# Induction

## 1 Proof by Induction

### 1.1 The Induction Axiom

Induction is by far the most powerful and commonly-used proof technique in Discrete Mathematics and Computer Science. In fact, one could say that applicabillity of induction is the defining characteristic of *discrete*, as opposed to *continuous*, Mathematics.

The standard formulation of induction involves proving properties of the natural numbers, $\mathbb{N} ::= 0, 1, 2, \ldots$. But since most objects of interest in Computer Science—computer programs, task schedules, game outcomes, steps in a computation—can be numbered[1], induction applies widely.

Induction captures a style of reasoning which is so obvious and familiar that its use often goes unnoticed. For example, suppose we had some recipe for assigning a unique "color" to every natural number. One recipe might, for example, assign red to even numbers and blue to odd numbers. Another recipe would be to color even numbers red, odd prime numbers blue, and all other numbers white. Now suppose someone formulates a recipe for natural number coloring, but doesn't tell you exactly what the recipe is. But they do tell you that zero is colored red, and that the coloring has the property that, whenever some number is red, then the next number is red. Can there be any doubt about what the unknown coloring is? Of course not: *every* number is colored red!

The Axiom of Induction essentially just this: if zero is red, and the next number after a red number is also red, then all numbers are red. So the Induction Axiom is both simple and obvious. What's not so obvious is how much mileage we get by using it. For example, let's prove by induction that

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

for all $n \in \mathbb{N}$. The trick for applying Induction is to use this equation for assigning colors to numbers: color the number $n$ red when equation (1) holds, otherwise color it white. To verify that equation (1) holds for all $n \in \mathbb{N}$, we must show that every number is red. Induction allows us to prove this using simple arithmetic.

To begin with, we have to show that zero is red. In other words, we have to show that zero satisfies equation (1). Now when $n = 0$, the lefthand side of the equation is simply 1 and the righthand side is $(0 + 2)(0 + 1)/2$, which equals 1. So zero is red.



[1] A variant of induction, called *structural induction*, is specially tailored for proof about recursively defined data structures and processes; structural induction will be discussed in later notes.

Next, we suppose we have arrived at some natural number, $m$, which is colored red. We only have to show that the next number, $m+1$, must also be red. Then by Induction all natural numbers are red. That is, equation (1) holds for all $n \in \mathbb{N}$.

Now in this case, saying that $m$ is red means

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

This is called the *induction hypothesis*.

How do we show the next number, $m+1$, is red? We have to show:

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

But that's easy using the redness of $m$ and rules of arithmetic:

$$\begin{aligned}
1 + 2 + \cdots + (m+1) + ((m+1)+1) =& [1 + 2 + \cdots + (m+1)] + (m+2) \\
=& [1 + 2 + \cdots + (m+1)] + (m+2) \quad \text{(associativity of } +\text{)} \\
=& \frac{(m+2)(m+1)}{2} + (m+2) \qquad \text{(by (2))} \\
=& (\frac{m+1}{2} + 1)(m+2) \\
=& (\frac{m+1}{2} + \frac{2}{2})(m+2) \\
=& \frac{(m+1)+2}{2}(m+2) \\
=& \frac{((m+1)+2)((m+1)+1)}{2}.
\end{aligned}$$

Here associativity for sums tells us it's ok to parenthesize the sum in any convenient way, and the unlabelled equalities each follow by simple arithmetic. So we have finished the proof by induction that (2)

The Induction Axiom is usually stated formally using logical formulas. To begin with, let's consider some fixed coloring, and interpret the predicate $P(n)$ to mean that "$n$ is colored red." Then we translate our informal language in logical formulas as follows: "we have a coloring that makes zero red" simply translates into $P(0)$. The clause "whenever some number is red, then the next number is red," translates first into "whenever some number, call it, $m$, satisfies $P(m)$, then $P(m+1)$." We can translate the "whenever some number $m$" phrase into a universal quantifier and the "if ... then" into $\longrightarrow$, so the whole phrase translates into

$$\forall m \in \mathbb{N}\ P(m) \longrightarrow P(m+1).$$

The conclusion that "every number is colored red" translates into $\forall n\ P(n)$. So now we can formally state the

**Axiom (Induction).** Suppose that $P(0)$ is true and

$$\forall m \in \mathbb{N}\ P(m) \longrightarrow P(m+1).$$

Then $\forall n \in \mathbb{N}\ P(n)$ is true.

