12.1 Proof by Induction

In this chapter, we're going to learn about two intertwined concepts: the mathematical proof technique of *induction*, and the programming technique of *recursion*. Even though these techniques may seem unrelated, we'll see over the course of this chapter that they are truly two sides of the same coin. Both are rooted in a fundamental way of representing data and problems, which can be summarized in this general strategy: identify how an entity or problem can be broken down into *smaller instances of that entity or problem with the same structure*.

A proof by induction

Let's start with an example of a common use of induction in mathematics: proving the correctness of various summation/product formulas.[1]

> [1] For example, the formulas found in Appendix C.1 can all be proved using induction.

Example. Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = \sum_{i=0}^{n} i$. Prove that for all $n \in \mathbb{N}$, $f(n) = \frac{n(n+1)}{2}$.

It is possible to verify that this formula is true for any concrete number like $n = 100$ just be computing the value of $f(n)$ and the fraction $\frac{n(n+1)}{2}$, and checking that these two values are equal. But of course a universally-quantified statement can't be proven just with specific exapmles, so we need a different approach: induction.

The principle of induction

The first explicit formulation of the principle of induction was given by the mathematician Blaise Pascal in 1665. However, its uses have been traced as far back as Plato (370 BC), and a variation of Euclid's proof of the existence of infinitely many primes (from around the same time period). We cannot stress enough the importance of the induction principle—it is *the* powerhorse behind nearly all proofs. The principle of induction applies to *universal* statements over the natural numbers—that is, statements of the form $\forall n \in \mathbb{N}, \ P(n)$. It cannot be used to prove statements of any other form! Note however that $P(n)$ can be quite complicated and can involve other possibly nested quantifiers.

In this course, we will only study rigorously the most basic form of induction, commonly called *simple* induction.[2] There are two steps to proving a statement $\forall n \in \mathbb{N}, \ P(n)$ by

> [2] In CSC236/CSC240, you'll learn about different forms of induction.

induction:

- The **base case** is a proof that the statement is True for the first natural number $n = 0$; that is, a proof that $P(0)$ holds.

- The **inductive step** is a proof that for all $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is also true.[3] That is:

[3] Our convention will be to use k as the variable for the inductive step, but you may prefer using n or some other variable name.

$$\forall k \in \mathbb{N}, \ P(k) \Rightarrow P(k+1).$$

Once the base case and inductive step are proven, by the principle of induction, one can conclude $\forall n \in \mathbb{N}, \ P(n)$.

Typical structure of a proof by induction.

Given statement to prove: $\forall n \in \mathbb{N}, \ P(n)$.

Proof. We prove this by induction on n.

Base case: Let $n = 0$.

[Proof that $P(0)$ is True.]

Inductive step: Let $k \in \mathbb{N}$, and *assume* that $P(k)$ is true. (The assumption that $P(k)$ is true is called the *induction hypothesis*.)

[Proof that $P(k+1)$ is True.] ∎

Back to our example

Let's see induction in action with our above example, proving that $\forall n \in \mathbb{N}, \ f(n) = \frac{n(n+1)}{2}$.

Proof. We prove this statement by induction on n.

Base case: Let $n = 0$.

In this case, $f(0) = \sum_{i=0}^{0} i = 0$, and $\frac{0(0+1)}{2} = 0$. So the two sides of the equation are equal.

Inductive step: Let $k \in \mathbb{N}$ and assume that $f(k) = \frac{k(k+1)}{2}$.[4] We want to prove that

[4] This assumption is the *induction hypothesis (I.H.)* for our proof.

$$f(k+1) = \frac{(k+1)(k+2)}{2}.$$

Mini-discussion. As with any proof by induction, the key part of completing the induction step is to determine how to use the induction hypothesis. Remember what we said at the beginning of this section: induction is all about breaking down an entity into smaller instances of the same entity. In our case, we know that $f(k+1) = \sum_{i=0}^{k+1} i$, which can be broken down by "taking out" the last term: $\left(\sum_{i=0}^{k} i\right) + (k+1)$.

Back to our proof. We'll start with the left-hand side of the equation:

$$
\begin{aligned}
f(k+1) &= \sum_{i=0}^{k+1} i && \text{(definition of } f) \\
&= \left(\sum_{i=0}^{k} i\right) + (k+1) && \text{(taking out last term)} \\
&= f(k) + (k+1) && \text{(definition of } f) \\
&= \frac{k(k+1)}{2} + (k+1) && \text{(by the \textbf{I.H.})} \\
&= \frac{(k+1)(k+2)}{2} \quad \blacksquare
\end{aligned}
$$

How does induction "work"?

Proofs by induction often feel like cheating when you first see them. Rather than directly proving a predicate (e.g., $f(n) = \frac{n(n+1)}{2}$) for an arbitrary n, we actually *assume* that the predicate is true for an arbitrary k instead! The reason why induction works is that the inductive step allows us to form a *chain of implications* going from 0 to every other natural number.[5]

---

[5] We often visualize induction as a line of dominos. Pushing over the first domino topples the second domino, then the third, etc.

In a proof by induction, our base case tells us that $P(0)$ is True, unconditionally (no assumptions). And from our induction step, we know that $P(0) \Rightarrow P(1)$, and so $P(1)$ must also be True. And since $P(1)$ is True, using our induction step again, $P(1) \Rightarrow P(2)$, and so $P(2)$ is also True. This chain of implications extends infinitely far out, covering all natural numbers.