# Chapter 6

# Induction

Induction is by far the most powerful and commonly-used proof technique in discrete mathematics and computer science. In fact, the use of induction is a defining characteristic of *discrete* —as opposed to *continuous* —mathematics. To understand how it works, suppose there is a professor who brings to class a bottomless bag of assorted miniature candy bars. She offers to share the candy in the following way. First, she lines the students up in order. Next she states two rules:

1. The student at the beginning of the line gets a candy bar.
2. If a student gets a candy bar, then the following student in line also gets a candy bar.

Let's number the students by their order in line, starting the count with 0, as usual in Computer Science. Now we can understand the second rule as a short description of a whole sequence of statements:

- If student 0 gets a candy bar, then student 1 also gets one.
- If student 1 gets a candy bar, then student 2 also gets one.
- If student 2 gets a candy bar, then student 3 also gets one.

$$\vdots$$

Of course this sequence has a more concise mathematical description:

> If student $n$ gets a candy bar, then student $n+1$ gets a candy bar, for all nonnegative integers $n$.

So suppose you are student 17. By these rules, are you entitled to a miniature candy bar? Well, student 0 gets a candy bar by the first rule. Therefore, by the second rule, student 1 also gets one, which means student 2 gets one, which means student 3 gets one as well, and so on. By 17 applications of the professor's second rule, you get your candy bar! Of course the rules actually guarantee a candy bar to *every* student, no matter how far back in line they may be.

## 6.1 Ordinary Induction

The reasoning that led us to conclude every student gets a candy bar is essentially all there is to induction.

**The Principle of Induction.**

Let $P(n)$ be a predicate. If

- $P(0)$ is true, and
- $P(n)$ IMPLIES $P(n+1)$ for all nonnegative integers, $n$,

then

- $P(m)$ is true for all nonnegative integers, $m$.

Since we're going to consider several useful variants of induction in later sections, we'll refer to the induction method described above as *ordinary induction* when we need to distinguish it. Formulated as a proof rule, this would be

**Rule.** ***Induction Rule***

$$\frac{P(0), \quad \forall n \in \mathbb{N}\,[P(n) \text{ IMPLIES } P(n+1)]}{\forall m \in \mathbb{N}.\, P(m)}$$

This general induction rule works for the same intuitive reason that all the students get candy bars, and we hope the explanation using candy bars makes it clear why the soundness of the ordinary induction can be taken for granted. In fact, the rule is so obvious that it's hard to see what more basic principle could be used to justify it.[1] What's not so obvious is how much mileage we get by using it.

### 6.1.1 Using Ordinary Induction

Ordinary induction often works directly in proving that some statement about nonnegative integers holds for all of them. For example, here is the formula for the sum of the nonnegative integer that we already proved (equation (2.2)) using the Well Ordering Principle:

**Theorem 6.1.1.** *For all $n \in \mathbb{N}$,*

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \tag{6.1}$$

[1]But see section 6.3.

This time, let's use the Induction Principle to prove Theorem 6.1.1.

Suppose that we define predicate $P(n)$ to be the equation (6.1). Recast in terms of this predicate, the theorem claims that $P(n)$ is true for all $n \in \mathbb{N}$. This is great, because the induction principle lets us reach precisely that conclusion, provided we establish two simpler facts:

- $P(0)$ is true.
- For all $n \in \mathbb{N}$, $P(n)$ IMPLIES $P(n+1)$.

So now our job is reduced to proving these two statements. The first is true because $P(0)$ asserts that a sum of zero terms is equal to $0(0+1)/2 = 0$, which is true by definition. The second statement is more complicated. But remember the basic plan for proving the validity of any implication: *assume* the statement on the left and then *prove* the statement on the right. In this case, we assume $P(n)$ in order to prove $P(n+1)$, which is the equation

$$1 + 2 + 3 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}. \tag{6.2}$$

These two equations are quite similar; in fact, adding $(n+1)$ to both sides of equation (6.1) and simplifying the right side gives the equation (6.2):

$$\begin{aligned} 1 + 2 + 3 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{(n+2)(n+1)}{2} \end{aligned}$$

Thus, if $P(n)$ is true, then so is $P(n+1)$. This argument is valid for every nonnegative integer $n$, so this establishes the second fact required by the induction principle. Therefore, the induction principle says that the predicate $P(m)$ is true for all nonnegative integers, $m$, so the theorem is proved.