In fact, we can get rid of the English altogether and formulate

**Rule 1.1 (Induction).**

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

We saved this last formulation to last because, until you're experienced translating logical formulas into intelligible language, the formula can hide how obvious and simple the Induction Axiom really is. Actually, you'll often see the Induction Axiom and Rule stated with $n$ in place of $m$, which can make them even harder to decipher. But since $m$ is a bound variable in the second hypothesis of the rule, it doesn't matter if we rename it to be $n$.

## 1.2 Ellipses

Incidentally, the argument above could be criticized because notation such as $1 + 2 + 3 + \cdots + n$ may seem imprecise. Alway watch out for notation with "$\cdots$" or " $\ldots$ " in it (the dots are called an "ellipsis"). This notation is common because it is convenient. The idea is to show enough of a sequence that anyone can figure out the pattern needed to fill in the ellipsis. We could have been more precise by using summation notation instead, namely, $1 + 2 + 3 + \cdots + n$ could be written either as

$$\sum_{i=1}^{n} i$$

or as

$$\sum_{1 \le i \le n} i.$$

In this notation, the pattern of terms in the summation is made explicit. In two important special cases, the definition of the summation $1 + 2 + 3 + \cdots + n$ requires some care. We already observed that if $n = 1$, then $1 + 2 + 3 + \cdots + n = \sum_{1 \le i \le 1} i = 1$. That is, There is only one term in the summation; the appearance of 2 and 3 to indicate the pattern is misleading in this case, because they don't appear.

What about when $n = 0$? Then $\sum_{1 \le i \le 0} i$ is a sum over an *empty set* of $i$'s. That is, there are no terms at all in the summation. In this case, the sum is *defined* to be zero by convention. This convention is useful, because, for example, we can say that for any function $f : \mathbb{N} \to \mathbb{R}$,

$$\sum_{1 \le i \le n+1} f(i) = \left( \sum_{1 \le i \le n} f(i) \right) + f(n+1)$$

for all $n \in \mathbb{N}$, even for $n = 0$.

## 1.3 Proof Format

The text of a proof by induction should consist of four parts. We've aleady seen each of these parts in the proof of equation (1).

1. **State that the proof is by induction.** This immediately conveys the general structure of the argument.

2. **Specify the induction hypothesis**: $P(n)$. Sometimes, the choice of $P(n)$ will come directly from the theorem statement. In the proof above, $P(n)$ was the equation (1) to be proved. Other times, the choice of $P(n)$ is not obvious at all; we will see an example of this soon.

3. **The basis step**: prove $P(0)$. The "basis step" or "base case" is a proof of the predicate $P(0)$.

4. **The inductive step**: prove that $\forall m \in \mathbb{N}\ P(m) \longrightarrow P(m+1)$. Begin the inductive step by writing, "For $m \geq 0$, assume $P(m)$ in order to prove $P(m+1)$." (You can substitute in the statements of the predicates $P(m)$ and $P(m+1)$ if the reminder seems helpful.) Then verify that $P(m)$ indeed implies $P(m+1)$ for every $m \in \mathbb{N}$.

In the case of equation (1), we used induction purely as a proof technique; it gave little insight into why the theorem is true.

Furthermore, while induction was essential in proving the summation equal to $n(n+1)/2$, it did not help us find this formula in the first place. We'll turn to the problem of finding sums of series in a couple weeks.

## 1.4 Induction Examples

This section contains several examples of induction proofs. We begin with an example about Fibonacci numbers, followed by an example from elementary plane geometry, and finally an application of induction to a design problem vital to the future of Computer Science at MIT. Then we illustrate some typical mistakes in using induction by proving (incorrectly!) that all horses are the same color and that camels can carry an unlimited amount of straw.

### 1.4.1 A Fibonacci Identity

Fibonacci was a thirteenth century mathematician who invented *Fibonacci numbers* to model population growth (or rabbits, see Rosen, pp. 205, 310). The first two Fibonacci numbers are 0 and 1, and each subsequent Fibonacci number is the sum of the two previous ones. The $n$ Fibonacci numbers is denoted $F_n$. In other words, the Fibonacci numbers are defined defined recursively by the rules

$$\begin{aligned} F_0 &::= 0, \\ F_1 &::= 1, \\ F_i &::= F_{i-1} + F_{i-2}, \text{ for } i \geq 2. \end{aligned}$$

Here, we're using the notation "::=" to indicate that an equality holds *by definition*. The first few Fibonacci numbers are

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

Fibonacci numbers come up in several different settings, but they have captivated a continued mathematical following out of proportion to their importance in applications because they have a

rich and surprising collection of properties, such as the one expressed in the following theorem. The theorem is a good thing to forget if you run low on brain space, its proof just provides a nice illustration of induction.

