1.7. Mathematical Induction

Terence Sim

Proofs are to mathematics what spelling is to poetry.

Mathematical works do consist of proofs, just as poems do consist of words.

Vladimir Arnold, 1937 — 2010

Reading

Section 5.2 — 5.4 of Epp.
Section 2.8 — 2.10 of Campbell.

Suppose I wish to convince you that I can climb a ladder of n steps, no matter how large n is.

My strategy is to use two rules:

Rule 1: I can "climb" to Step 0 (the base of the ladder).

Rule 2: If I am on Step k, I know how to climb to Step $k+1$.

http://geneburnett.blogspot.sg/2012/06/ladder-of-progress.html

If you give me a ladder of 3 steps,

- First, I use Rule 1 to "climb" to Step 0.
- Then, let $k = 0$, and I use Rule 2 to climb to Step 1.
- Then, let $k = 1$, and I use Rule 2 to climb to Step 2.
- Then, let $k = 2$, and I use Rule 2 to climb to Step 3.

It should be clear how I can use these two Rules to climb a ladder of n steps, for any n, no matter how large. I simply use Rule 1 once, then Rule 2 as many times as needed.

This is the essence of a proof technique called Mathematical Induction.

1.7.1. Regular Induction

The Principle of Mathematical Induction is an inference rule concerning a predicate $P(n)$:

$$
\begin{array}{ll}
P(0) & \longleftarrow \text{Base case} \\
\forall k \in \mathbb{N},\ P(k) \to P(k+1) & \longleftarrow \text{Inductive step} \\
\bullet\, \forall n \in \mathbb{N},\ \ P(n) & \longleftarrow \text{Conclusion}
\end{array}
$$

$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$ is the set of natural counting numbers.

In English: If we know that $P(0)$ is true, and also that $P(k)$ implies $P(k+1)$ for any k, then we can conclude that $P(n)$ is true for all $n \in \mathbb{N}$.

This gives us a structure to write an Induction Proof. You are strongly advised to follow this structure, because otherwise it is easy to introduce errors into your proof.

These are the steps:

1. Identify the predicate $P(n)$. A predicate is a statement that evaluates to true or false. Usually, $n \in \mathbb{N}$, but not always.
2. Prove the Base case, also called Basis step, $P(0)$. Note that there could be more than one Base case.
3. Prove the Inductive step, which is an implication statement involving universal quantification. The usual rules for proving such statements apply here, and should have the following steps:

   3.1 For any $k \in \mathbb{N}$:
   3.2 Assume $P(k)$ is true. [Called the Inductive hypothesis.]
   3.3 [Write out the predicate $P(k)$.]
   3.4 [Consider the problem of size $k + 1$. Break it down into a smaller problem of size k.]
   3.5 [Apply the Inductive hypothesis on the size-k problem.]
   3.6 [Proceed to show that $P(k + 1)$ is true.]

4. Write the Conclusion.

1.7.2. Example

Prove that $\forall n \in \mathbb{N}$, $(4^n - 1)$ is divisible by 3.

Proof: (by Mathematical Induction)

1. For all $n \in \mathbb{N}$, let $P(n) = (3 \mid (4^n - 1))$.
2. Base case: $n = 0$
3. Clearly, $(4^0 - 1) = 0 = 3 \cdot 0$.
4. Thus, $P(0)$ is true.

...

proof cont'd

5. Inductive step: For any $k \in \mathbb{N}$:
6. Assume $P(k)$ is true, ie. $3 \mid (4^k - 1)$.
7. Consider the $k+1$ case:
8. $4^{k+1} - 1 = 4 \cdot 4^k - 1 = 4(4^k - 1) + 3$, by basic algebra.
9. By the Inductive hypothesis, $3 \mid (4^k - 1)$.
10. Clearly, $3 \mid 3$.
11. So by Theorem 4.1.1, $3 \mid (4(4^k - 1) + 3)$.
12. Thus, $P(k+1)$ is true.
13. So by Mathematical Induction, the statement is true. ■

Remarks

- In Line 1, note that we need to qualify the domain of n, by saying "For all $n \in \mathbb{N}$". But this is outside the definition of $P(n)$.
- A common mistake is to define the predicate as $P(n) = 4^n - 1$. This is wrong because $4^n - 1$ is not a statement; it does not evaluate to **true** or **false**.

