Math 221 Winter 2023, Lecture 2: Induction

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wd`

1. Induction and recursion (cont'd)

Last time, we defined the sequence $(m_0, m_1, m_2, \ldots)$, whose entry m_n is the # of moves needed to win the Tower of Hanoi game with n disks.

We proved that $m_0 = 0$ and

$$m_n = 2m_{n-1} + 1 \qquad \text{for each } n \geq 1.$$

I then claimed that

$$m_n = 2^n - 1 \qquad \text{for each } n \geq 0.$$

I gave a rather hasty and untrustworthy proof of $m_n = 2^0 + 2^1 + \cdots + 2^{n-1}$, and the right hand side here can be simplified to $2^n - 1$ with a bit of work. Today, I will not use this approach; instead, we will prove $m_n = 2^n - 1$ using a different technique.

1.2. The Principle of Mathematical Induction

This technique is one of the fundamental proof techniques in mathematics. It is called **proof by induction**, and it relies on the following principle:

Theorem 1.2.1 (Principle of Mathematical Induction)**.** Let b be an integer.

Let $P(n)$ be a mathematical statement defined for each integer $n \geq b$.

(For example, $P(n)$ can be "$n + 1 > n$" or "n is even" or "n is prime" or "there exists a prime number larger than n". Note that not every statement needs to be true (for example, "n is even" is true for some n's and false for others). So $P(n)$ is a statement that depends on n; in logic, such a statement is called a **predicate**.)

Assume the following:

1. The statement $P(b)$ holds (i.e., the statement $P(n)$ holds for $n = b$).
2. For each integer $n \geq b$, the implication $P(n) \Longrightarrow P(n+1)$ holds (i.e., if $P(n)$ holds, then $P(n+1)$ does as well)[1].

Then, the statement $P(n)$ holds for every integer $n \geq b$.

Before we discuss the true meaning of this principle, let me show how to use it to prove our $m_n = 2^n - 1$ claim. We state this claim as a theorem:

[1] Let me recall the meaning of the "$\Longrightarrow$" symbol:

Theorem 1.2.2 (explicit answer to Tower of Hanoi)**.** For each integer $n \geq 0$, we let m_n be the # of moves needed to win the Tower of Hanoi game (or ∞ if it cannot be won).

Then,

$$m_n = 2^n - 1 \qquad \text{for each integer } n \geq 0.$$

Proof. We denote the statement "$m_n = 2^n - 1$" by $P(n)$. So we must prove that $P(n)$ holds for each integer $n \geq 0$.

According to the Principle of Mathematical Induction (applied to $b = 0$), it suffices (for this purpose) to show that

1. the statement $P(0)$ holds;
2. for each integer $n \geq 0$, the implication $P(n) \Longrightarrow P(n+1)$ holds.

Proving these two claims will be our two goals; we call them Goal 1 and Goal 2. Let us see if we can achieve them.

Goal 1 is easy: The statement $P(0)$ is just saying that $m_0 = 2^0 - 1$, which is true since both sides are 0.

We now start working towards Goal 2. Let $n \geq 0$ be an integer. We must prove the implication $P(n) \Longrightarrow P(n+1)$. To prove this, we assume that $P(n)$ holds, and we set out to prove that $P(n+1)$ holds.

Our assumption says that $P(n)$ holds, i.e., that

$$m_n = 2^n - 1.$$

In particular, m_n is an integer, so that the Tower of Hanoi game for n disks is winnable.

If A and B are two statements, then "$A \Longrightarrow B$" means the statement "if A, then B". This statement is true whenever B is true, but also true whenever A is false; only in the remaining case (i.e., when A is true but B is false) is it false. In other words, its truth table is as follows:

A	B	$A \Longrightarrow B$
true	true	true
true	false	false
false	true	true
false	false	true

.

You can think of it as a contract: "If you make A true, then I make B true". If you don't make A true, then this contract places no obligation on me, since you haven't done your part! The only way for me to violate the contract is if you make A true but I don't make B true. In other words, $A \Longrightarrow B$ is a "relative" statement, which is true by default if A is not.

Usually, if you want to prove an implication $A \Longrightarrow B$, you start by assuming that A holds, and you need to show that B holds (under this assumption).

We need to prove that $P(n+1)$ holds, i.e., that

$$m_{n+1} \stackrel{?}{=} 2^{n+1} - 1.$$

(The question mark above the equality sign just serves to remind us that we have not proved this equality yet.)

