Math 220 Fall 2021, Lecture 15: Mathematical induction

1. Mathematical induction (cont'd)

1.1. What is induction? (cont'd)

Last time, we proved that the Tower of Hanoi puzzle can be solved in $2^n - 1$ moves. We proved this by induction. The **big disk** (i.e., the biggest disk in the puzzle) played a crucial role. Now we shall prove that our solution was optimal in the sense that there is no quicker way to solve the puzzle:

Theorem 1.1.1. Each solution to the Tower of Hanoi puzzle requires at least $2^n - 1$ moves.

Proof. We induct on n:

Base case: For $n = 0$, we have $2^n - 1 = 0$, and sure, each solution requires at least 0 moves.

Induction step: Let $n \in \mathbb{N}$. Assume (as the induction hypothesis) that each solution to the Tower of Hanoi puzzle with n disks requires at least $2^n - 1$ moves. We must now prove that each solution to the ToHP (= Tower of Hanoi puzzle) with $n + 1$ disks requires at least $2^{n+1} - 1$ moves.

Consider a solution to the ToHP with $n + 1$ disks. At some point during this solution, the big disk must get moved. Consider the first move where this happens. Let's say we make a moves before this move (i.e., we make a moves before we move the big disk), and we make b moves after this move. So the total number of moves in our solution is $a + 1 + b$. So our goal is to prove that $a + 1 + b \geq 2^{n+1} - 1$.

Consider the situation after the first a moves. At that point, the big disk has to be movable. This implies that the big disk is alone on its peg, and also that the other peg to which we move it must be empty. So all the other disks must be on the third peg. So, at that point, we must have solved the ToHP with n disks. Since a moves were used to do so, we thus conclude using the induction hypothesis that $a \geq 2^n - 1$.

A similar, but subtler, argument can be used to show that $b \geq 2^n - 1$. The probably easiest way to argue this is as follows: We consider the **last** time that the big disk moves. Let c be the number of moves after that last move of the big disk. Then, $b \geq c$ because the first time cannot be later than the last time. However, the c moves that come after the last big-disk move must constitute a solution to the ToHP with n disks, because the remaining disks must be moved to the peg that contains the big disk. So $c \geq 2^n - 1$ by the induction hypothesis. Since $b \geq c$, we now obtain $b \geq c \geq 2^n - 1$.

Now,

$$\underbrace{a}_{\geq 2^n - 1} + 1 + \underbrace{b}_{\geq 2^n - 1} \geq (2^n - 1) + 1 + (2^n - 1) = 2 \cdot 2^n - 1 = 2^{n+1} - 1.$$

This completes the induction step, and thus the proof. □

1.2. Induction with arbitrary base

Recall the Principle of Mathematical Induction:

> **Principle of Mathematical Induction** (or, short, **Principle of Induction):**
>
> Let $P(n)$ be a predicate that depends on a variable n, which is supposed to be a nonnegative integer.
>
> Assume that you have proved $P(0)$.
>
> Assume further that you have proved
>
> $$\forall n \in \mathbb{N} : (P(n) \Longrightarrow P(n+1)).$$
>
> Then, you can deduce that
>
> $$\forall n \in \mathbb{N} : P(n).$$

Now, assume that you want to prove a predicate $P(n)$ not for all $n \in \mathbb{N}$, but for all integers $n \geq 3$ or for all integers $n \geq -5$ or for all positive integers (i.e., for all integers $n \geq 1$). To do so, you can apply the following variant of the above principle:

> **Principle of Mathematical Induction with base case** g (or, short, **Principle of Induction):**
>
> Let g be a fixed integer. Let $\mathbb{Z}_{\geq g} := \{\text{all integers } \geq g\} = \{g, g+1, g+2, \ldots\}$.
>
> Let $P(n)$ be a predicate that depends on a variable n, which is supposed to be an integer $\geq g$.
>
> Assume that you have proved $P(g)$.
>
> Assume further that you have proved
>
> $$\forall n \in \mathbb{Z}_{\geq g} : (P(n) \Longrightarrow P(n+1)).$$
>
> Then, you can deduce that
>
> $$\forall n \in \mathbb{Z}_{\geq g} : P(n).$$

This "new" principle of induction is actually just the old principle of induction, with $P(n)$ replaced by $P(g+n)$.