1.7.3. Non-zero base case

We may relax the requirement for the Base case to start from 0, to let it start from any $a \in \mathbb{Z}$.

The Induction rule becomes:

$$\begin{array}{l} P(a) \\ \forall \text{ integers } k \geq a,\ P(k) \rightarrow P(k+1) \\ \bullet\ \forall \text{ integers } n \geq a,\ P(n) \end{array}$$

Note that the conclusion says $P(n)$ is true for $n \geq a$, and is silent about $P(n)$ for $n < a$.

1.7.4. Negative example

http://assets.inhabitat.com/wp-content/blogs.dir/1/files/2012/03/brown-cows.jpg

Claim: All cows have the same color.

(Faulty) Proof by Mathematical Induction

1. Let $P(n) =$ (Any group of n cows have the same color), for any $n \in \mathbb{Z}^+$.
2. Clearly, a single cow has one color, so $P(1)$ is true.
3. Suppose $P(k)$ is true for any integer $k \geq 1$:
4. In any group of $k+1$ cows, number them from 1 to $k+1$.
5. Then cows $\#1$ to $\#k$ form a group of k, which have one color by the Inductive hypothesis.
6. Similarly, cows $\#2$ to $\#k+1$ have one color.
7. Now cows $\#2$ to $\#k$ are common to both groups, and cows don't change color because we assign them to different groups.
8. Thus cow $\#k+1$ has the same color as cow $\#1$, which means all $(k+1)$ cows have the same color.
9. Thus $P(k+1)$ is true. ■

What is wrong?

1.7.5. Strong Induction

- The difference between Strong Induction and Regular Induction lies only in the Inductive hypothesis. All other steps remain unchanged.
- In the Inductive hypothesis in Regular Induction, you assume $P(k)$ is true. In Strong Induction, you assume $P(k), P(k-1), P(k-2), \ldots, P(a)$ are *all* true.
- That is, you make a stronger assumption about the values of n which make $P(n)$ true, hence the name Strong Induction. From this stronger assumption, you proceed as before to show that $P(k+1)$ is true.
- It may be shown that Regular Induction implies Strong Induction and vice versa. That is, anything that can be proven using Regular Induction can be proven using Strong Induction, and vice versa. However, the benefit of using Strong Induction is the convenience of using more assumptions. The next example illustrates this.

1.7.6. Example

Prove: $\forall$ integers $n > 1$, n has a prime factorization.

Proof by Strong Induction

1. Let $P(n) = (n$ has a prime factorization$)$, for any integer $n > 1$.
2. Base case: $n = 2$
3. Since 2 is prime, $2 = 2$ is a trivial prime factorization.
4. Thus $P(2)$ is true.

...

proof cont'd

5. Inductive step: For any integer $k > 1$:
6. Assume $P(i)$ is true for $1 < i \leq k$. (Stronger assumption)
7. That is, all integers i in the range $1 < i \leq k$ have prime factorizations.
8. Consider the integer $k + 1$:
9. If $k + 1$ is prime:
10. Then $k + 1 = k + 1$ is a trivial prime factorization, and $P(k + 1)$ is true.

...

proof cont'd

11. Else $k + 1$ is composite:
12. Then $k + 1 = rs$, for some integers r, s such that $1 < r, s < k + 1$, by definition of composite.
13. Then both r and s have prime factorizations, by the Inductive hypothesis.
14. Let these be $r = p_1 p_2 \dots p_u$ and $s = q_1 q_2 \dots q_v$, where all the factors are prime.
15. Then $k + 1 = rs = p_1 p_2 \dots p_u q_1 q_2 \dots q_v$, by basic algebra.
16. Thus $k + 1$ has a prime factorization, and $P(k + 1)$ is true.
17. So by Strong Induction, the statement is true. ■

Remarks

Note that in Line 12, the definition of composite does not guarantee that $r = k$ or $s = k$.

Thus, the Inductive hypothesis in Regular Induction cannot apply here (because that hypothesis says only $P(k)$ is true, but r, s may not be equal to k).

However, Strong Induction overcomes this problem by making stronger assumptions about the truth set of $P(k)$. This allows the proof to proceed.

Finally, note that the proof only proves the existence of a prime factorization, not uniqueness. Try proving uniqueness yourself.