Math 220 Fall 2021, Lecture 16: Mathematical induction

1. Mathematical induction (cont'd)

1.1. Strong induction (cont'd)

We use induction to prove a statement about all nonnegative integers, or more generally, about all integers $\geq g$ for some fixed integer g. Recall how this situation looks like, and what induction can do for us.

So we have some fixed integer g (usually 0 or 1, but can be anything). We have a predicate $P(n)$ defined for each integer $n \geq g$. Our goal is to show that $P(n)$ holds for all integers $n \geq g$.

To prove this by regular induction, we show that $P(g)$ holds, and that $P(n) \Longrightarrow P(n+1)$ holds for each $n \geq g$. Thus, we show that

$$\begin{aligned} & P(g)\,; \\ P(g) \Longrightarrow {} & P(g+1)\,; \\ P(g+1) \Longrightarrow {} & P(g+2)\,; \\ P(g+2) \Longrightarrow {} & P(g+3)\,; \\ P(g+3) \Longrightarrow {} & P(g+4)\,; \\ & \ldots . \end{aligned}$$

In contrast, to prove this by strong induction, we show that

$$(P(g) \text{ AND } P(g+1) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n)$$

holds for each $n \geq g$. Thus, we show that

$$\begin{aligned} (\text{nothing}) \Longrightarrow {} & P(g)\,; \\ P(g) \Longrightarrow {} & P(g+1)\,; \\ (P(g) \text{ AND } P(g+1)) \Longrightarrow {} & P(g+2)\,; \\ (P(g) \text{ AND } P(g+1) \text{ AND } P(g+2)) \Longrightarrow {} & P(g+3)\,; \\ (P(g) \text{ AND } P(g+1) \text{ AND } P(g+2) \text{ AND } P(g+3)) \Longrightarrow {} & P(g+4)\,; \\ & \ldots . \end{aligned}$$

So, in a way, strong induction is "induction with a long memory": In the induction step, instead of just using the statement for the previous number, you are allowed to use the statements for all previously traversed numbers from g on.

As an example of strong induction, let me finish a proof that was left unfinished last time: the proof of the Binet formula for Fibonacci numbers.

Recall the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$, which is defined by $f_0 = 0$ and $f_1 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$.

Theorem 1.1.1 (Binet's formula)**.** Let $\varphi = \dfrac{1+\sqrt{5}}{2}$ and $\psi = \dfrac{1-\sqrt{5}}{2}$. Then,

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}} \qquad \text{for each } n \in \mathbb{N}.$$

Proof of the Theorem. Let's prove this by strong induction on n. We need to show that

$$(P(0) \text{ AND } P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n)$$

for each $n \in \mathbb{N}$, where $P(n)$ is the statement "$f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$". This is a form of induction step, but for $n = 0$ it serves as a de-facto base case.

So let us do this. We fix an $n \in \mathbb{N}$. We assume that

$$P(0) \text{ AND } P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(n-1)$$

holds. We must prove that $P(n)$ holds. In other words, we must prove that $f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$.

The recursive definition of the Fibonacci sequence yields $f_n = f_{n-1} + f_{n-2}$. Now, our assumption says that $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$ holds. In particular, $P(n-1)$ holds. That is, we have

$$f_{n-1} = \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}}.$$

But we also obtain from our assumption that $P(n-2)$ holds. That is, we have

$$f_{n-2} = \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}}.$$

Now, substitute both of these equations into $f_n = f_{n-1} + f_{n-2}$, and get

$$\begin{aligned} f_n = f_{n-1} + f_{n-2} &= \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}} + \frac{\varphi^{n-2} - \psi^{n-2}}{\sqrt{5}} \\ &= \frac{1}{\sqrt{5}} \underbrace{\left(\varphi^{n-1} + \varphi^{n-2}\right)}_{\substack{=\varphi^n \\ \text{(by the computation below)}}} - \frac{1}{\sqrt{5}} \underbrace{\left(\psi^{n-1} + \psi^{n-2}\right)}_{\substack{=\psi^n \\ \text{(by the computation below)}}} \\ &= \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n = \frac{\varphi^n - \psi^n}{\sqrt{5}}, \end{aligned}$$

because of the following two computations:

$$\varphi^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{\left(1+\sqrt{5}\right)^2}{4} = \frac{1+5+2\sqrt{5}}{4} = \frac{6+2\sqrt{5}}{4}$$
$$= \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1+\varphi$$

and thus $\varphi^n = \varphi^{n-2} \underbrace{\varphi^2}_{=1+\varphi} = \varphi^{n-2}(1+\varphi) = \varphi^{n-2} + \varphi^{n-1} = \varphi^{n-1} + \varphi^{n-2}$

and similarly $\psi^n = \psi^{n-1} + \psi^{n-2}$.

