Induction

Benjamin Cosman, Patrick Lin and Mahesh Viswanathan

Fall 2020

TAKE-AWAYS

- *Induction* is a proof technique where to prove $\forall n \geq 0(P(n))$, you first prove $P(0)$ (the *base case*) and then prove $\forall k > 0((P(0) \wedge P(1) \wedge ... \wedge P(k-1)) \rightarrow P(k))$ (the *inductive case*)
- Sometimes you may need multiple base cases and/or a base case that isn't 0.
- Common errors in proofs by induction include omitting the base case, reversing the implication, writing an inductive step that fails for certain values, and using a $P(n)$ that isn't a predicate.

Induction

Consider the following claim and its proof:

Proposition 1. *For any $k > 0$, if powers of 6 smaller than 6^k are each one more than a multiple of 5, then 6^k is also one more than a multiple of 5.*

Proof. Fix $k > 0$ and assume towards a direct proof that powers of 6 smaller than 6^k are each one more than a multiple of 5. Then in particular, 6^{k-1} is one more than a multiple of 5, i.e. it is $5m + 1$ for some $m \in \mathbb{Z}$, so we derive the following sequence of equations:

$$\begin{aligned} 6^{k-1} &= 5m + 1 && \text{(from assumption)} \\ 6^k &= 30m + 6 && \text{(algebra)} \\ 6^k &= 5(6m + 1) + 1 && \text{(algebra)} \end{aligned}$$

$(6m + 1) \in \mathbb{Z}$ because $m \in \mathbb{Z}$, so we have shown that 6^k is one more than a multiple of 5. □

This claim is true and the proof is valid, but by *itself* it's pretty useless: it doesn't tell us that any given power of 6 is actually one more than a multiple of 5 unless we already know that the previous ones are. In fact, we could just as well have proven this other claim instead:

Proposition 2. *For any $k > 0$, if powers of 6 smaller than 6^k are each a multiple of 5, then 6^k is also a multiple of 5.*

Proof. Fix $k > 0$ and assume towards a direct proof that powers of 6 smaller than 6^k are each a multiple of 5. Then in particular, 6^{k-1} is a multiple of 5, i.e. it is $5m$ for some $m \in \mathbb{Z}$, so we derive the following sequence of equations:

$$\begin{aligned} 6^{k-1} &= 5m && \text{(from assumption)} \\ 6^k &= 30m && \text{(algebra)} \\ 6^k &= 5(6m) && \text{(algebra)} \end{aligned}$$

$(6m) \in \mathbb{Z}$ because $m \in \mathbb{Z}$, so we have shown that 6^k is a multiple of 5. □

Both propositions are true: 6^k cannot be both a multiple of 5 and one more than a multiple of 5 at the same time, but remember that a true implication statement can mean *either* that its right-hand side is true or that its left-hand side is false, so the propositions do not contradict each other. But that leaves us with the question: are powers of 6 actually always multiples of 5, one more than multiples of 5, or perhaps something different we haven't thought of yet? To answer this, we consider one more proposition:

Proposition 3. *6^0 is one more than a multiple of 5.*

Proof. $6^0 = 1 = 5(0) + 1$ □

Again, by itself this proposition is pretty useless. But combined with Proposition 1, this proposition allows us to prove a general statement about all the powers of 6:

Proposition 4. *For $n \in \mathbb{N}$, 6^n is one more than a multiple of 5.*

"Proof". [1] From Proposition 3, we know 6^0 is one more than a multiple of 5. Then because 6^0 is one more than a multiple of 5, Proposition 1 tells us that 6^1 is also one more than a multiple of 5. Then because 6^1 and 6^0 are each one more than a multiple of 5, Proposition 1 tells us that 6^2 is also one more than a multiple of 5. And so on forever, so *every* power of 6 is one more than a multiple of 5. □

[1] Don't actually write a proof like this - we'll see a better way to do this with induction in a moment

This idea is formalized in a proof technique called *induction*: to prove that some property is true about every natural number, it suffices to prove that the property is true about 0, and then prove that if the property is true for numbers smaller than some k, it is also true for k. Here's what the ideas from Proposition 1, Proposition 3, and Proposition 4 look like in a unified proof by induction:

Proposition 5. *For $n \in \mathbb{N}$, 6^n is one more than a multiple of 5.*

Proof. We proceed by induction on n.

Base Case: $6^0 = 1 = 5(0) + 1$.