**Theorem 1.2.** $\forall n \geq 1, F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$

For example, for $n = 4$ we have $1^2 + 1^2 + 2^2 + 3^2 = 15 = 3 \cdot 5$.

Let's look for a proof by induction. First, the theorem statement suggests that the induction hypothesis $P(n)$ be

$$P(n) ::= \left[ \sum_{i=1}^{n} F_i^2 = F_n F_{n+1} \right].$$

.

Second, we want to identify the gap between $P(m)$ and $P(m+1)$. The predicate $P(m+1)$ states that $\sum_{i=1}^{m+1} F_i^2 = F_{m+1} F_{m+2}$. Now the plan is to use $P(m)$ to reduce this statement to a simpler assertion. An easy way is to subtract the equation in predicate $P(m)$. Taking the $P(m+1)$ equation "minus" $P(m)$ equation gives:

$$F_{m+1}^2 = F_{m+1} F_{m+2} - F_m F_{m+1}.$$

This is the Fibonacci recurrence in disguise; dividing by $F_{m+1}$ and moving a term gives $F_m + F_{m+1} = F_{m+2}$. This is the extra fact need to bridge the gap between $P(m)$ and $P(m+1)$ in the inductive step. The full proof is written below.

*Proof.* The proof is by induction. Let $P(n)$ be the proposition that $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$. In the base case, $P(0)$ is true because $0 = F_0 F_1 = 0 \cdot 1 = 0$. For $m \geq 0$, assume $\sum_{i=1}^{m} F_i^2 = F_m F_{m+1}$ to prove $\sum_{i=1}^{m+1} F_i^2 = F_{m+1} F_{m+2}$.

For all $m \geq 0$, the equation $F_m + F_{m+1} = F_{m+2}$ holds by the definition of the Fibonacci numbers. Multiplying both sides by $F_{m+1}$ and rearranging terms gives $F_{m+1}^2 = F_{m+1} F_{m+2} - F_m F_{m+1}$. Adding this identity to the equation in the proposition $P(m)$ gives:

$$\begin{aligned} F_{m+1}^2 + \sum_{i=1}^{m} F_i^2 &= (F_{m+1} F_{m+2} - F_m F_{m+1}) + F_m F_{m+1} \\ \sum_{i=1}^{m+1} F_i^2 &= F_{m+1} F_{m+2} \end{aligned}$$

This proves that for all $m \in \mathbb{N}$, $P(m) \longrightarrow P(m+1)$ and completes the proof. □

### 1.4.2 Geometry

**Definition 1.3.** A convex polygon is a polygon such that any straight line between any two vertices doesn't leave the polygon.

**Theorem.** *The sum of the interior angles in any $n$-sided convex polygon is exactly $(n-2) \cdot 180$ degrees, for all $n \geq 3$.*

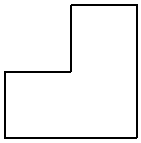

Figure 1: One of the L-shaped tiles that will be used in the courtyard of the new computer science building.

*Proof.* The proof is by induction. The induction hypothesis is $P(n)$::= The sum of the interior angles in any $n$-sided convex polygon is exactly $(n-2)\cdot 180$ degrees.

**Base case** $n = 3$: An 3-sided polygon is a triangle, whose interior angles were shown always to sum to $180$ degrees by Euclid.

**Inductive step**: Assume that $P(m)$ holds for some $m \geq 3$. We must show that $P(m+1)$ holds.

So let $X$ be any $(m+1)$-vertex convex polygon, say with successive vertices $x_1, x_2, \ldots, x_{m+1}$. Let $Y$ be the polygon with vertices $x_1, x_2, \ldots, x_m$. That is, $Y$ is obtained by cutting out one vertex from $X$. Now $Y$ is also a convex polygon (proof left to the reader!), so by induction hypothesis $P(m)$, the sum of the interior angles of $Y$ is $(m-2)180$. Now let $T$ be the triangle with vertices $x_m, x_{m+1}, x_1$. The sum of the interior angles in $X$ is the sum of those in $Y$ plus the sum of those in $T$ (proof again left to the reader: draw a picture [2]). So the sum of the interior angles in $X$ is $(m-2)180+180 = ((m+1)-2)180$. Since $X$ was arbitrary, we conclude that the sum of the interior angles of any $(m+1)$-sided convex polygon is $((m-2)+1)180$. That is, $P(m+1)$ holds. □

Note that this induction argument started with base case $n = 3$ rather than 0. The induction step proved that $P(m) \longrightarrow P(m+1)$ for all $m \geq 3$. The final conclusion was that $\forall n \geq 3\ P(n)$. This is a valid variant of induction.

