Mathematical Induction

Introduction

Mathematical induction, or just induction, is a proof technique. Suppose that for every natural number n, $P(n)$ is a statement. We wish to show that all statements $P(n)$ are true.

In a proof by induction, we show that $P(1)$ is true, and that whenever $P(n)$ is true for some n, $P(n+1)$ must also be true. In other words, we show that the conditional $P(n) \rightarrow P(n+1)$ is true for all n.

This creates a logical "chain reaction" – the truth of $P(1)$ implies the truth of $P(2)$, which implies the truth of $P(3)$, which implies the truth of $P(4)$, and so on.

On the next slide, we will restate this so-called principle of induction, prove it, and introduce some terminology.

The Principle of Induction

Theorem (Principle of Induction):
Suppose $P(n)$ is a statement for every natural number n. Further suppose that

1. The first statement, $P(1)$ is true.
2. For every n, the conditional $P(n) \rightarrow P(n+1)$ is true.

Then $P(n)$ is true for all n.

Proof: Suppose $P(n)$ is not true for all n. Then there must be at least one n for which it is false. Let n_0 be the smallest of all these n. Since we know that $P(1)$ is true, $n_0 \geq 2$. Since n_0 is the smallest n for which $P(n)$ is false, and $n_0 - 1$ is a natural number, $P(n_0 - 1)$ is true. By assumption, the conditional $P(n_0 - 1) \rightarrow P(n_0)$ is true as well, hence $P(n_0)$ is true. That is a contradiction because $P(n_0)$ is false.

This proves that $P(n)$ is true for all n.

In an inductive proof, verifying condition 1 is called the base case. Verifying condition 2 is called the induction step or inductive step. We verify condition 2 by assuming $P(n)$ (called the inductive hypothesis) for **some** n, and showing that then $P(n+1)$ is true as well.

The Renaming Ritual

Many textbooks, including Rosen, highlight the fact that the inductive hypothesis is made about some arbitrary n value by giving this *n* a new name such as *k*. In the inductive hypothesis, rather than assuming $P(n)$ “for some n”, they assume $P(n)$ “for some $n = k$" and then demonstrate that $P(k+1)$ must be true as well.

This renaming ritual is not necessary, and has the disadvantage that it may cause serious confusion when the statement about n already involves some variable named k. The slide titled “Common Mistakes (4)” illustrates this.

Example I

Let us prove by induction that for all natural numbers n,

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

This equation is the statement $P(n)$.

1. Base case: we verify $P(1) = \left(1 = \frac{1 \cdot 2}{2}\right)$. This is true.
2. Inductive step: let us assume $P(n)$ for **some** n, i.e.

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

We now add the next term of the summation, which in this case is just $n+1$, to both sides. On the left side, that "upgrades" the sum to the next higher upper limit. On the right, we hope that the right side of $P(n+1)$ emerges. (Note that generally, when you write an inductive proof of a summation formula, the next term is not always going to be $n+1$.)

$$\sum_{k=1}^{n+1} k = \frac{n(n+1)}{2} + n + 1 = \left(\frac{n}{2} + 1\right)(n+1) = \frac{(n+1)(n+2)}{2}$$

This statement,

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2},$$

is the statement $P(n+1)$. We just completed the inductive step: we showed that if $P(n)$ is true, then $P(n+1)$ is true as well. That completes the proof by induction.

Common Mistakes (1)

Students often confuse the statement P(n) with the algebraic expression about which a statement is being made.

In the previous example, we proved the statement

$$P(n) = \left(\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \right)$$

for all n. Notice the parentheses - $P(n)$ is not the sigma sum, and it's not the expression $\frac{n(n+1)}{2}$. It is the <u>statement</u> that these two quantities are equal.

Therefore, you must not write equations like $P(n) = \frac{n(n+1)}{2}$ in your inductive proofs. If you must have a notation for an expression that is frequently referred to, you are free to define your own notation for it, for example,

$$a_n = \frac{n(n+1)}{2}$$

but you must not use $P(n)$. You must also not write equations like this:

$$P(n) = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Without the critical parentheses, $P(n)$ is no longer the statement that the middle and right quantity are equal. It is the common value of that quantity. So on top of using wrong notation, you are assuming the conclusion of the proof with this.

Common Mistakes (2)

A second, somewhat common mistake is to confuse *stating* $P(n+1)$ with *proving* it. Merely stating it does not prove it.