Proposition 1.1.4 from Lecture 1 yields that $m_n = 2m_{n-1} + 1$ if $n \geq 1$ (and if m_{n-1} is not ∞). But this is not very helpful, since we are looking for m_{n+1}, not for m_n.

However, we can also apply Proposition 1.1.4 from Lecture 1 to $n+1$ instead of n (since n is just an arbitrary integer ≥ 1 in that proposition; it is not bound to be our current n). This gives us

$$m_{n+1} = 2m_n + 1.$$

Thus,

$$\begin{aligned} m_{n+1} &= 2 \underbrace{m_n}_{=2^n-1} + 1 = 2 \cdot (2^n - 1) + 1 = 2 \cdot 2^n - 2 + 1 = \underbrace{2 \cdot 2^n}_{\substack{=2^{n+1} \\ \text{(by one of the laws} \\ \text{of exponents)}}} - 1 \\ &= 2^{n+1} - 1. \end{aligned}$$

But this is precisely the statement $P(n+1)$. So we have shown that $P(n+1)$ holds.

More precisely, we have shown that $P(n+1)$ holds under the assumption that $P(n)$ holds. In other words, we have proved the implication $P(n) \Longrightarrow P(n+1)$. This achieves Goal 2.

So we have achieved both goals, and thus the Principle of Mathematical Induction yields that $P(n)$ holds for every integer $n \geq 0$. In other words, $m_n = 2^n - 1$ holds for every integer $n \geq 0$. This proves the theorem. □

What have we really done here? How did this proof work? What is the logic underlying the Principle of Mathematical Induction?

Let us take a look at the structure of our above proof.

Our goal was to prove that $P(n)$ holds for every $n \geq 0$.

In other words, our goal was to prove the statements

$$P(0),\ P(1),\ P(2),\ P(3),\ \ldots.$$

This is an infinite sequence of statements.

We have proved that $P(0)$ holds; that was our Goal 1.

We have then proved that $P(n) \Longrightarrow P(n+1)$ for each n. In other words, we have proved that each statement in our sequence implies the next. In particular, $P(0) \Longrightarrow P(1)$ and $P(1) \Longrightarrow P(2)$ and $P(2) \Longrightarrow P(3)$ and so on.

Combining $P(0)$ with $P(0) \Longrightarrow P(1)$, we obtain $P(1)$.
Combining $P(1)$ with $P(1) \Longrightarrow P(2)$, we obtain $P(2)$.
Combining $P(2)$ with $P(2) \Longrightarrow P(3)$, we obtain $P(3)$.

And so on. Continuing this logic, you obtain $P(4)$, then $P(5)$, then $P(6)$, and so on. By common sense, it is clear that if you keep going on like this, you will eventually reach each statement in our infinite sequence; i.e., you will obtain $P(n)$ for any given integer $n \geq 0$. Of course, this reasoning is informal ("common sense" is not a mathematical concept, nor are the words "and so on").

Thus, if we want to use this kind of reasoning in a mathematical proof, we need to state it as a precise principle and we need this principle to be true. The Principle of Mathematical Induction is doing precisely that.

(You can metaphorically think of this as an infinite daisy chain. Or, to use a common illustration, you have an infinite sequence of dominos arranged in a row, at sufficiently close distances so that tipping over one domino will tip over the next. After you tip over the first domino, all the dominos will eventually fall down.)

I called the Principle of Mathematical Induction a theorem, but I will not prove it, since it is one of the fundamental axioms of mathematics. You can at best replace it by a different axiom, but this doesn't change much; you need some kind of axiom that allows you to "chain together" arbitrarily many little implications.

1.3. Another proof by induction

A proof that uses the Principle of Mathematical Induction is called a **proof by induction**. So our above proof of Theorem 1.2.2 was a proof by induction.

Let us see another (simpler) example of a proof by induction. We will prove the following result:

Theorem 1.3.1 ("Little Gauss formula")**.** For every integer $n \geq 0$, we have

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

The LHS (= left hand side) here is understood to be the sum of the first n positive integers. For $n = 0$, this sum is an empty sum (i.e., it has no addends at all), so its value is 0 by definition.

First proof of Theorem 1.3.1. We set

$$s_n := 1 + 2 + \cdots + n$$

for each $n \geq 0$. Thus, we must prove that $s_n = \dfrac{n(n+1)}{2}$ for each $n \geq 0$.