### 1.4.3 The Fate of Computer Science at MIT

In the preceding examples, induction has served purely as a proof technique. However, it can be useful more generally in problem solving.

MIT is constructing a new Stata Center on the site of the old Building 20. Designed by the world famous architect Frank Gehry, the current cost of the project is budgeted at around $200 million. The Center includes two Computer Science Buildings, one of which is already named after Bill Gates in recognition of his $20 million donation toward construction. But the budget has grown enormously—it was originally supposed to be $100 million. Despite the dramatic recent declines in the stock market, Bill can still afford to make another contribution to cover the shortfall[3], but it will take some special enticement.

Gehry has designed an atrium with a spacious central plaza to be tiled in L-shaped tiles, and MIT is thinking about offering to place a statue of Bill in the courtyard.

The planned courtyard consists of $2^n \times 2^n$ squares. Most of these will be covered by L-shaped tiles, each covering three squares as shown in Figure 1. However, one square will be covered by

[2] see Velleman, example 6.2.3

[3] Up to this point, the story is all true.

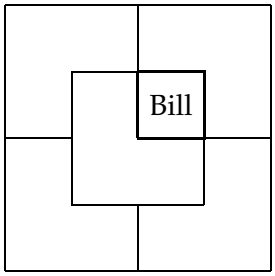


Figure 2: Example with $n = 2$: a legal tiling of a 4x4 courtyard.

the statue of Bill; in fact, this should be one of the central squares. The problem is to find a suitable tiling. An example solution for the case of $n = 2$ is shown.

(The phrase "central squares" is a little ambiguous. If $n = 0$, then the courtyard is a single square, and Bill takes it. If $n > 0$, then there are four central squares, and Bill will take any of them.)

Let's try to prove by induction that such a tiling exists. As usual, we first try to lift the inductive hypothesis directly from the theorem statement.

**Theorem 1.4.** *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. In the base case, $P(0)$ is true because Bill fills the whole courtyard. For $n \geq 0$, assume that there is a tiling of a $2^n \times 2^n$ courtyard with Bill in the center to prove that there is is a legal tiling of 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 is of no obvious help in tiling a larger courtyard with Bill in the center. The usual recipe for finding an inductive proof will not work!

Sometimes, making the induction hypothesis *stronger* makes a proof *easier*. For example, we could make $P(n)$ the proposition that for every position of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder. This hypothesis is "stronger" in the sense that the earlier claim was just a special case. However, when we have to prove $P(n) \longrightarrow P(n+1)$, we will be in better shape because we can *assume* $P(n)$, which is now a more general, more useful statement.

**Method 1.** If you can not show that $P(n) \longrightarrow P(n+1)$ in a proof by induction, change the induction hypothesis; in particular, strengthening the hypothesis may make the proof easier.

Even with this new hypothesis, finding the right way to prove that $P(n) \longrightarrow P(n+1)$ requires some work.

*Proof. (successful attempt)* The proof is by induction. Let $P(n)$ be the proposition that if any one square of a $2^n \times 2^n$ courtyard must be left blank, then there exists a tiling of the remainder. In the base case, $P(0)$ is true because if the one and only square is left blank, then there exists a tiling of the remainder (which is nothing). For $n \geq 0$, assume that if any one square of a $2^n \times 2^n$ courtyard must be left blank, then there exists a tiling of the remainder. We will use this to prove that if any one square of a $2^{n+1} \times 2^{n+1}$ courtyard must be left blank, then 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 will contain the square that must be left blank and can be tiled by induction. Now place a tile in the center of the courtyard so that it covers one square in each remaining quadrant. All that remains is to tile each of these three quadrants, excluding the one square in each that is already covered. But this can also be done by induction. This proves that $\forall n \geq 1\ P(n) \longrightarrow P(n+1)$. The theorem follows as a special case in which a central square is left blank during tiling and is later covered by a statue of Bill. □

This proof has two nice properties. First, we have a stronger result; if Bill wants his statue on the edge of the courtyard, away from the pigeons, we can accommodate him. Second, not only does the proof guarantee that a tiling exists, it actually gave a *recursive procedure* for producing one. For example: To tile a $2^3 \times 2^3$ square leaving the upper right corner empty, divide it into 4, put one tile in the center, and recursively tile the 4 pieces, each with one square missing. (See Figure 3)