So we have shown that $f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$. In other words, we have proved that $P(n)$ holds.

This completes the induction step, right?

Well, almost right. We used a little bit more than we knew. In fact, we have used $P(n-1)$ and $P(n-2)$. We argued that both of these follow from our assumption

$$(P(0) \text{ AND } P(1) \text{ AND } P(2) \text{ AND } \cdots \text{ AND } P(n-1)).$$

This argument works for $n \geq 2$, but does not work for $n = 1$ (because in this case, $P(n-2) = P(-1)$ is not contained in the conjunction $P(0)$ AND $P(1)$ AND $P(2)$ AND $\cdots$ AND $P(n-1)$), and also does not work for $n = 0$ (because in this case, neither $P(n-2)$ nor $P(n-1)$ is contained in this conjunction). So we need to prove $P(0)$ and $P(1)$ separately. Our above argument only works for $n \geq 2$.

Fortunately, proving $P(0)$ and $P(1)$ is a straightforward task: Comparing

$$f_0 = 0 \qquad \text{versus} \qquad \frac{\varphi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0$$

yields $P(0)$. Comparing

$$f_1 = 1 \qquad \text{versus} \qquad \frac{\varphi^1 - \psi^1}{\sqrt{5}} = \frac{\varphi - \psi}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = 1$$

yields $P(1)$. Now our proof of Binet's formula is complete. □

Note that our "manual" proofs of $P(0)$ and $P(1)$ were "de-facto base cases". Theoretically, a strong induction has no base case, so they were instead being two special values of n treated separately within the induction step. But of course, these two cases are "the force that starts the induction".

Remark 1.1.2. Binet's formula tells us a lot of things about Fibonacci numbers. For one, it makes it easy to prove results like the addition formula $f_{n+m+1} = f_n f_m + f_{n+1} f_{m+1}$ (a few lectures ago). But it is also helpful in computing the "asymptotics" of the Fibonacci sequence – i.e., finding out how fast it grows. Indeed,

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618\ldots > 1 \qquad \text{and} \qquad \psi = \frac{1-\sqrt{5}}{2} \approx -0.618\ldots \in (-1, 0).$$

So when $n \to \infty$, the powers φ^n grow exponentially, whereas the powers ψ^n tend to 0. So

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}} \text{ grows like } \frac{\varphi^n}{\sqrt{5}}.$$

This is exponential growth, with factor $\varphi \approx 1.618\ldots$. So the Fibonacci numbers grow slower than the powers of 2, but faster than the powers of 1.5, and certainly faster than any polynomial.

The method of strong induction is called this way because it "feels stronger" than the usual method of induction: Instead of deriving $P(n)$ from $P(n-1)$, it allows you to derive $P(n)$ from the conjunction of all previous P's (so $P(n-1)$ and $P(n-2)$ and $P(n-3)$ and so on, all the way back to $P(g)$). This suggests that it is "logically stronger", i.e., can prove more theorems than the usual method of induction. However, this is not the case! The theorems that can be proved using strong induction are precisely the theorems that can be proved using usual induction.

How comes? Didn't we just successfully prove Binet's formula using strong induction after failing to prove it by usual induction? Yes, but we can repackage our strong-induction proof as a usual-induction proof. The trick is to "package the memory into $P(n)$". So instead of proving $P(n)$ by strong induction on n, you can prove

$$P(g) \text{ AND } P(g+1) \text{ AND } P(g+2) \text{ AND } \cdots \text{ AND } P(n)$$

by usual induction on n. So, for example, to prove Binet's formula by usual induction, you restate Binet's formula as follows:

Proposition 1.1.3. Let $n \in \mathbb{N}$. Then,

$$f_k = \frac{\varphi^k - \psi^k}{\sqrt{5}} \text{ holds for all } k \in \{0, 1, \ldots, n\}.$$

Proof. We induct on n (using usual induction):

Base case: For $n = 0$, we just check this by hand.