Let us denote the statement "$s_n = \dfrac{n(n+1)}{2}$" by $P(n)$. So we need to prove that $P(n)$ holds for every $n \geq 0$.

According to the Principle of Mathematical Induction, it suffices to show that

1. the statement $P(0)$ holds;
2. for each $n \geq 0$, the implication $P(n) \Longrightarrow P(n+1)$ holds.

Goal 1 is easy: To prove $P(0)$, we must show that $s_0 = \dfrac{0(0+1)}{2}$, but this is true because both sides equal 0.

Now to Goal 2. We let $n \geq 0$ be an integer, and we want to prove the implication $P(n) \Longrightarrow P(n+1)$. So we assume that $P(n)$ holds, and we set out to prove $P(n+1)$.

By assumption, $P(n)$ holds, so that we have

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

We must prove $P(n+1)$; in other words, we must prove that

$$s_{n+1} \stackrel{?}{=} \frac{(n+1)((n+1)+1)}{2}.$$

To do so, we observe that

$$\begin{aligned} s_{n+1} &= 1+2+\cdots+(n+1) = \underbrace{(1+2+\cdots+n)}_{=s_n} + (n+1) \\ &= s_n + (n+1) = \frac{n(n+1)}{2} + (n+1) \qquad \left(\text{since } s_n = \frac{n(n+1)}{2}\right) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+2)(n+1)}{2} = \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2}. \end{aligned}$$

In other words, $P(n+1)$ holds. Thus, we have proved the implication $P(n) \Longrightarrow P(n+1)$.

We have now achieved both goals, so the Principle of Mathematical Induction yields that $P(n)$ holds for every $n \geq 0$. This proves the theorem. □

There is also a non-inductive proof; this is how Gauss supposedly did it:

Second proof of Theorem 1.3.1. We have

$$\begin{aligned}
&2 \cdot (1+2+\cdots+n) \\
&= (1+2+\cdots+n) + (1+2+\cdots+n) \\
&= (1+2+\cdots+n) + (n+(n-1)+\cdots+1) \\
&\qquad \left(\begin{array}{c} \text{here, we turned the second sum upside-down, i.e.,} \\ \text{we reversed the order of its addends} \end{array} \right) \\
&= \underbrace{(1+n)}_{=n+1} + \underbrace{(2+(n-1))}_{=n+1} + \cdots + \underbrace{(n+1)}_{=n+1} \\
&\qquad \left(\begin{array}{c} \text{here, we rearranged the sum by matching} \\ \text{up each addend inside the first pair of} \\ \text{parentheses with the corresponding addend} \\ \text{inside the second pair of parentheses} \end{array} \right) \\
&= \underbrace{(n+1) + (n+1) + \cdots + (n+1)}_{n \text{ addends}} \\
&= n \cdot (n+1) .
\end{aligned}$$

Dividing this by 2, we find

$$1+2+\cdots+n = \frac{n \cdot (n+1)}{2},$$

and thus Theorem 1.3.1 is proved again. □

Here is a similar theorem:

Theorem 1.3.2. For every integer $n \geq 0$, we have

$$1^2 + 2^2 + \cdots + n^2 = \frac{n\,(n+1)\,(2n+1)}{6}.$$

Proof. The following proof is almost a word-by-word copy of the first proof of Theorem 1.3.1. The structure is the same; only the calculations change.

We set

$$s_n := 1^2 + 2^2 + \cdots + n^2.$$

Thus, we must prove that $s_n = \dfrac{n\,(n+1)\,(2n+1)}{6}$ for each $n \geq 0$.

Let us denote the statement "$s_n = \dfrac{n\,(n+1)\,(2n+1)}{6}$" by $P\,(n)$. So we need to prove that $P\,(n)$ holds for every $n \geq 0$.

According to the Principle of Mathematical Induction, it suffices to show that

1. the statement $P\,(0)$ holds;

2. for each $n \geq 0$, the implication $P(n) \Longrightarrow P(n+1)$ holds.

Goal 1 is easy: To prove $P(0)$, we must show that $s_0 = \dfrac{0(0+1)(2\cdot 0+1)}{6}$, but this is true because both sides equal 0.

Now to Goal 2. We let $n \geq 0$ be an integer, and we want to prove the implication $P(n) \Longrightarrow P(n+1)$. So we assume that $P(n)$ holds, and we set out to prove $P(n+1)$.