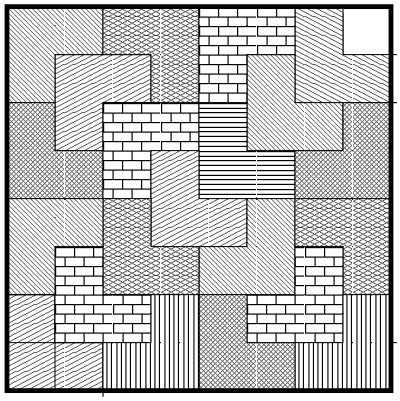

Figure 3: A valid tiling for an 8x8 square leaving the upper right corner empty

### 1.4.4 A False Proof

**False Theorem 1.5.** *All horses are the same color.*

*Proof.* The proof is by induction. Let $P(n)$ be the proposition that in any set of $n$ horses, all the horses are the same color. This is true in the base case $n = 1$, since there is only one horse in the set. For $n \geq 1$, assume that in every set of $n$ horses, all are the same color in order to prove that in every set of $n+1$ horses, all are the same color. Consider a set of $n+1$ horses $h_1, h_2, \ldots, h_{n+1}$. By induction, $h_1, h_2, \ldots, h_n$ all are the same color. Likewise, $h_2, \ldots, h_{n+1}$ all are the same color. Therefore, $h_1, h_2, \ldots, h_{n+1}$ must all share the same color, namely the color of $h_2$. This proves that $P(n) \longrightarrow P(n+1)$ for any $n$, and so completes the proof. □

Where is the bug?—it's in the sentence beginning "Therefore." The " ... " notation helps create confusion about an implicit assumption that the sets $\{h_1, h_2, \ldots, h_n\}$ and $\{h_2, \ldots, h_{n+1}\}$ overlap at $h_2$, and therefore are colored the same. But if $n = 1$, then the first set is just $\{h_1\}$ and the second is $\{h_2\}$, and they do not overlap at all.

Because of this bug, we have really only proven $P(1)$, and $P(n) \longrightarrow P(n+1)$ for $n \geq 2$. But we haven't proved that $P(1) \longrightarrow P(2)$, which of course does not hold.

### 1.4.5 Another False Proof

**False Theorem 1.6.** *A camel can always carry all the straw in a barn.*

*Proof.* The proof is by induction. Let $P(n)$ be the predicate, "The camel can carry $n$ pieces of straw." The base case $P(1)$ is true because a camel can certainly carry one piece of straw. In the inductive step, assume that the camel can carry $n$ pieces of straw to prove that it can carry $n+1$ pieces. But if it can carry $n$ pieces of straw, then surely it can carry $n+1$: one little piece of straw won't make any difference. Therefore $P(n) \longrightarrow P(n+1)$, completing the proof. □

The flaw here is in the bogus assertion that the camel can carry $n+1$ straws if it can carry $n$. Just because it is hard to say exactly for which $n$ this is false, we have no doubt that there is an $n$ that finally exceeds the camel's carrying ability. There will always be "a straw that broke the camel's back."

## 2 Strong Induction

"Strong" induction[4] is a variation of the induction proof method. Strong induction is quite similar to ordinary induction, but is sometimes easier to use when solving problems.

The difference between ordinary induction and strong induction is subtle. Both proofs can be written with nearly the same structure. The only difference is that in an ordinary induction proof we assume only $P(n)$ in order to prove $P(n+1)$. In a strong induction proof, we get to assume all of $P(0), P(1), \ldots, P(n)$ in order to prove $P(n+1)$. This can be a big help. When we try to prove $P(n+1)$ in the inductive step, we do not have just one fact in hand, but rather a whole list of facts!

### 2.1 The Strong Induction Axiom

Like ordinary induction, strong induction can be expressed as an axiom:

**Axiom (Strong Induction).** If $P(0)$ is true and $\forall n \geq 0\ (P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \longrightarrow P(n+1)$, then $P(n)$ is true for all $n \geq 0$.

The expression $(P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \longrightarrow P(n+1)$ might be a little hard to decrypt. It just means that $P(n+1)$ logically follows if we accept all the statements $P(0), P(1), \ldots, P(n)$. Writing this as a rule with logical formulas makes this explicit

**Rule 2.1.** *[Strong Induction]*

$$\frac{P(0), \quad \forall n \in \mathbb{N}\, \forall m \leq n\ P(m) \longrightarrow P(m+1)}{\forall n \in \mathbb{N}\ P(n)}$$

[4] Strong Induction is the same as what Rosen calls the *Second Principle of Induction*

Strong induction is as obvious a principle as ordinary induction, so we could confidently take it as another axiom. Actually, we don't have to make it an axiom, because we could prove the correctness of strong induction by very elementary reasoning starting from the induction axiom.