### 6.1.2 A Template for Induction Proofs

The proof of Theorem 6.1.1 was relatively simple, but even the most complicated induction proof follows exactly the same template. There are five components:

1. **State that the proof uses induction.** This immediately conveys the overall structure of the proof, which helps the reader understand your argument.
2. **Define an appropriate predicate $P(n)$.** The eventual conclusion of the induction argument will be that $P(n)$ is true for all nonnegative $n$. Thus, you should define the predicate $P(n)$ so that your theorem is equivalent to (or follows from) this conclusion. Often the predicate can be lifted straight from the claim, as in the example above. The predicate $P(n)$ is called the *induction hypothesis*. Sometimes the induction hypothesis will involve several variables, in which case you should indicate which variable serves as $n$.

3. **Prove that $P(0)$ is true.** This is usually easy, as in the example above. This part of the proof is called the *base case* or *basis step*.

4. **Prove that $P(n)$ implies $P(n+1)$ for every nonnegative integer $n$.** This is called the *inductive step*. The basic plan is always the same: assume that $P(n)$ is true and then use this assumption to prove that $P(n+1)$ is true. These two statements should be fairly similar, but bridging the gap may require some ingenuity. Whatever argument you give must be valid for every nonnegative integer $n$, since the goal is to prove the implications $P(0) \rightarrow P(1)$, $P(1) \rightarrow P(2)$, $P(2) \rightarrow P(3)$, etc. all at once.

5. **Invoke induction.** Given these facts, the induction principle allows you to conclude that $P(n)$ is true for all nonnegative $n$. This is the logical capstone to the whole argument, but it is so standard that it's usual not to mention it explicitly,

Explicitly labeling the *base case* and *inductive step* may make your proofs clearer.

### 6.1.3 A Clean Writeup

The proof of Theorem 6.1.1 given above is perfectly valid; however, it contains a lot of extraneous explanation that you won't usually see in induction proofs. The writeup below is closer to what you might see in print and should be prepared to produce yourself.

*Proof.* We use induction. The induction hypothesis, $P(n)$, will be equation (6.1).

**Base case:** $P(0)$ is true, because both sides of equation (6.1) equal zero when $n = 0$.

**Inductive step:** Assume that $P(n)$ is true, where $n$ is any nonnegative integer. Then

$$\begin{aligned} 1 + 2 + 3 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) && \text{(by induction hypothesis)} \\ &= \frac{(n+1)(n+2)}{2} && \text{(by simple algebra)} \end{aligned}$$

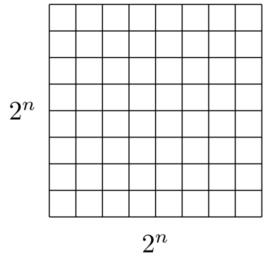
which proves $P(n+1)$.

So it follows by induction that $P(n)$ is true for all nonnegative $n$. ∎

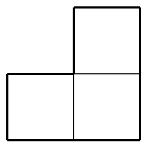
Induction was helpful for *proving the correctness* of this summation formula, but not helpful for *discovering* it in the first place. Tricks and methods for finding such formulas will appear in a later chapter.

### 6.1.4 Courtyard Tiling

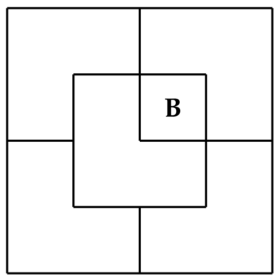
During the development of MIT's famous Stata Center, costs rose further and further over budget, and there were some radical fundraising ideas. One rumored plan was to install a big courtyard with dimensions $2^n \times 2^n$:




One of the central squares would be occupied by a statue of a wealthy potential donor. Let's call him "Bill". (In the special case $n = 0$, the whole courtyard consists of a single central square; otherwise, there are four central squares.) A complication was that the building's unconventional architect, Frank Gehry, was alleged to require that only special L-shaped tiles be used:



A courtyard meeting these constraints exists, at least for $n = 2$:




For larger values of $n$, is there a way to tile a $2^n \times 2^n$ courtyard with L-shaped tiles and a statue in the center? Let's try to prove that this is so.

**Theorem 6.1.2.** *For all $n \geq 0$ there exists a tiling of a $2^n \times 2^n$ courtyard with Bill in a central square.*

*Proof. (doomed attempt)* The proof is by induction. Let $P(n)$ be the proposition that there exists a tiling of a $2^n \times 2^n$ courtyard with Bill in the center.