By assumption, $P(n)$ holds, so that we have

$$s_n = \frac{n(n+1)(2n+1)}{6}.$$

We must prove $P(n+1)$; in other words, we must prove that

$$s_{n+1} \stackrel{?}{=} \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.$$

To do so, we observe that

$$\begin{aligned}
s_{n+1} &= 1^2 + 2^2 + \cdots + (n+1)^2 \\
&= \underbrace{\left(1^2 + 2^2 + \cdots + n^2\right)}_{=s_n} + (n+1)^2 \\
&= s_n + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \qquad \left(\text{since } s_n = \frac{n(n+1)(2n+1)}{6}\right) \\
&= (n+1)\cdot\left(\frac{n(2n+1)}{6} + (n+1)\right) \\
&= (n+1)\cdot\frac{2n^2+7n+6}{6} \\
&= \frac{(n+1)\left(2n^2+7n+6\right)}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6} \qquad \left(\begin{array}{c}\text{since } 2n^2+7n+6 \text{ can be} \\ \text{factored as } (n+2)(2n+3)\end{array}\right) \\
&= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.
\end{aligned}$$

In other words, $P(n+1)$ holds. Thus, we have proved the implication $P(n) \Longrightarrow P(n+1)$.

We have now achieved both goals, so the Principle of Mathematical Induction yields that $P(n)$ holds for every $n \geq 0$. This proves the theorem. □

As we said, our above proof of Theorem 1.3.2 was an almost verbatim copy of our first proof of Theorem 1.3.1; we only needed to make the obvious changes

and calculate a little bit harder. Both proofs were more or less determined by the idea to use induction. In contrast, the slick second proof of Theorem 1.3.1 cannot be adapted to Theorem 1.3.2. So the induction proof has the advantage of better generalizability.

However, it has the disadvantage that it can only be used to **prove** a formula (in our case, $1+2+\cdots+n = \dfrac{n(n+1)}{2}$ or $1^2+2^2+\cdots+n^2 = \dfrac{n(n+1)(2n+1)}{6}$), not to **find** this formula in the first place. We could not have used induction to answer the question "what is $1+2+\cdots+n$?"; we could only use it to prove the answer after guessing it in some way.

1.4. Notations for an induction proof

Here is some standard terminology that is commonly used in proofs by induction. Let's say that you are proving a statement of the form $P(n)$ for every integer $n \geq b$ (where b is some fixed integer).

- The n is called the **induction variable**; you say that you **induct on** n. It does not have to be called n. Your statement might just as well be "for every integer $a \geq 0$, we have $1+2+\cdots+a = \dfrac{a(a+1)}{2}$", and then you can prove it by inducting on a.
- The proof of $P(b)$ (that is, Goal 1 in our above proofs) is called the **induction base** or the **base case**. In our above examples, this was always the proof of $P(0)$, but in general b can be another integer. (For example, if you are proving the statement "every integer $n \geq 4$ satisfies $2^n \geq n^2$", then b will have to be 4, so your induction base consists in proving that $2^4 \geq 4^2$.)
- The proof of "$P(n) \Longrightarrow P(n+1)$ for every $n \geq b$" (that is, Goal 2 in our above proofs) is called the **induction step**. For example, in the proof of Theorem 1.3.2, this was the part where we assumed that $s_n = \dfrac{n(n+1)(2n+1)}{6}$ and proved that $s_{n+1} = \dfrac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$.
  In the induction step, the assumption that $P(n)$ holds is called the **induction hypothesis** or the **induction assumption**, and the claim that $P(n+1)$ holds (this is the claim that you are trying to prove) is called the **induction goal**. The induction step is complete when the induction goal is reached.

As an example, let us rewrite our above proof of Theorem 1.2.2 using this language:

Proof of Theorem 1.2.2, rewritten. We induct on n.

Base case: The theorem[2] holds for $n = 0$, since both m_0 and $2^0 - 1$ equal 0.

[2] i.e., Theorem 1.2.2

Induction step: Let $n \geq 0$ be an integer. We assume that the theorem holds for n (this is what we previously called $P(n)$). We will now show that the theorem holds for $n+1$ as well (this is what we previously called $P(n+1)$).

We have assumed that the theorem holds for n. In other words, $m_n = 2^n - 1$. This is our induction hypothesis.