There's also another interesting way to justify strong induction without using ordinary induction at all. The proof is by contradiction: suppose that some statement in the list $P(0), P(1), \ldots, P(n), \ldots$ was actually false. Since there's some false statement in the list, there must be a *first* one, say $P(k)$ for some $k > 0$, that is false. (The number $k$ has to be $> 0$ because we know $P(0)$ is true.) Now we know that $P(0), P(1), \ldots, P(k-1)$ are true, since $P(k)$ is the first false statement. But since $P(k)$ logically followed from the preceding statements $P(0), P(1), \ldots, P(k-1)$, it must be true, contradicting our assumption that it was false. So there can't be any false statement in the list, that is, $P(n)$ is true for all $n \in \mathbb{N}$.

Of course, we do not prove axioms; we just accept them as facts. But in this case we didn't need to *assume* a strong induction axiom, because we were able to prove the correctness of strong induction, and we did it without even using induction! How come? Well, if you look back at the previous argument, you can see we made a key assumption: that there exists a *first* false statement, $P(k)$. This assumption is an instance of another axiom called the *Least Number Principle* which says that in any set of one or more natural numbers, there must be a *least* (smallest) number. So we have proved the soundness of strong induction, and could similarly prove the soundness of ordinary induction too, by elementary reasoning from the Least Number Principle. This may help you think more clearly about why induction works.

## 2.2 Postage Stamp Example

Now we're ready to solve a problem using strong induction.

**Problem:** Given an unlimited supply of 3 cent and 5 cent stamps, what postages are possible?

**Solution:** Let's first try to guess the answer and then try to prove it. A table that shows the values of all possible combinations of 3 and 5 cent stamps will help. The column heading is the number of 5 cent stamps and the row heading is the number of 3 cent stamps.

| | 0 | 1 | 2 | 3 | 4 | 5 | ... |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 5 | 10 | 15 | 20 | 25 | ... |
| 1 | 3 | 8 | 13 | 18 | 23 | ... | |
| 2 | 6 | 11 | 16 | 21 | ... | | |
| 3 | 9 | 14 | 19 | 24 | ... | | |
| 4 | 12 | 17 | 22 | ... | | | |
| 5 | 15 | 20 | ... | | | | |
| ... | ... | ... | | | | | |

Looking at the table, a reasonable guess is that the possible postages are 0, 3, 5, and 6 cents and every value of 8 or more cents. Let's try to prove this last part using strong induction.

**Claim 2.2.** *For all $n \geq 8$, it is possible to produce $n$ cents of postage from 3¢ and 5¢ stamps.*

Now let's preview the proof. The induction hypothesis will be

$$P(n)::=\text{if } n \geq 8, \text{ then } n\text{¢ postage can be produced using 3¢ and 5¢ stamps} \tag{4}$$

A proof by strong induction will have the same four-part structure as an ordinary induction proof. The base case, $P(0)$, won't be interesting because $P(n)$ is *vacuously* true for all $n < 8$.

In the inductive step we have to show how to produce $n+1$ cents of postage, assuming the strong induction hypothesis that we know how to produce $k$¢ of postage for all values of $k$ between 8 and $n$. A simple way to do this is to let $k = n - 2$ and produce $k$¢ of postage; then add a 3¢ stamp to get $n + 1$ cents.

But we have to be careful; there is a pitfall in this method. If $n + 1$ is 8, 9 or 10, then we can not use the trick of creating $n + 1$ cents of postage from $n - 2$ cents and a 3 cent stamp. In these cases, $n - 2$ is less than 8. None of the strong induction assumptions help us make less than 8¢ postage. Fortunately, making $n + 1$ cents of postage in these three cases can be easily be done directly.

*Proof.* The proof is by strong induction. The induction hypothesis, $P(n)$, is given by (4).

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

In the inductive step, we assume that it is possible to produce postage worth $8, 9, \ldots, n$ cents in order to prove that it is possible to produce postage worth $n + 1$ cents.

There are four cases:

1. $n + 1 < 8$: So $P(n + 1)$ holds vacuously.
2. $n + 1 = 8$: $P(n + 1)$ holds because we produce 8¢postage using one 3¢and one 5¢stamp.
3. $n + 1 = 9$: $P(n + 1)$ holds by using three 3¢stamps.
4. $n + 1 = 10$: $P(n + 1)$ holds by using two 5¢stamps.
5. $n + 1 > 10$: We have $n \geq 10$, so $n - 2 \geq 8$ and by strong induction we may assume we can produce exactly $n - 2$ cents of postage.