**Base case:** $P(0)$ is true because Bill fills the whole courtyard.

**Inductive step:** Assume that there is a tiling of a $2^n \times 2^n$ courtyard with Bill in the center for some $n \geq 0$. We must prove that there is a way to tile a $2^{n+1} \times 2^{n+1}$ courtyard with Bill in the center .... ■

Now we're in trouble! The ability to tile a smaller courtyard with Bill in the center isn't much help in tiling a larger courtyard with Bill in the center. We haven't figured out how to bridge the gap between $P(n)$ and $P(n + 1)$.

So if we're going to prove Theorem 6.1.2 by induction, we're going to need some *other* induction hypothesis than simply the statement about $n$ that we're trying to prove.

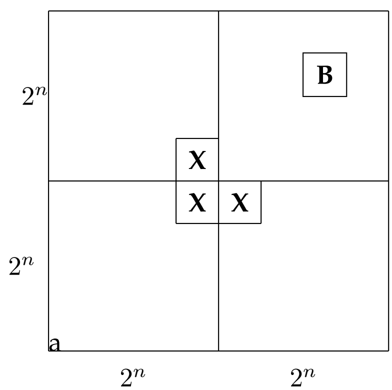
When this happens, your first fallback should be to look for a *stronger* induction hypothesis; that is, one which implies your previous hypothesis. For example, we could make $P(n)$ the proposition that for *every* location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder.

This advice may sound bizarre: "If you can't prove something, try to prove something grander!" But for induction arguments, this makes sense. In the inductive step, where you have to prove $P(n)$ IMPLIES $P(n+1)$, you're in better shape because you can *assume* $P(n)$, which is now a more powerful statement. Let's see how this plays out in the case of courtyard tiling.

*Proof. (successful attempt)* The proof is by induction. Let $P(n)$ be the proposition that for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder.

**Base case:** $P(0)$ is true because Bill fills the whole courtyard.

**Inductive step:** Assume that $P(n)$ is true for some $n \geq 0$; that is, for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder. Divide the $2^{n+1} \times 2^{n+1}$ courtyard into four quadrants, each $2^n \times 2^n$. One quadrant contains Bill (**B** in the diagram below). Place a temporary Bill (**X** in the diagram) in each of the three central squares lying outside this quadrant:




Now we can tile each of the four quadrants by the induction assumption. Replacing the three temporary Bills with a single L-shaped tile completes the job. This proves that $P(n)$ implies $P(n+1)$ for all $n \geq 0$. The theorem follows as a special case. ■

This proof has two nice properties. First, not only does the argument guarantee that a tiling exists, but also it gives an algorithm for finding such a tiling. Second, we have a stronger result: if Bill wanted a statue on the edge of the courtyard, away from the pigeons, we could accommodate him!

Strengthening the induction hypothesis is often a good move when an induction proof won't go through. But keep in mind that the stronger assertion must actually be *true*; otherwise, there isn't much hope of constructing a valid proof! Sometimes finding just the right induction hypothesis requires trial, error, and insight. For example, mathematicians spent almost twenty years trying to prove or disprove the conjecture that "Every planar graph is 5-choosable"[2]. Then, in 1994, Carsten Thomassen gave an induction proof simple enough to explain on a napkin. The key turned out to be finding an extremely clever induction hypothesis; with that in hand, completing the argument is easy!

### 6.1.5 A Faulty Induction Proof

**False Theorem.** *All horses are the same color.*

Notice that no $n$ is mentioned in this assertion, so we're going to have to reformulate it in a way that makes an $n$ explicit. In particular, we'll (falsely) prove that

**False Theorem 6.1.3.** *In every set of $n \geq 1$ horses, all are the same color.*

This a statement about all integers $n \geq 1$ rather $\geq 0$, so it's natural to use a slight variation on induction: prove $P(1)$ in the base case and then prove that $P(n)$ implies $P(n+1)$ for all $n \geq 1$ in the inductive step. This is a perfectly valid variant of induction and is *not* the problem with the proof below.

*False proof.* The proof is by induction on $n$. The induction hypothesis, $P(n)$, will be

$$\text{In every set of } n \text{ horses, all are the same color.} \tag{6.3}$$

**Base case:** $(n = 1)$. $P(1)$ is true, because in a set of horses of size 1, there's only one horse, and this horse is definitely the same color as itself.