Inductive Case: Fix $k > 0$ and assume as our inductive hypothesis that 6^i is one more than a multiple of 5 for each i where $0 \leq i < k$. Then in particular, 6^{k-1} is one more than a multiple of 5, i.e. it is $5m + 1$ for some $m \in \mathbb{Z}$, so we derive the following sequence of equations:

$$\begin{aligned} 6^{k-1} &= 5m + 1 && \text{(from inductive hypothesis)} \\ 6^k &= 30m + 6 && \text{(algebra)} \\ 6^k &= 5(6m + 1) + 1 && \text{(algebra)} \end{aligned}$$

$(6m + 1) \in \mathbb{Z}$ because $m \in \mathbb{Z}$, so we have shown that 6^k is one more than a multiple of 5.

Induction complete. □

Let's check where the arguments from the proofs of Proposition 3, Proposition 1, and Proposition 4 appear in the proof above.

- The argument from Proposition 3 appears unchanged in the "base case".
- The argument from Proposition 1 appears mostly unchanged in the "inductive case". In a proof by induction we traditionally call the assumption being made an "inductive hypothesis", but note that it is the same as and serves the same purpose as the "direct proof" version from Proposition 1.
- The argument from Proposition 4 has vanished entirely, because it's considered built in to the meaning of "induction": when you write a proof using the template above ("We proceed by induction...base case...inductive case...induction complete"), it is understood that you are implicitly making this infinite chain argument at the end.

In general, for any predicate $P(n)$, the proof template to prove a claim $\forall n \in \mathbb{N}(P(n))$ by induction is as follows:

Proof. We proceed by induction on n.

Base Case: We need to show $P(0)$. *(insert argument here deriving $P(0)$ from other math facts; this will usually be quite trivial).* Therefore, $P(0)$ is true.

Inductive Case: Fix $k > 0$ and assume as our inductive hypothesis that $P(i)$ is true for each i with $0 \leq i < k$. Then we need to show that

$P(k)$ is also true. *(insert argument here that uses the assumption - often just $P(k-1)$ but sometimes smaller i as well - to derive $P(k)$)*. Therefore, $P(k)$ is true.

Induction complete. □

Proposition 5 is almost already written for you as $\forall n \in \mathbb{N}(P(n))$, but in other cases it may be a challenge to figure out what the inductive variable n or what the property $P(n)$ should be. For example, imagine a robot moving on a grid, which starts at the origin $(0,0)$ and at each step can only move diagonally - that is, if its current position is (x,y) then it can move to any of $(x+1,y+1)$, $(x+1,y-1)$, $(x-1,y+1)$, or $(x-1,y-1)$.

Proposition 6. *The robot described above can never reach* $(1,0)$.

To prove this, we first prove the following lemma:

Lemma 7. *For any $n \geq 0$, after the robot has made any n moves, the sum of the coordinates of its ending space is even.*

Proof. We proceed by induction on n.

Base Case: We need to show that after the robot has made any 0 moves, the sum of the coordinates of its ending space is even. [2] After the robot has made 0 moves, it is still at its starting location of $(0,0)$, and $0+0$ is indeed even.

Inductive Case: Fix $k > 0$ and assume as our inductive hypothesis that after taking any number of steps *less* than k, the robot's ending location has even sum of coordinates. Then we need to show that after any k steps, the robot's location also has even sum of coordinates.[3] Consider some sequence of k steps that the robot takes. After the first $k-1$ of those steps, it is at a location (x,y), and by the inductive hypothesis, $x+y$ is even. Then for the final, kth step, there are four cases:

Case 1: The robot moves to $(x+1,y+1)$. In this case, its ending coordinates sum to $(x+y)+2$. $(x+y)$ and 2 are both even, so $(x+y)+2$ is also even.

Case 2: The robot moves to $(x+1,y-1)$. In this case, its ending coordinates sum to $x+y$, which we have already determined is even.

Case 3 and 4: Omitted since they're very similar to 1 and 2.

Thus in every case the final coordinates are even, which is what we needed to show; induction complete. □

Now that we have this lemma, the original proposition is trivial to prove: every location the robot can reach in *any* finite number of moves has an even sum of coordinates, so $(1,0)$ must not be reachable.

[2] Identifying in advance what you need to prove in each case is not strictly necessary since it should be clear from the structure of the proof, but it's probably a good idea to write it anyway for your own sake so you keep it straight.

[3] As above, this sentence can be omitted once you're comfortable with inductive proofs.

The hardest part of proving Proposition 6 is thus structuring it as an inductive proof at all: once you've figured out that it should be proven by induction and how to state the lemma at all, proving the lemma becomes a straightforward proof by induction, which will hopefully become easy with practice. The trick of structuring this as an inductive proof by using "path length" or "time" as the inductive variable (or more generally, "number of state transitions") is a trick that is particularly useful for computer scientists: it's a key tool for proving that a program is correct.