So in every case, $P(0) \wedge P(1) \wedge \ldots P(n) \longrightarrow P(n+1)$. By strong induction, we have conclude that $P(n)$ is true for all $n \in \mathbb{N}$. □

### 2.2.1 Induction with nonzero base cases

To conform to the standard format, we organized the proof of Claim 2.2 with a base case of 0. But since we only were interested in 8 or more cents postage, it would have made more sense to start the induction at 8 instead of 0, to treat 8, 9 and 10 as *three* base cases, and to consider the induction step only for $n + 1 > 10$. From now on, we will allow induction proofs formatted with several base cases in this way.

At the other extreme, we can formulate strong induction with no base case at all—just an induction step. Namely, we could replace the strong induction Rule 2.1 with another logical rule:

**Rule 2.3.** *[Strong Induction without base case]*

$$\frac{\forall n \in \mathbb{N}\ (\forall m < n\ P(m)) \longrightarrow P(n))}{\forall n \in \mathbb{N}\ P(n)}$$

Notice that the base case antecedent, $P(0)$, is missing from Rule 2.3. That's because it's hidden in the single, "induction-step" antecedent of the rule. Namely, when $n = 0$ the antecedent requires that $P(0)$ holds as long as $P(m)$ holds for all natural numbers $m < 0$. But we can say that $P(m)$ *does* hold for *all* such natural numbers $m < 0$ since there aren't any! In practice, using this form of strong induction means that even though the proof has no base case, doing the induction step requires handling $n = 0$ as a separate case.

## 2.3 Strong Induction False Proof

In the preceding proof, we were careful not to accidently assume more than is permitted by the strong induction axiom. Now let's be sloppy and see what fun facts we can prove!

**False Theorem 2.4.** *All Fibonacci numbers are even.*

Remember that the Fibonacci numbers are denoted by $F_0, F_1, F_2, \ldots$ where $F_0 = 0$, $F_1 = 1$, and $F_i = F_{i-1} + F_{i-2}$ for $i \geq 2$. The first few Fibonacci numbers are $0, 1, 1, 2, 3, 5, 8, 13, \ldots$.

*Proof.* The proof is by strong induction. Let $P(n)$ be the predicate that $F_n$ is even. In the base case, $P(0)$ is true because $F_0 = 0$, which is even. In the inductive step, for $n \geq 0$ assume that $F_0, F_1, \ldots, F_n$ are all even in order to prove that $F_{n+1}$ is even. By definition, $F_{n+1} = F_n + F_{n-1}$. Since both $F_n$ and $F_{n-1}$ are even, $F_{n+1}$ is even. □

Where is the bug? If $n = 0$, then the statement "By definition, $F_{n+1} = F_n + F_{n-1}$" is false. In this case, $F_{n+1} = F_1$, which equals 1 by definition. We forgot a special case!

We really only proved $P(0)$ and $P(0) \wedge P(1) \longrightarrow P(2), P(1) \wedge P(2) \longrightarrow P(3), \ldots$. We forgot to check one little thing, $P(1)$, and reached an infinite number of false conclusions!

## 2.4 Winning the Game of Nim

The game of Nim is defined as follows: Some positive number of sticks are placed on the ground. Two players take turns removing one, two, or three sticks. The player to remove the last stick loses.

**Theorem 2.5.** *The first player has a winning strategy iff the number of sticks, $n$, is not $4k + 1$ for any $k \in \mathbb{N}$.*

A strategy is a rule for how many sticks to remove when there are $n$ left. We show that if $n = 4k+1$, then player 2 has a strategy that will force a win for him, otherwise, player 1 has a strategy that will force a win for him.

*Proof.* The induction hypothesis is: for all $k \in \mathbb{N}$, if $n = 4k + 1$, then the first player loses, and if $n = 4k$, $4k + 2$, or $4k + 3$, the first player wins. This exhausts all possible cases for $n$.

We proceed by strong induction, using starting from $1$.

**Base case**: $n = 1$. The first player has no choice but to remove $1$ stick and lose, which is what the theorem says for this case.

**Strong inductive step**: Suppose the theorem is true for numbers $1$ through $n$ and show that it is true for $n + 1$. For the inductive step, there are four cases:

- $n + 1 = 4k + 1$: show that the first player loses. We've already handled the base case (1) so we can assume $n + 1 \geq 5$. Consider what the first player might do to win: he can choose to remove 1, 2 or 3 sticks. If he removes one stick, the remaining number of sticks is $n = 4k$. By strong induction, the player who plays at this point has a winning strategy. So the player who played first will lose.