**Inductive step:** Assume that $P(n)$ is true for some $n \geq 1$. that is, assume that in every set of $n$ horses, all are the same color. Now consider a set of $n+1$ horses:

$$h_1,\ h_2,\ \ldots,\ h_n,\ h_{n+1}$$

By our assumption, the first $n$ horses are the same color:

$$\underbrace{h_1,\ h_2,\ \ldots,\ h_n,}_{\text{same color}}\ h_{n+1}$$

Also by our assumption, the last $n$ horses are the same color:

$$h_1,\ \underbrace{h_2,\ \ldots,\ h_n,\ h_{n+1}}_{\text{same color}}$$

[2] 5-choosability is a slight generalization of 5-colorability. Although every planar graph is 4-colorable and therefore 5-colorable, not every planar graph is 4-choosable. If this all sounds like nonsense, don't panic. We'll discuss graphs, planarity, and coloring in a later chapter.

So $h_1$ is the same color as the remaining horses besides $h_{n+1}$, and likewise $h_{n+1}$ is the same color as the remaining horses besides $h_1$. So $h_1$ and $h_{n+1}$ are the same color. That is, horses $h_1, h_2, \ldots, h_{n+1}$ must all be the same color, and so $P(n+1)$ is true. Thus, $P(n)$ implies $P(n+1)$.

By the principle of induction, $P(n)$ is true for all $n \geq 1$. ■

We've proved something false! Is math broken? Should we all become poets? No, this proof has a mistake.

The error in this argument is in the sentence that begins, "So $h_1$ and $h_{n+1}$ are the same color." The "$\ldots$" notation creates the impression that there are some remaining horses besides $h_1$ and $h_{n+1}$. However, this is not true when $n = 1$. In that case, the first set is just $h_1$ and the second is $h_2$, and there are no remaining horses besides them. So $h_1$ and $h_2$ need not be the same color!

This mistake knocks a critical link out of our induction argument. We proved $P(1)$ and we *correctly* proved $P(2) \longrightarrow P(3)$, $P(3) \longrightarrow P(4)$, etc. But we failed to prove $P(1) \longrightarrow P(2)$, and so everything falls apart: we can not conclude that $P(2)$, $P(3)$, etc., are true. And, of course, these propositions are all false; there are horses of a different color.

Students sometimes claim that the mistake in the proof is because $P(n)$ is false for $n \geq 2$, and the proof assumes something false, namely, $P(n)$, in order to prove $P(n+1)$. You should think about how to explain to such a student why this claim would get no credit on a 6.042 exam.

### 6.1.6 Problems

**Class Problems**

**Problem 6.1.**
Use induction to prove that

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2. \tag{6.4}$$

for all $n \geq 1$.

Remember to formally

1. Declare proof by induction.

2. Identify the induction hypothesis $P(n)$.

3. Establish the base case.

4. Prove that $P(n) \Rightarrow P(n+1)$.

5. Conclude that $P(n)$ holds for all $n \geq 1$.

as in the five part template.

**Problem 6.2.**
Prove by induction on $n$ that

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1} \tag{6.5}$$

for all $n \in \mathbb{N}$ and numbers $r \neq 1$.

**Problem 6.3.**
Prove by induction:

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}, \tag{6.6}$$

for all $n > 1$.

**Problem 6.4. (a)** Prove by induction that a $2^n \times 2^n$ courtyard with a $1 \times 1$ statue of Bill in *a corner* can be covered with L-shaped tiles. (Do not assume or reprove the (stronger) result of Theorem 6.1.2 that Bill can be placed anywhere. The point of this problem is to show a different induction hypothesis that works.)

**(b)** Use the result of part (a) to prove the original claim that there is a tiling with Bill in the middle.

**Problem 6.5.**
Find the flaw in the following bogus proof that $a^n = 1$ for all nonnegative integers $n$, whenever $a$ is a nonzero real number.

*Bogus proof.* The proof is by induction on $n$, with hypothesis

$$P(n) ::= \forall k \leq n.\, a^k = 1,$$

where $k$ is a nonnegative integer valued variable.

**Base Case:** $P(0)$ is equivalent to $a^0 = 1$, which is true by definition of $a^0$. (By convention, this holds even if $a = 0$.)

**Inductive Step:** By induction hypothesis, $a^k = 1$ for all $k \in \mathbb{N}$ such that $k \leq n$. But then

$$a^{n+1} = \frac{a^n \cdot a^n}{a^{n-1}} = \frac{1 \cdot 1}{1} = 1,$$

which implies that $P(n+1)$ holds. It follows by induction that $P(n)$ holds for all $n \in \mathbb{N}$, and in particular, $a^n = 1$ holds for all $n \in \mathbb{N}$.

■

**Problem 6.6.**
We've proved in two different ways that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

But now we're going to prove a *contradictory* theorem!