In the previous examples, we have been assuming that our properties hold for all values less than k, but only actually *using* that assumption on $k-1$.[4] Here is an example where the full assumption becomes useful:

Theorem 8. *Every $n \geq 2$ is a product of one or more primes.*[5]

Here's an informal argument "proving" this theorem: Any integer is either a prime itself (thus already a product of just one prime), or it's the product of two smaller integers which are each products of primes. So for example, 30 is a product of primes because it's the product of 3 and 10, where 3 is already a prime and 10 is a further product of 2 and 5. Just like with the inductive arguments in the previous examples, this argument relies on smaller cases being true to prove bigger ones, but now we are relying on various arbitrarily-smaller cases, e.g. proving $P(30)$ using $P(3)$ and $P(10)$, rather than using $P(29)$. Here is the argument formalized using induction:

Proof. We proceed by induction on n.

Base Case: We need to show that 2 is the product of one or more primes. 2 is a prime, so it is a product of just itself.

Inductive Case: Fix $k > 2$ and assume as our inductive hypothesis that each number from 2 through $k-1$ can be written as a product of primes. Now we need to show that k can also be written as a product of primes. There are two cases:

Case 1: k is prime. In this case, k is a product of just itself.

Case 2: k is not prime. In this case, by the definition of prime, $k = pq$ for some integers p and q greater than 1. p and q are also less than k, so the inductive hypothesis applies to them: p can be written as some product of primes $p_1 p_2 ... p_x$ and q as a product of primes $q_1 q_2 ... q_y$. Then k is the product of primes $p_1 p_2 ... p_x q_1 q_2 ... q_y$.

In both cases, k is a product of primes, which is what we needed to show; induction complete. □

This example had a minor new twist: we started somewhere other than 0 (in this case, 2). This was appropriate given the statement of the theorem, and is completely valid - the principle underlying

[4] In some texts including our MCS textbook, what we call induction is called "strong" induction, and then they have a separate version where you *only* assume $P(k-1)$, which they call "weak", "ordinary", or "mathematical" induction. In this class we will only be using strong induction.

[5] By convention, the "product of one number" is just itself. Recall: for integers greater than 1, a composite number is one that can be written as a product pq for some integers p and q greater than 1, and a prime is a number which is not composite.

induction doesn't rely on any special properties of 0 in the natural numbers. (Instead, we *could* have written this to start at 0, as long as we used an alternate predicate, e.g. instead of our implicit $P(n)$ ="n can be written as a product of primes", we could have used $Q(n)$ ="$n+2$ can be written as a product of primes", in which case the theorem could be written as $\forall n \geq 0(Q(n))$ rather than the more natural $\forall n \geq 2(P(n))$.)

Finally, sometimes we need multiple base cases, as in the example below:

Theorem 9. *It is possible to pay any amount of money* $12¢$ *or greater using just* $4¢$ *and* $5¢$ *coins.*

Proof. Let $P(n)$ be "it is possible to pay $n¢$ using just $4¢$ and $5¢$ coins", and we proceed by induction on n.

Base Cases: 12, 13, 14, and 15 can be paid using $4+4+4$, $5+4+4$, $5+5+4$, and $5+5+5$, respectively.

Inductive Case: Fix $k > 15$ and assume as our inductive hypothesis that it is possible to pay all values between 12 and $k-1$ (inclusive). Then we need to show that it is also possible to pay $k¢$. Since $k-4$ is between 12 and $k-1$, by the inductive hypothesis there is some pile of coins that pays $(k-4)¢$. Then adding a $4¢$ coin to that pile pays $k¢$, induction complete. □

Note that the inductive step relies on $P(k-4)$ instead of $P(k-1)$, so e.g. $P(16)$ relies on $P(12)$, $P(17)$ relies on $P(13)$, and so on. This means that $P(12)$ through $P(15)$ don't have anything else to rely on, so they must each be proven separately as a base case. (Another way of thinking about this: if we had made the base case just 12 and then began the inductive step with "Fix $k > 12$", then the later statement "$k-4$ is between 12 and $k-1$" would not be true. And if we had made the base case just 12 and then left the inductive step beginning with "Fix $k > 15$, then neither of the two cases would have explained why the property is true for $n = 13$, 14, or 15.)

Bogus induction proofs

There are several common ways of getting an induction proof wrong.

Leaving out the base case

The base case of an inductive proof is often trivial - see all the examples above. However, it's still critical, and the proof isn't valid if you leave it out. To see this, here's a false claim and an inductive "proof" of that claim:

False Claim 10. *For $n \in \mathbb{N}$, 6^n is a multiple of 5.*

"Proof". We proceed by induction on n.