We must prove that the theorem holds for $n+1$. In other words, we must prove that $m_{n+1} \stackrel{?}{=} 2^{n+1} - 1$.

To prove this, we apply Proposition 1.1.4 from Lecture 1 to $n+1$ instead of n (we can do this, since $m_n = 2^n - 1$ is not ∞). This gives us

$$\begin{aligned} m_{n+1} &= 2 \underbrace{m_n}_{\substack{=2^n-1 \\ \text{(by the induction hypothesis)}}} + 1 = 2 \cdot (2^n - 1) + 1 \\ &= 2 \cdot 2^n - 2 + 1 = \underbrace{2 \cdot 2^n}_{=2^{n+1}} - 1 = 2^{n+1} - 1. \end{aligned}$$

Thus, the induction goal is reached, and the induction is complete. Hence, the theorem is proved. □

1.5. The Fibonacci numbers

Our next applications of induction will be some properties of the **Fibonacci sequence**. The Fibonacci sequence is defined **recursively** – i.e., a given entry is not defined directly, but rather defined in terms of the previous entries. Specifically, it is defined as follows:

Definition 1.5.1. The **Fibonacci sequence** is the sequence $(f_0, f_1, f_2, \ldots)$ of nonnegative integers defined recursively by setting

$$\begin{aligned} &f_0 = 0, \qquad f_1 = 1, \qquad \text{and} \\ &f_n = f_{n-1} + f_{n-2} \qquad \text{for each } n \geq 2. \end{aligned}$$

In other words, the Fibonacci sequence starts with the two entries 0 and 1, and then every next entry is the sum of the two previous entries.

The entries of the Fibonacci sequence are called the **Fibonacci numbers**. Let us compute the first fourteen of them:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233

.

As we see, a recursive definition is a perfectly valid way to define (e.g.) a sequence of numbers. It allows you to compute each entry of the sequence eventually, as long as you compute the entries in order (i.e., first f_0, then f_1,

then f_2, and so on). In a sense, the reason why this works is the same as the reason why induction works: You can get to any integer $n \geq 0$ if you start at 0 and keep adding 1.

Note that it is important that our recursive definition of f_n uses only previous entries of the sequence (in our case, f_{n-1} and f_{n-2}). If we had instead defined the Fibonacci sequence by

$$f_n = f_{n+1} - f_{n-2},$$

then we could not even compute f_2, since this would require knowing f_3, which would in turn require knowing f_4, and so on.

Let us now see some properties of the Fibonacci sequence:

Theorem 1.5.2. For any integer $n \geq 0$, we have

$$f_1 + f_2 + \cdots + f_n = f_{n+2} - 1.$$

For example, for $n = 8$, this is saying that

$$1 + 1 + 2 + 3 + 5 + 8 + 13 + 21 = 55 - 1.$$

Proof of Theorem 1.5.2. We induct on n.

Base case: For $n = 0$, the theorem claims that $f_1 + f_2 + \cdots + f_0 = f_{0+2} - 1$. This is true, since the LHS is an empty sum (thus $= 0$) whereas the RHS is $f_2 - 1 = 1 - 1 = 0$.

Induction step: Let $n \geq 0$ be an integer. Assume that the theorem holds for n. We must prove that the theorem holds for $n + 1$.

So we assumed that

$$f_1 + f_2 + \cdots + f_n = f_{n+2} - 1.$$

We must prove that

$$f_1 + f_2 + \cdots + f_{n+1} \stackrel{?}{=} f_{(n+1)+2} - 1.$$

We have

$$\begin{aligned} f_1 + f_2 + \cdots + f_{n+1} &= \underbrace{(f_1 + f_2 + \cdots + f_n)}_{\substack{= f_{n+2} - 1 \\ \text{(by our induction hypothesis)}}} + f_{n+1} = f_{n+2} - 1 + f_{n+1} \\ &= \underbrace{f_{n+2} + f_{n+1}}_{\substack{= f_{n+3} \\ \text{(since the recursive definition of the Fibonacci sequence yields } f_{n+3} = f_{n+2} + f_{n+1}\text{)}}} - 1 = f_{n+3} - 1 \\ &= f_{(n+1)+2} - 1 \qquad (\text{since } n + 3 = (n+1) + 2). \end{aligned}$$

This is precisely what we wanted to prove – i.e., it says that the theorem holds for $n + 1$. This completes the induction step. Thus, the theorem is proved. $\square$