**False Theorem.** *For all* $n \geq 0$*,*

$$2 + 3 + 4 + \cdots + n = \frac{n(n+1)}{2}$$

*Proof.* We use induction. Let $P(n)$ be the proposition that $2 + 3 + 4 + \cdots + n = n(n+1)/2$.
*Base case:* $P(0)$ is true, since both sides of the equation are equal to zero. (Recall that a sum with no terms is zero.)
*Inductive step:* Now we must show that $P(n)$ implies $P(n+1)$ for all $n \geq 0$. So suppose that $P(n)$ is true; that is, $2 + 3 + 4 + \cdots + n = n(n+1)/2$. Then we can reason as follows:

$$\begin{aligned} 2 + 3 + 4 + \cdots + n + (n+1) &= [2 + 3 + 4 + \cdots + n] + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

Above, we group some terms, use the assumption $P(n)$, and then simplify. This shows that $P(n)$ implies $P(n+1)$. By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$. ■

Where exactly is the error in this proof?

**Homework Problems**

**Problem 6.7.**

**Claim 6.1.4.** *If a collection of positive integers (not necessarily distinct) has sum* $n \geq 1$*, then the collection has product at most* $3^{n/3}$.

For example, the collection 2, 2, 3, 4, 4, 7 has the sum:

$$2 + 2 + 3 + 4 + 4 + 7 = 22$$

On the other hand, the product is:

$$\begin{aligned} 2 \cdot 2 \cdot 3 \cdot 4 \cdot 4 \cdot 7 &= 1344 \\ &\leq 3^{22/3} \\ &\approx 3154.2 \end{aligned}$$

**(a)** Use strong induction to prove that $n \leq 3^{n/3}$ for every integer $n \geq 0$.

**(b)** Prove the claim using induction or strong induction. (You may find it easier to use induction on the *number of positive integers in the collection* rather than induction on the sum $n$.)

**Problem 6.8.**
For any binary string, $\alpha$, let num $(\alpha)$ be the nonnegative integer it represents in binary notation. For example, num $(\texttt{10}) = 2$, and num $(\texttt{0101}) = 5$.

An $n+1$-*bit adder* adds two $n+1$-bit binary numbers. More precisely, an $n+1$-bit adder takes two length $n+1$ binary strings

$$\alpha_n ::= a_n \ldots a_1 a_0,$$
$$\beta_n ::= b_n \ldots b_1 b_0,$$

and a binary digit, $c_0$, as inputs, and produces a length $n+1$ binary string

$$\sigma_n ::= s_n \ldots s_1 s_0,$$

and a binary digit, $c_{n+1}$, as outputs, and satisfies the specification:

$$\text{num}(\alpha_n) + \text{num}(\beta_n) + c_0 = 2^{n+1} c_{n+1} + \text{num}(\sigma_n). \tag{6.7}$$

There is a straighforward way to implement an $n+1$-bit adder as a digital circuit: an $n+1$-bit *ripple-carry circuit* has $1 + 2(n+1)$ binary inputs

$$a_n, \ldots, a_1, a_0, b_n, \ldots, b_1, b_0, c_0,$$

and $n+2$ binary outputs,

$$c_{n+1}, s_n, \ldots, s_1, s_0.$$

As in Problem 3.5, the ripple-carry circuit is specified by the following formulas:

$$s_i ::= a_i \ \text{XOR}\ b_i \ \text{XOR}\ c_i \tag{6.8}$$
$$c_{i+1} ::= (a_i \ \text{AND}\ b_i) \ \text{OR}\ (a_i \ \text{AND}\ c_i) \ \text{OR}\ (b_i \ \text{AND}\ c_i),. \tag{6.9}$$

for $0 \leq i \leq n$.

**(a)** Verify that definitions (6.8) and (6.9) imply that

$$a_n + b_n + c_n = 2c_{n+1} + s_n. \tag{6.10}$$

for all $n \in \mathbb{N}$.

**(b)** Prove by induction on $n$ that an $n+1$-bit ripple-carry circuit really is an $n+1$-bit adder, that is, its outputs satisfy (6.7).

*Hint:* You may assume that, by definition of binary representation of integers,

$$\text{num}(\alpha_{n+1}) = a_{n+1} 2^{n+1} + \text{num}(\alpha_n). \tag{6.11}$$

**Problem 6.9.**
The 6.042 mascot, Theory Hippotamus, made a startling discovery while playing with his prized collection of unit squares over the weekend. Here is what happened.