Here are two real and one fake example of proofs using this principle.

Theorem 1.2.1. We have $2^n \geq n^2$ for all integers $n \geq 4$.

Proof. We induct on n, using this "new" principle with base case 4 (so $g = 4$).

Base case: Our claim $2^n \geq n^2$ holds for $n = 4$, because $2^4 = 16$ and $4^2 = 16$.

Induction step: Let $n \geq 4$ be an integer. Assume that our claim holds for n, i.e., we have $2^n \geq n^2$. We must prove that the claim also holds for $n+1$ instead of n, i.e., that we have $2^{n+1} \geq (n+1)^2$.

We have[1]

$$2^{n+1} = 2 \cdot \underbrace{2^n}_{\substack{\geq n^2 \\ \text{(by the IH)}}} \geq 2 \cdot n^2 = n^2 + n^2 = n^2 + \underbrace{n}_{\geq 4} n \geq n^2 + \underbrace{4n}_{\substack{\geq 2n+1 \\ \text{(since } n \geq 4 \geq 1)}}$$
$$\geq n^2 + 2n + 1 = (n+1)^2 .$$

This completes the induction step. $\square$

The next example comes from calculus:

Theorem 1.2.2. We have $(x^n)' = nx^{n-1}$ for all integers $n \geq 1$.

Proof. We induct on n.

Base case: For $n = 1$, the claim $(x^n)' = nx^{n-1}$ holds, since

$$\left(x^1\right)' = x' = 1 = 1 \cdot x^0.$$

Induction step: Let $n \geq 1$ be an integer. Assume that our claim holds for n, i.e., we have $(x^n)' = nx^{n-1}$. We must prove that the claim also holds for $n+1$ instead of n, i.e., that we have $\left(x^{n+1}\right)' = (n+1)\, x^n$.

Recall that $(fg)' = f'g + fg'$ for any two functions f and g (this is the Leibniz rule, aka the product rule). Applying this rule to $f = x^n$ and $g = x$, we obtain

$$(x^n x)' = \underbrace{(x^n)'}_{\substack{= nx^{n-1} \\ \text{(by the IH)}}} x + x^n \underbrace{x'}_{=1} = n \underbrace{x^{n-1} x}_{= x^n} + x^n \cdot 1 = nx^n + x^n = (n+1)\, x^n.$$

In other words, $\left(x^{n+1}\right)' = (n+1)\, x^n$. This completes the induction step. $\square$

Incidentally, we could state Theorem 1.2.2 for all $n \geq 0$, not just for $n \geq 1$, if we agreed that nx^{n-1} is to be understood as 0 when $n = 0$.

Here is a fake example:

[1]"IH" means "induction hypothesis".

Theorem 1.2.3 (Fake theorem)**.** In any set of $n \geq 1$ horses, all the horses are the same color.

Proof. We induct on n.

Base case: This is clearly true for $n = 1$.

Induction step: Let $n \geq 1$ be an integer. Assume that in any set of n horses, all the horses are the same color. We must now prove the same claim about any set of $n + 1$ horses.

So, consider a set of $n + 1$ horses. Arrange them all into a line:

$$H_1 \;\; H_2 \;\; H_3 \;\; \cdots \;\; H_n \;\; H_{n+1}.$$

By the IH, the first n horses $H_1, H_2, \ldots, H_n$ have the same color. Likewise, the last n horses $H_2, H_3, \ldots, H_{n+1}$ have the same color. Thus, each of the $n + 1$ horses has the same color as the "middle horses" $H_2, H_3, \ldots, H_n$. So we conclude that all $n + 1$ horses $H_1, H_2, \ldots, H_{n+1}$ have the same color. Proof complete? □

The problem with this proof is that the induction step works only for $n \geq 2$. If $n = 1$, then our $n + 1$ horses $H_1, H_2, \ldots, H_{n+1}$ are just two horses H_1, H_2, and there are no "middle horses", so the argument we did does not work.

The upshot is: Make sure that you are really using only what you assumed in the induction step. In the above proof, we assumed $n \geq 1$, but we tacitly used the existence of the "middle horses", which is true only for $n \geq 2$.