Induction step: Let $n \in \mathbb{N}$. Assume that

$$f_k = \frac{\varphi^k - \psi^k}{\sqrt{5}} \text{ holds for all } k \in \{0, 1, \ldots, n\}.$$

We must now prove that

$$f_k = \frac{\varphi^k - \psi^k}{\sqrt{5}} \text{ holds for all } k \in \{0, 1, \ldots, n+1\}.$$

To do so, we observe that this is already proved for all $k \in \{0, 1, \ldots, n\}$ (by our induction hypothesis), so we only need to prove it for $k = n + 1$. That is, we only need to prove that $f_{n+1} = \dfrac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}}$.

Our induction hypothesis tells us that $f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$ and also that $f_{n-1} = \dfrac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}}$, as long as $n \geq 1$. We can WLOG assume that $n \geq 1$ (because the $n = 0$ case we can check by hand), and now we can prove $f_{n+1} = \dfrac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}}$ by the same argument that we used above in our strong-induction proof. (Beware that our $n + 1$ now plays the role of the n.) Details are left to the reader. □

Similarly, any proof using strong induction can be repackaged as a proof using usual induction. To wit, if you have a proof of $P(n)$ using strong induction, you can rewrite it as a proof of

$$Q(n) := (P(g) \text{ AND } P(g+1) \text{ AND } P(g+2) \text{ AND } \cdots \text{ AND } P(n))$$

using usual induction. Of course, once you have proved $Q(n)$, the original claim $P(n)$ follows.

Let us see another application of strong induction:

Theorem 1.1.4. Every positive integer is a product of finitely many primes.

(Recall that a **prime** – short for "prime number" – is defined to be an integer $p > 1$ whose only positive divisors are 1 and p.)

Proof of the Theorem. For each integer $n \geq 1$, we let $P(n)$ be the statement "n is a product of finitely many primes". Thus, we must prove $P(n)$ for each integer $n \geq 1$.

We do this by strong induction. So we must prove that

$$(P(1) \text{ AND } P(2) \text{ AND } P(3) \text{ AND } \cdots \text{ AND } P(n-1)) \Longrightarrow P(n)$$

for each integer $n \geq 1$.

Let $n \geq 1$ be an integer. We assume that $P(1)$ AND $P(2)$ AND $P(3)$ AND $\cdots$ AND $P(n-1)$ holds. We must prove that $P(n)$ holds. In other words, we must prove that n is a product of primes.

If $n = 1$, then this is obvious (because 1 is the empty product, i.e., a product of an empty list of primes). From now on, we WLOG assume that $n \neq 1$. So $n > 1$. Now, we are in one of the following two cases:

Case 1: The number n is itself a prime.

Case 2: The number n is not a prime.

In Case 1, the number n is itself a prime, so n is the product of a single prime (itself). So $P(n)$ is proved in Case 1.

Let us now consider Case 2. In this case, the number n is not a prime. Thus, n must have a divisor that is neither 1 nor n (by the definition of "prime"). Pick such a divisor, and call it d. Now, $1 < d < n$ and therefore $1 < \frac{n}{d} < n$; moreover, $\frac{n}{d}$ is an integer because d is a divisor of n.

Now, our induction hypothesis tells us that $P(1)$ AND $P(2)$ AND $P(3)$ AND $\cdots$ AND $P(n-1)$ holds. Thus, $P(d)$ holds (because d is an integer with $1 < d < n$). In other words, d is a product of primes. In other words,

$$d = p_1 p_2 \cdots p_k \qquad \text{for some primes } p_1, p_2, \ldots, p_k.$$

However, from our induction hypothesis, we also conclude that $P\left(\frac{n}{d}\right)$ holds (since $\frac{n}{d}$ is an integer with $1 < \frac{n}{d} < n$). In other words, $\frac{n}{d}$ is a product of primes. In other words,

$$\frac{n}{d} = q_1 q_2 \cdots q_\ell \qquad \text{for some primes } q_1, q_2, \ldots, q_\ell.$$

Multiplying these two equalities, we obtain

$$d \cdot \frac{n}{d} = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_\ell.$$

In other words,

$$n = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_\ell.$$

Thus, n is a product of primes. This proves $P(n)$. Thus, the strong-induction proof is complete. □