First, Theory Hippotamus put his favorite unit square down on the floor as in Figure 6.1 (a). He noted that the length of the periphery of the resulting shape was 4, an even number. Next, he put a second unit square down next to the first so that the two squares shared an edge as in Figure 6.1 (b). He noticed that the length of the periphery of the resulting shape was now 6, which is also an even number. (The periphery of each shape in the figure is indicated by a thicker line.) Theory Hippotamus continued to place squares so that each new square shared an edge with at least one previously-placed square and no squares overlapped. Eventually, he arrived at the shape in Figure 6.1 (c). He realized that the length of the periphery of this shape was 36, which is again an even number.

Our plucky porcine pal is perplexed by this peculiar pattern. Use induction on the number of squares to prove that the length of the periphery is always even, no matter how many squares Theory Hippotamus places or how he arranges them.

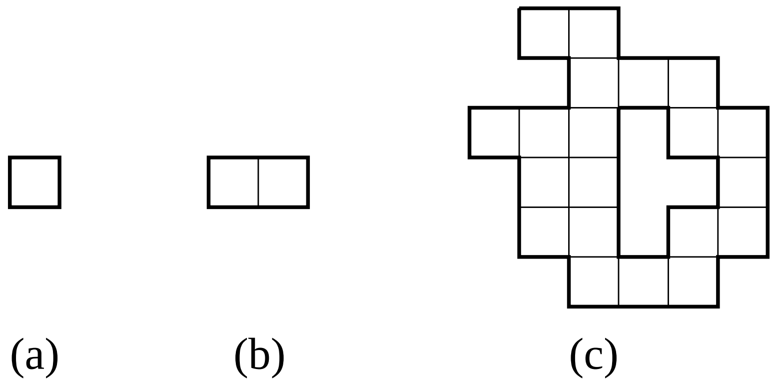



Figure 6.1: Some shapes that Theory Hippotamus created.

## 6.2 Strong Induction

A useful variant of induction is called *strong induction*. Strong Induction and Ordinary Induction are used for exactly the same thing: proving that a predicate $P(n)$ is true for all $n \in \mathbb{N}$.

**Principle of Strong Induction.** Let $P(n)$ be a predicate. If

- $P(0)$ is true, and
- for all $n \in \mathbb{N}$, $P(0), P(1), \ldots, P(n)$ *together* imply $P(n+1)$,

then $P(n)$ is true for all $n \in \mathbb{N}$.

The only change from the ordinary induction principle is that strong induction allows you to assume more stuff in the inductive step of your proof! In an ordinary induction argument, you assume that $P(n)$ is true and try to prove that $P(n+1)$ is also true. In a strong induction argument, you may assume that $P(0)$, $P(1)$, ..., and $P(n)$ are *all* true when you go to prove $P(n+1)$. These extra assumptions can only make your job easier.

### 6.2.1 Products of Primes

As a first example, we'll use strong induction to re-prove Theorem 2.4.1 which we previously proved using Well Ordering.

**Lemma 6.2.1.** *Every integer greater than 1 is a product of primes.*

*Proof.* We will prove Lemma 6.2.1 by strong induction, letting the induction hypothesis, $P(n)$, be

$$n \text{ is a product of primes.}$$

So Lemma 6.2.1 will follow if we prove that $P(n)$ holds for all $n \geq 2$.

**Base Case:** ($n = 2$) $P(2)$ is true because $2$ is prime, and so it is a length one product of primes by convention.

**Inductive step:** Suppose that $n \geq 2$ and that $i$ is a product of primes for every integer $i$ where $2 \leq i < n+1$. We must show that $P(n+1)$ holds, namely, that $n+1$ is also a product of primes. We argue by cases:

If $n+1$ is itself prime, then it is a length one product of primes by convention, so $P(n+1)$ holds in this case.

Otherwise, $n+1$ is not prime, which by definition means $n+1 = km$ for some integers $k, m$ such that $2 \leq k, m < n+1$. Now by strong induction hypothesis, we know that $k$ is a product of primes. Likewise, $m$ is a product of primes. it follows immediately that $km = n$ is also a product of primes. Therefore, $P(n+1)$ holds in this case as well.

So $P(n+1)$ holds in any case, which completes the proof by strong induction that $P(n)$ holds for all nonnegative integers, $n$.

■

### 6.2.2 Making Change

The country Inductia, whose unit of currency is the Strong, has coins worth 3Sg (3 Strongs) and 5Sg. Although the Inductians have some trouble making small change like 4Sg or 7Sg, it turns out that they can collect coins to make change for any number that is at least 8 Strongs.