1.3. Strong induction

The following variant of the principle of induction is known as **strong induction**:

> **Principle of Strong Induction with base case g:**
>
> Let g be a fixed integer. Let $\mathbb{Z}_{\geq g} := \{\text{all integers } \geq g\} = \{g, g+1, g+2, \ldots\}$.
>
> Let $P(n)$ be a predicate that depends on a variable n, which is supposed to be an integer $\geq g$.
>
> Assume further that you have proved
>
> $$\forall n \in \mathbb{Z}_{\geq g} : \left(\left(P(g) \text{ AND } P(g+1) \text{ AND } P(g+2) \text{ AND } \cdots \text{ AND } P(n-1)\right) \Longrightarrow P(n)\right).$$
>
> Then, you can deduce that
>
> $$\forall n \in \mathbb{Z}_{\geq g} : P(n).$$

Let us take a look at how the "induction step" looks like when we use this new principle. We let $n \in \mathbb{Z}_{\geq g}$, and we prove that

$$\left(P(g) \text{ AND } P(g+1) \text{ AND } P(g+2) \text{ AND } \cdots \text{ AND } P(n-1)\right) \Longrightarrow P(n).$$

For $n = g$, this is saying that

$$(\text{nothing}) \Longrightarrow P(g).$$

So we must prove $P(g)$ using no assumptions. This is precisely what the base case would be with the old principle of induction.

For $n = g + 1$, we must prove that

$$P(g) \Longrightarrow P(g+1).$$

This is the same that we prove in a regular induction proof.

For $n = g + 2$, we must prove that

$$(P(g) \text{ AND } P(g+1)) \Longrightarrow P(g+2).$$

So we derive $P(g+2)$ not only from $P(g+1)$ (as in a regular induction proof), but from the stronger hypothesis $P(g)$ AND $P(g+1)$.

For $n = g + 3$, we must prove that

$$(P(g) \text{ AND } P(g+1) \text{ AND } P(g+2)) \Longrightarrow P(g+3).$$

And so on.

Let us see an example of a proof by strong induction:

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 $n \geq 2$. Now we shall prove an explicit formula for each entry of this sequence:

Theorem 1.3.1 (Binet's formula)**.** Let $\varphi = \dfrac{1+\sqrt{5}}{2}$ and $\psi = \dfrac{1-\sqrt{5}}{2}$. Then,

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

Example 1.3.2. Applying this formula to $n = 17$, we obtain

$$f_{17} = \frac{\varphi^{17} - \psi^{17}}{\sqrt{5}} = \frac{\left(\dfrac{1+\sqrt{5}}{2}\right)^{17} - \left(\dfrac{1-\sqrt{5}}{2}\right)^{17}}{\sqrt{5}} = 1597.$$

Theorem 1.3.1 should be surprising. It is far from expectable that the n-th Fibonacci number should have an explicit formula that involves $\sqrt{5}$.

An attempt to prove Theorem 1.3.1. Let's try to just prove this by (usual) induction on n:

Base case: For $n = 0$, our claim holds because $f_0 = 0 = \dfrac{\varphi^0 - \psi^0}{\sqrt{5}}$.

Induction step: Let $n \in \mathbb{N}$. Assume that $f_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$. We must prove that $f_{n+1} = \dfrac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}}$.

We want to apply the recursion $f_{n+1} = f_n + f_{n-1}$. This requires $n \geq 1$. So we need to check the $n = 0$ case separately, i.e., to check that $f_1 = \dfrac{\varphi^1 - \psi^1}{\sqrt{5}}$. However, this is straightforward:

$$\frac{\varphi^1 - \psi^1}{\sqrt{5}} = \frac{\varphi - \psi}{\sqrt{5}} = \frac{\dfrac{1+\sqrt{5}}{2} - \dfrac{1-\sqrt{5}}{2}}{\sqrt{5}} = 1,$$

which is precisely f_1.

So we can WLOG assume that $n \geq 1$. Therefore, we can apply our recursion $f_{n+1} = f_n + f_{n-1}$, and obtain

$$f_{n+1} = f_n + f_{n-1} = \frac{\varphi^n - \psi^n}{\sqrt{5}} + f_{n-1} \qquad \text{by the IH.}$$

But what do we do about f_{n-1} now? With regular induction, we don't know much about f_{n-1}.

So we need to "remember" the "previous" induction hypothesis: i.e., we need not just our claim for n, but also our claim for $n - 1$. Therefore, we need strong induction. Next time, we will complete this proof using strong induction. $\square$