The following variation of the inductive step of Example 1 illustrates that mistake:

"Let us assume that $P(n)$ is true for some n, i.e.

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Then $P(n+1)$ is the statement

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$$

This completes the proof by induction. "

The psychology of this mistake seems to be that merely writing $P(n+1)$ required some algebra work. You had to replace each n by n+1 and simplify, so it may feel like "you did something". You did, you just didn't prove $P(n+1)$.

Common Mistakes (3)

When $P(n)$ is a summation formula, people may confuse the *n* with the running variable in the summation.

We earlier proved that

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

is true for all *n.* Notice that both sides are functions of *n* alone: *n* is the ONLY free variable in this formula. You may think that you are seeing another free variable, *k*, on the left, but this hallucination is easily dispelled by remembering the meaning of the sigma notation: it means simply $1 + 2 + 3 + \cdots + n$. Our formula is

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

There is no "k" there. If you replace k by k+1, you simply break the sigma sum and turn it into something unrelated.

People who are unclear about the distinction between *k* and *n* may think that they need to increment k when they form $\sum_{k=1}^{n+1} k$, either instead of incrementing n, or in addition to it:

$$\sum_{k=1}^{n} (k+1\,) \text{ or } \sum_{k=1}^{n+1} (k+1)\,.$$

Neither is equal to $\sum_{k=1}^{n+1} k$.

From a programming perspective, you can think of the k inside the sigma notation as a local variable inside a function that is invisible from the outside:

```
function sum(int n)
  int sum = 0;
  for (int k=1;k<=n;k++)
     sum +=k;
```

Common Mistakes (4)

If you practice the "renaming ritual" of assuming in the inductive step that $P(n)$ is true "for some $n = k$ " rather than just "for some n", and if your $P(n)$ involves a sigma sum that uses k as a running variable, you're in danger of writing wholly nonsensical expressions like this:

$$\sum_{k=1}^{k} k$$

If you don't see what's wrong with that, consider the following equivalent code:

```
function sum(int k)
  int sum = 0;
  for (int k=1;k<=k;k++)
     sum +=k;
```

The best way to avoid this is to not rename the induction variable n and to assume that $P(n)$ is true for some *n* in the inductive step.

Common Mistakes (5)

What's wrong with the following inductive step?

"Inductive Step. Let us assume $P(n)$ for all n.."

In the inductive step, we prove that the conditional $P(n) \rightarrow P(n+1)$ is true for all n, i.e. we prove

$$\forall n\big(P(n) \rightarrow P(n+1)\big).$$

We do this by assuming that $P(n)$ is true for some (arbitrary) n, and then showing that $P(n+1)$ must then be true as well. By universal generalization, that shows $\forall n\big(P(n) \rightarrow P(n+1)\big)$.

In the proof fragment above, it is assumed that $P(n)$ is true for all n. That's assuming the conclusion. If we already know that $P(n)$ is true for all n, we don't need a proof.

Example II

Theorem: if S is a finite set with $|S| = n$, then $|\mathcal{P}(S)| = 2^n$, for $n = 0,1,2,3, \ldots$

Let us define $P(n) =$ (if S is a set with $|S| = n$, then $|\mathcal{P}(S)| = 2^n$). Since the smallest n for which $P(n)$ is defined is $n = 0$, the base case is to verify $P(0)$.

Proof by induction:

1. Base case: $P(0)$ is the statement (if S is a set with $|S| = 0$, then $|\mathcal{P}(S)| = 1$). This statement is true, because $|S| = 0$ implies that $S = \emptyset$, hence $\mathcal{P}(S) = \{\emptyset\}$, so $|\mathcal{P}(S)| = 1$.

2. Inductive step: suppose $P(n)$ is true for some n. We must verify the statement $P(n+1) =$ (if S is a set with $|S| = n + 1$, then $|\mathcal{P}(S)| = 2^{n+1}$). To verify this conditional, we will assume its premise and show that the conclusion must be true.

Let S be a set with $|S| = n + 1$. Let us single out an arbitrary element of S and call it x. Define $R = S - \{x\}$. Then $|R| = n$. Now let us count how many subsets S has. The number of subsets of S equals $A + B$, where

$A =$ the number of subsets of S that don't contain x,
$B =$ the number of subsets that do contain x.

A subset of S that doesn't contain x is a subset of R, hence $A = |\mathcal{P}(R)| = 2^n$ by the inductive hypothesis.