Strong induction makes this easy to prove for $n+1 \geq 11$, because then $(n+1) - 3 \geq 8$, so by strong induction the Inductians can make change for exactly $(n+1)-3$ Strongs, and then they can add a 3Sg coin to get $(n+1)$Sg. So the only thing to do is check that they can make change for all the amounts from 8 to 10Sg, which is not too hard to do.

Here's a detailed writeup using the official format:

*Proof.* We prove by strong induction that the Inductians can make change for any amount of at least 8Sg. The induction hypothesis, $P(n)$ will be:

> If $n \geq 8$, then there is a collection of coins whose value is $n$ Strongs.

Notice that $P(n)$ is an implication. When the hypothesis of an implication is false, we know the whole implication is true. In this situation, the implication is said to be *vacuously* true. So $P(n)$ will be vacuously true whenever $n < 8$.[3]

We now proceed with the induction proof:

**Base case:** $P(0)$ is vacuously true.

**Inductive step:** We assume $P(i)$ holds for all $i \leq n$, and prove that $P(n+1)$ holds. We argue by cases:

**Case** ($n+1 < 8$): $P(n+1)$ is vacuously true in this case.

**Case** ($n+1 = 8$): $P(8)$ holds because the Inductians can use one 3Sg coin and one 5Sg coins.

**Case** ($n+1 = 9$): Use three 3Sg coins.

**Case** ($n+1 = 10$): Use two 5Sg coins.

**Case** ($n+1 \geq 11$): Then $n \geq (n+1) - 3 \geq 8$, so by the strong induction hypothesis, the Inductians can make change for $(n+1)-3$ Strong. Now by adding a 3Sg coin, they can make change for $(n+1)$Sg.

So in any case, $P(n+1)$ is true, and we conclude by strong induction that for all $n \geq 8$, the Inductians can make change for $n$ Strong.

∎

### 6.2.3 The Stacking Game

Here is another exciting 6.042 game that's surely about to sweep the nation!

You begin with a stack of $n$ boxes. Then you make a sequence of moves. In each move, you divide one stack of boxes into two nonempty stacks. The game

[3] Another approach that avoids these vacuous cases is to define

$$Q(n) ::= \text{there is a collection of coins whose value is } n + 8\text{Sg},$$

and prove that $Q(n)$ holds for all $n \geq 0$.

ends when you have $n$ stacks, each containing a single box. You earn points for each move; in particular, if you divide one stack of height $a + b$ into two stacks with heights $a$ and $b$, then you score $ab$ points for that move. Your overall score is the sum of the points that you earn for each move. What strategy should you use to maximize your total score?

As an example, suppose that we begin with a stack of $n = 10$ boxes. Then the game might proceed as follows:

| Stack Heights | | | | | | | | | | Score |
|---|---|---|---|---|---|---|---|---|---|---|
| $\underline{10}$ | | | | | | | | | | |
| 5 | $\underline{5}$ | | | | | | | | | 25 points |
| $\underline{5}$ | 3 | 2 | | | | | | | | 6 |
| $\underline{4}$ | 3 | 2 | 1 | | | | | | | 4 |
| 2 | $\underline{3}$ | 2 | 1 | 2 | | | | | | 4 |
| $\underline{2}$ | 2 | 2 | 1 | 2 | 1 | | | | | 2 |
| 1 | $\underline{2}$ | 2 | 1 | 2 | 1 | 1 | | | | 1 |
| 1 | 1 | $\underline{2}$ | 1 | 2 | 1 | 1 | 1 | | | 1 |
| 1 | 1 | 1 | 1 | $\underline{2}$ | 1 | 1 | 1 | 1 | | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | | | | | | **Total Score** | | = | | 45 points |

On each line, the underlined stack is divided in the next step. Can you find a better strategy?

### Analyzing the Game

Let's use strong induction to analyze the unstacking game. We'll prove that your score is determined entirely by the number of boxes —your strategy is irrelevant!

**Theorem 6.2.2.** *Every way of unstacking $n$ blocks gives a score of $n(n-1)/2$ points.*

There are a couple technical points to notice in the proof:

- The template for a strong induction proof is exactly the same as for ordinary induction.
- As with ordinary induction, we have some freedom to adjust indices. In this case, we prove $P(1)$ in the base case and prove that $P(1), \ldots, P(n)$ imply $P(n+1)$ for all $n \geq 1$ in the inductive step.

*Proof.* The proof is by strong induction. Let $P(n)$ be the proposition that every way of unstacking $n$ blocks gives a score of $n(n-1)/2$.

**Base case:** If $n = 1$, then there is only one block. No moves are possible, and so the total score for the game is $1(1-1)/2 = 0$. Therefore, $P(1)$ is true.

