1, start tower, extra tower, end tower) )
    move the nth disk from the start tower to the end tower
    recursively move the n-1 disks on extra to end, using start as third tower
        (that is, call tower(n-1, extra tower, end tower, start tower) )
```

Step 1. For any $n \geq 0$, we will prove that the algorithm moves n disks from the start tower to the end tower one disk at a time, such that larger disks are never on smaller disks, in $2^n - 1$ steps.

Step 2. We will argue by induction on the number of disks, n.

Step 3. As a base case, consider when $n = 0$. We will show that the algorithm moves 0 disks in $2^0 - 1 = 0$ moves, following the rules. And this is what it does.

Step 4. For the inductive hypothesis, suppose that the algorithm moves k disks from the start tower to the end tower, following the rules, in $2^k - 1$ steps.

Step 5. Now we prove that the algorithm moves $k+1$ disks from the start tower to the end tower, following the rules, in $2^{k+1} - 1$ steps.

The proof is as follows: We have to prove that the algorithm uses $2^{k+1} - 1$ steps, and that each of these steps is "valid". For the steps:

$$\begin{aligned}
\text{left-hand side} &= \text{\# steps to move } k+1 \text{ disks} \\
&= 2(\text{\# steps to move } k \text{ disks}) + 1 \qquad \text{by the algorithm definition} \\
&= 2(2^k - 1) + 1 \qquad\qquad\qquad\qquad\qquad \text{by the IH} \\
&= 2^{k+1} - 1 \qquad = \text{right-hand side}
\end{aligned}$$

As for the validity of the steps, the algorithm on $k+1$ towers leaves the largest disk on the bottom of the start tower, then makes a recursive call on the smallest k disks. All of these moves are (by the IH) valid, and never move the largest disk. We then make one valid move, of this largest disk from the start tower to an empty tower, then again recursively move the smallest k disks (valid, by the IH).

Step 6. The steps above have shown that for any $k \geq 0$, if if the algorithm moves k disks from the start tower to the end tower while following the rules, it also does so for $k+1$ disks. Combined with the base case, this proves the claim for any $n \geq 0$.