Inductive Case: Fix $k > 0$ and assume as our inductive hypothesis that 6^i is a multiple of 5 for each i where $0 \leq i < k$. Then in particular, 6^{k-1} is a multiple of 5, i.e. it is $5m$ for some $m \in \mathbb{Z}$, so we derive the following sequence of equations:

$$\begin{aligned} 6^{k-1} &= 5m && \text{(from inductive hypothesis)} \\ 6^k &= 30m && \text{(algebra)} \\ 6^k &= 5(6m) && \text{(algebra)} \end{aligned}$$

$(6m) \in \mathbb{Z}$ because $m \in \mathbb{Z}$, so we have shown that 6^k is a multiple of 5.

Induction complete. □

The algebra in the inductive case is completely valid; it establishes the same true implication statement we saw in Proposition 2. But just as in that earlier proposition, the implication is useless without also proving that 6^0 is a multiple of 5, which can't be done because it isn't true. Note that leaving out the base case in our proof of Proposition 5 would be equally unacceptable - an invalid proof technique doesn't become valid just because the statement it's proving happens to be true.

Reversing the implication

Recall that to prove $p \rightarrow q$, you assume p and then derive q; it is *not* a valid technique to assume q and derive p. Similarly, to prove some equation $x = y$, you can start with various facts you already know and derive $x = y$, but you can *not* just start with $x = y$ and then simplify it down to something that is true - that would be the equivalent of proving $[(x = y) \rightarrow \mathit{True}]$, which may be true even as $x = y$ is false. (For example, just take *any* equation, true or false, and multiply both sides by 0 to get something true.)

The same principles go for proof by induction, but are worth restating here because it is a common error, perhaps because the p and q in question look so similar. So in a standard proof by induction, you will assume some $P(0) \wedge P(1) \wedge ... \wedge P(k-1)$ and try to derive $P(k)$; do *not* instead assume $P(k)$ and derive $P(k-1)$, e.g. if $P(k)$ is an equation, don't start with $P(k)$ and then "simplify" it down to $P(k-1)$.

Inductive step that fails for some values

Consider the following false claim and its "proof":

False Claim 11. *For $n \in \mathbb{N}$, in any group of n cats, all the cats are the same color.*

"Proof". By induction on n.

Base Case: In any group with just 1 cat, all cats in the group are clearly the same color.

Inductive Case: Fix $k > 1$ and assume as our inductive hypothesis that in any group with fewer than k cats, all the cats are the same color. Then if we have k cats $c_1, c_2, ..., c_k$, we can split them into two overlapping groups $c_1, c_2..., c_{k-1}$, and $c_2, c_3..., c_k$. Each of those groups has $k-1$ cats, so by the inductive hypothesis they are all the same color within each group. But then since the groups overlap, all k must be the same color, induction complete. □

One way to find the flaw in the proof is to consider the *smallest* case when the claim is false, namely 2 (there are definitely groups of 2 cats where there 2 are different colors). It would be tempting to then say that the flaw in the proof is that when $k = 3$, the proof is assuming something false (i.e. that groups of $k - 1 = 2$ cats must have the same color). However, this is *not* the flaw - assuming something false can be a valid step in many proofs, such as a proof by contradiction, or a direct proof of a vacuously true implication statement. So if $P(n)$ here is the statement "in any group of n cats, all the cats are the same color", then the problem is *not* in the $(P(1) \wedge P(2)) \rightarrow P(3)$ instance of the inductive case - that one's actually (vacuously) true. Rather, it must be somewhere in the $P(1) \rightarrow P(2)$ (i.e. $k = 2$) instance, because a true statement ($P(1)$) cannot imply a false one ($P(2)$). And we see that sure enough, when $k = 2$, the group of cats c_1, c_2 is being split into groups c_1 and c_2 that *don't* actually overlap, so all talk of "two overlapping groups" and "since the groups overlap" is wrong.

P(n) that isn't a predicate

Notice that in every example, $P(n)$ was always a *predicate* - that is, a statement that has a truth value of true or false once you plug in a specific n. A final common mistake is to use something else instead, like a numeric value. For example:

Proposition 12. *For $n \in \mathbb{N}$, 6^n is one more than a multiple of 5.*

"Proof". Define $P(n)$ as 6^n. We proceed by induction.

Base case: We need to prove $P(0)$... □

No, what would "proving $P(0)$" even mean now? $P(0)$ was just defined to be 6^0 aka 1; you can't prove or disprove the number 1.