A subset of S that contains x is the union of a subset of R with $\{x\}$, hence $B = |\mathcal{P}(R)| = 2^n$. Therefore, $|\mathcal{P}(S)| = A + B = 2^n + 2^n = 2^{n+1}$. That completes our proof.

Example III

Theorem: 21 divides $4^{n+1} + 5^{2n-1}$ for all natural numbers n.
Proof by induction: we first verify the statement for $n = 1$: 21 divides $4^2 + 5^1 = 21$. This is true.
Now suppose that 21 divides $4^{n+1} + 5^{2n-1}$ for some natural number n. This means $4^{n+1} + 5^{2n-1} = 21k$ for some integer k. Let us consider

$$4^{n+2} + 5^{2(n+1)-1} = 4^{n+2} + 5^{2n+1}$$

By using laws of exponentiation, we can rewrite this as $4 \cdot 4^{n+1} + 25 \cdot 5^{2n-1}$.

It would be nice here if we could just factor out a common factor in order to substitute the inductive hypothesis, but that is not possible. So we split the second term to make at least a partial factorization possible:

$$4 \cdot 4^{n+1} + 25 \cdot 5^{2n-1} = 4 \cdot 4^{n+1} + 4 \cdot 5^{2n-1} + 21 \cdot 5^{2n-1}$$

Therefore,

$$4^{n+2} + 5^{2(n+1)-1} = 4(4^{n+1} + 5^{2n-1}) + 21 \cdot 5^{2n-1} = 21(4k + 5^{2n-1}).$$

We have demonstrated that $4^{n+2} + 5^{2(n+1)-1}$ is divisible by 21. This completes the proof.

Example IV

Theorem: $n^2 < 2^n$ for all integers $n \geq 5$.

Proof by induction: we first verify the statement for $n = 5$: $5^2 < 2^5$ because $25 < 32$. This was the base case.

Inductive step: Now suppose that $n^2 < 2^n$ for some natural number $n \geq 5$. We will show $(n+1)^2 < 2^{n+1}$.

Since $(n+1)^2 = n^2 + 2n + 1$, we only need to show that $2n + 1 < 2^n$ for $n \geq 5$. Then, $n^2 + 2n + 1 < 2^n + 2^n = 2^{n+1}$ by the inductive hypothesis and thus $(n+1)^2 < 2^{n+1}$.

It remains to show that $2n + 1 < 2^n$ for all $n \geq 5$. We do this once again by induction.

Base case: $2n + 1 < 2^n$ is true for $n = 5$ because $11 < 32$.

Inductive step: suppose $2n + 1 < 2^n$ for some $n \geq 5$. Our goal is to show $2(n+1) + 1 < 2^{n+1}$. Let us add two to the inequality of the inductive hypothesis: $2n + 3 < 2^n + 2$. Since $2 < 2^n$ for $n \geq 2$, and certainly for $n \geq 5, 2n + 3 < 2^n + 2 < 2^n + 2^n = 2^{n+1}$. Therefore, $2(n+1) + 1 < 2^{n+1}$.

An Example of a Incorrect Proof by Induction

False Theorem: for all nonnegative integers n, $n = 2n$.
This statement is of course absurd – $n = 2n$ is true for only one number, $n = 0$. Now let us consider the following (incorrect) proof by induction. Define $P(n) = (n = 2n)$.

Base case: for $n = 0$, the statement is correct.
Inductive Step: suppose $n = 2n$ for some nonnegative integer n. Multiply both sides of the equation by $\frac{n+1}{n}$ to get $n + 1 = 2(n + 1)$. That completes the proof.

It is clear that this proof is incorrect, because any alleged proof of a false statement must be incorrect. Let us try to pinpoint the mistake.

The base case $P(0)$ was correctly verified. $P(0) = (0 = 2 \cdot 0)$ is a true statement.

The argument of the inductive step is correct for all n except the first. When $n = 0$, then the argument asks us to multiply by the undefined quantity $\frac{1}{0}$.
Indeed, any argument that claims to prove $P(n) \to P(n + 1)$ for all n must at least be invalid for $n = 0$, because $P(0)$ is a true statement and $P(1)$ is a false statement, so the conditional $P(0) \to P(1)$ is false. (The following conditionals, $P(1) \to P(2)$, etc, are actually true, and our proof above showed that.)