**Inductive step:** Now we must show that $P(1), \ldots, P(n)$ imply $P(n+1)$ for all $n \geq 1$. So assume that $P(1), \ldots, P(n)$ are all true and that we have a stack of $n+1$ blocks. The first move must split this stack into substacks with positive sizes $a$ and

$b$ where $a + b = n + 1$ and $0 < a, b \leq n$. Now the total score for the game is the sum of points for this first move plus points obtained by unstacking the two resulting substacks:

$$\begin{aligned}
\text{total score} &= \text{(score for 1st move)} \\
&\quad + \text{(score for unstacking } a \text{ blocks)} \\
&\quad + \text{(score for unstacking } b \text{ blocks)} \\
&= ab + \frac{a(a-1)}{2} + \frac{b(b-1)}{2} && \text{by } P(a) \text{ and } P(b) \\
&= \frac{(a+b)^2 - (a+b)}{2} = \frac{(a+b)((a+b)-1)}{2} \\
&= \frac{(n+1)n}{2}
\end{aligned}$$

This shows that $P(1)$, $P(2)$, ..., $P(n)$ imply $P(n + 1)$.

Therefore, the claim is true by strong induction. ■

Despite the name, strong induction is technically no more powerful than ordinary induction, though it makes some proofs easier to follow. But any theorem that can be proved with strong induction could also be proved with ordinary induction (using a slightly more complicated induction hypothesis). On the other hand, announcing that a proof uses ordinary rather than strong induction highlights the fact that $P(n + 1)$ follows directly from $P(n)$, which is generally good to know.

### 6.2.4 Problems

#### Class Problems

**Problem 6.10.**
A group of $n \geq 1$ people can be divided into teams, each containing either 4 or 7 people. What are all the possible values of $n$? Use induction to prove that your answer is correct.

**Problem 6.11.**
The following Lemma is true, but the *proof* given for it below is defective. Pinpoint *exactly* where the proof first makes an unjustified step and explain why it is unjustified.

**Lemma 6.2.3.** *For any prime p and positive integers* $n, x_1, x_2, \ldots, x_n$, *if* $p \mid x_1 x_2 \ldots x_n$, *then* $p \mid x_i$ *for some* $1 \leq i \leq n$.

*False proof.* Proof by strong induction on $n$. The induction hypothesis, $P(n)$, is that Lemma holds for $n$.

**Base case** $n = 1$: When $n = 1$, we have $p \mid x_1$, therefore we can let $i = 1$ and conclude $p \mid x_i$.

**Induction step**: Now assuming the claim holds for all $k \leq n$, we must prove it for $n+1$.

So suppose $p \mid x_1 x_2 \ldots x_{n+1}$. Let $y_n = x_n x_{n+1}$, so $x_1 x_2 \ldots x_{n+1} = x_1 x_2 \ldots x_{n-1} y_n$. Since the righthand side of this equality is a product of $n$ terms, we have by induction that $p$ divides one of them. If $p \mid x_i$ for some $i < n$, then we have the desired $i$. Otherwise $p \mid y_n$. But since $y_n$ is a product of the two terms $x_n, x_{n+1}$, we have by strong induction that $p$ divides one of them. So in this case $p \mid x_i$ for $i = n$ or $i = n+1$. ■

**Problem 6.12.**
Define the *potential*, $p(S)$, of a stack of blocks, $S$, to be $k(k-1)/2$ where $k$ is the number of blocks in $S$. Define the potential, $p(A)$, of a set of stacks, $A$, to be the sum of the potentials of the stacks in $A$.

Generalize Theorem 6.2.2 about scores in the stacking game to show that for any set of stacks, $A$, if a sequence of moves starting with $A$ leads to another set of stacks, $B$, then $p(A) \geq p(B)$, and the score for this sequence of moves is $p(A) - p(B)$.

*Hint:* Try induction on the number of moves to get from $A$ to $B$.

## 6.3 Induction versus Well Ordering

The Induction Axiom looks nothing like the Well Ordering Principle, but these two proof methods are closely related. In fact, as the examples above suggest, we can take any Well Ordering proof and reformat it into an Induction proof. Conversely, it's equally easy to take any Induction proof and reformat it into a Well Ordering proof.

So what's the difference? Well, sometimes induction proofs are clearer because they resemble recursive procedures that reduce handling an input of size $n+1$ to handling one of size $n$. On the other hand, Well Ordering proofs sometimes seem more natural, and also come out slightly shorter. The choice of method is really a matter of style—but style does matter.