  Similarly, if the first player removes two sticks, the remaining number is $4(k - 1) + 3$. Again, he loses, by the same reasoning. Similarly, by removing $3$ sticks, he loses. So, however the first player moves, he loses.

- $n + 1 = 4k$: show that the first player can win.

  Have the first player remove 3 sticks: the second player then sees $4(k - 1) + 1$ sticks, and loses, by the strong inductive hypothesis.

- $n + 1 = 4k + 2$: show that the first player can win.

  Have the first player remove 1 stick: the second player then sees $4k + 1$ sticks, and loses as in the previous case.

- $n + 1 = 4k + 3$: show that the first player can win.

  Have the first player remove 2 sticks: again, the second player sees $4k + 1$ sticks and loses.

□

## 3 Induction, Strong Induction, and Least Number Principle

We argued above that strong induction is better than ordinary induction, but it's worth observing now that it's only "better" from the point of view of writing up a proof, not because it can be used to prove *more* theorems. It is always possible to convert a proof using one form of induction into a proof using the other.

Of course the conversion from induction to strong induction is trivial because an ordinary induction proof already *is* a strong induction proof—think about that! It's conversion the other way that's interesting.

## 3.1 Converting Strong Induction to Ordinary Induction [Optional]

Here is a recipe for converting, piece-by-piece, a strong induction proof that some proposition, $P(n)$, holds for all $n$, into an ordinary induction proof.

- For the new, ordinary induction proof, use the hypothesis $Q(n)$ where

$$Q(n) ::= \forall m \leq n\ P(m).$$

- In the base case, the strong induction proof establishes $P(0)$. In the new proof, we can use exactly the same argument to establish $Q(0)$, since $Q(0)$ is equivalent to $P(0)$.
- In the inductive step, the strong induction proof shows that $\forall m \leq n\ P(m) \longrightarrow P(n+1)$. In other words, the old induction step proof concludes that

$$Q(n) \longrightarrow P(n+1).$$

  But since $Q(n)$ implies itself, we can add an additional conclusion to the proof, namely,

$$Q(n) \longrightarrow (Q(n) \wedge P(n+1)).$$

- But $(Q(n) \wedge P(n+1))$ is equivalent to $Q(n+1)$, so we can add as a final conclusion that

$$Q(n) \longrightarrow Q(n+1).$$

So by adding the previous two conclusions at the end of the induction case of the strong induction proof, we wind up with an ordinary induction proof of $\forall n\ Q(n)$.

## 3.2 Least Number Principle

Another proof method closely related to induction depends on the

**Axiom (Least Number Principle).** Every nonempty subset, $S \subseteq \mathbb{N}$, has a smallest element.

The Least Number Principle (LNP) looks nothing like the induction axiom, and it may seem obvious but useless.

But as for obvious, note that this axiom would be false if the set of non-negative integers, $\mathbb{N}$, were replaced by, say, the set, $\mathbb{Z}$, of *all* integers, or the set, $\mathbb{Q}^+$, of positive rational numbers. Neither of these sets has a least element. So the LNP is capturing something special about the natural numbers.

As for useless, recall that at the end of Section 2 we used the LNP to "prove" the strong induction axiom. If you look back at this proof, you can read it as a recipe for converting any strong induction proof into an LNP proof—similar to the recipe we gave for converting a strong induction into ordinary induction. So LNP is at least as useful as strong induction!

Conversely, we can use strong induction to prove the LNF. This allows us to convert any LNF proof into a strong induction proof, if we choose. In short, a proof using induction, strong induction, or the LNF to prove some proposition can always be converted in a proof using any the other methods. Mathematicians like LNP, because it is often "prettier" (fewer symbols) than an induction proof. On the other hand, as it often involves proof by contradiction, using the LNP

is not always the best approach. The choice of method is really a matter of style—but style does matter.

[Optional] To prove the LNP by strong induction, let $P(n)$ be the predicate that every set of natural numbers containing the number $n$ also contains a smallest element. So if we prove $\forall n\ P(n)$, then we have proved the LNP, since a nonempty set has to contain *some* element $n$.

*Proof.* We prove $\forall n\ P(n)$ by strong induction. The induction hypothesis is $P(n)$.

**Base case** $P(0)$: If a set contains $0$, then $0$ is its smallest element.

**strong induction step**: Assume $\forall m \leq n\ P(m)$, and prove $P(n+1)$.

Consider any set, $S$, containing the integer, $n+1$. If $n+1$ is actually the smallest element of $S$, then we are done. Otherwise, $S$ must contain a smaller element $m < n+1$. But then $m \leq n$, and the strong induction hypothesis implies that $S$ contains a smallest element, and we are done in this case too. □