

Introduction to Induction

Key topics:

- * Introduction and Definitions
 - * Examples of Weak Induction
 - * Proper Proof Form
 - * Examples of Strong Induction
 - * A Faulty Proof and Some Interesting Proofs
 - * Some Useful Formulas
-

One of the most important tasks of mathematics is to discover and characterize regular patterns or sequences. The main mathematical tool we use to prove statements about sequences is induction. Induction is a very important tool in computer science for several reasons, one of which is the fact that a characteristic of most programs is repetition of a sequence of statements.

To illustrate how induction works, imagine that you are climbing an infinitely high ladder. How do you know whether you will be able to reach an arbitrarily high rung? Suppose you make the following two assertions about your climbing abilities:

- 1) I can definitely reach the first rung.
- 2) Once I get to any rung, I can always climb to the next one up.

If both statements are true, then by statement 1 you can get to the first one, and by statement 2, you can get to the second. By statement 2 again, you can get to the third, and fourth, etc. Therefore, you can climb as high as you wish. Notice that both of these assertions are necessary for you to get anywhere on the ladder. If only statement 1 is true, you have no guarantee of getting beyond the first rung. If only statement 2 is true, you may never be able to get started.

Assume that the rungs of the ladder are numbered with the positive integers (1,2,3...). Now think of a specific property that a number might have. Instead of "reaching an arbitrarily high rung", we can talk about an arbitrary positive integer having that property. We will use the shorthand $P(n)$ to denote the positive integer n having property P . How can we use the ladder-climbing technique to prove that $P(n)$ is true for all positive n ? The two assertions we need to prove are:

- 1) $P(1)$ is true
- 2) for any positive k , if $P(k)$ is true, then $P(k+1)$ is true

Assertion 1 means we must show the property is true for 1; assertion 2 means that if any number has property P then so does the next number. If we can prove both of these statements, then $P(n)$ holds for all positive integers, just as you could climb to an arbitrary rung of the ladder.

The foundation for arguments of this type is the **Principle of Mathematical Induction**. The Principle of Mathematical Induction can be used as a proof technique on statements that have a particular form. First of all, we must be working with positive integers or numbers of objects, and we must be talking about some kind of sequence or pattern. The Principle tells us that if we can prove the assertion is true for 1, and then prove that it is also true for $k+1$ (assuming it is true for k), we have proven the assertion for all positive integers, because if it is true for 1 and $k+1$, then it is true for k . When it is true for all three, it is true for all positive integers. Thus, the following steps are required:

- i) Prove that $P(1)$ is true.
- ii) Assume that $P(k)$ is true, and prove that $P(k+1)$ is true.

Note that we do not *prove* that $P(k)$ is true (except for $k = 1$). Instead, we show that *if* $P(k)$ is true, then $P(k+1)$ must also be true. That's all that is necessary according to the Principle of Mathematical Induction. Step (i) is called the **basis of induction**, and step (ii) is called the **induction step**. The assumption that $P(k)$ is true is called the **induction hypothesis**.

As an another illustration, consider an infinite number of dominoes positioned one behind the other in such a way that if any given one falls, then the one behind it falls too. In order to establish that the entire chain will fall under a certain set of circumstances, two things are necessary. First, someone has to push over the first domino; this corresponds to the basis of induction. Second, we must also know that whenever any domino falls, it will knock over the next in the chain. This requirement can be expressed by saying that whenever domino N falls, so does $N+1$. This corresponds to using the induction hypothesis to establish the result for the next value of N .

Example 1: Suppose that great, great, great.... grandpa Fred married and had two children. Call this generation 1, so generation 1 contains the offspring of Fred (2). Each of these children have two children, so generation 2 has four offspring. Each of these 4 has two children so at generation 3, we have 8 offspring. This continues, without fail, for generation to generation. It appears that generation n will have 2^n offspring. We are guessing that $P(n) = 2^n$. We can use induction to *prove* that our guess is correct.

- i) base case: prove that $P(1)$ is true

$$P(1) = 2^1 = 2 \text{ (generation 1 has 2 offspring)}$$

- ii) assume our guess is correct for an arbitrary generation k , and prove it is also true for generation $k+1$.

induction hypothesis is to assume $P(k)$: $P(k) = 2^k$
and show: $P(k+1) = 2^{(k+1)}$

PROOF:

By the rules of this family, each offspring is required to have 2 children, thus the number of offspring at generation $k+1$ will be twice the number of generation k , or $P(k+1) = 2P(k)$.

By the inductive hypothesis, $P(k) = 2^k$, so :

$$P(k+1) = 2P(k) = 2(2^k) = 2^{(k+1)}$$

$P(k+1)$ is true when $P(k)$ is true, and therefore $P(n)$ is true for all natural numbers.

Example 2: Prove that for every positive integer n , the sum of the first n positive integers is $n(n+1)/2$. This is the *classic* example of an inductive proof:

$$P(n) \text{ denotes: } 1+2+3+\dots+n = n(n+1)/2$$

$$\text{if } n = 2 \text{ then: } 1+2 = 2(2+1)/2 = 3$$

$$\text{if } n = 3 \text{ then: } 1+2+3 = 3(3+1)/2 = 6 \text{ etc.}$$

To prove this for all positive integers, we follow the steps given above for inductive proofs:

i) base case: prove that $P(1)$ is true

$$1 = 1(1+1)/2 = 1$$

ii) induction hypothesis is to assume $P(k)$: $1+2+3+\dots+k = k(k+1)/2$
and show: $P(k+1)$:

$$1+2+3+\dots+(k+1) = (k+1)[(k+1)+1]/2 \quad (\text{by substituting } (k+1) \text{ for } k \text{ in the induction hypothesis})$$

PROOF:

By the induction hypothesis, we already have a formula for the first k integers. So, a formula for the first $(k+1)$ integers may be found by simply adding $(k+1)$ to both sides of the induction hypothesis, and simplifying:

$$\begin{aligned} 1+2+3+\dots+k+(k+1) &= k(k+1)/2 + (k+1) \\ &= [k(k+1) + 2(k+1)] / 2 \\ &= (k^2 + 3k + 2) / 2 \\ &= [(k+1)(k+2)] / 2 \\ &= (k+1)[(k+1)+1] / 2 \end{aligned}$$

$P(k+1)$ is true when $P(k)$ is true, and therefore $P(n)$ is true for all natural numbers.

Steps to doing an inductive proof:

- 1) state $P(n)$
- 2) show that $P(\text{base case})$ is true
- 3) state the inductive hypothesis (substitute k for n)
- 4) state what must be proven (substitute $k+1$ for n)
- 5) state that you are beginning your proof, and proceed to manipulate the inductive hypothesis (which we assume is true) to find a link between the inductive hypothesis and the statement to be proven. Always state explicitly where you are invoking the inductive hypothesis.
- 6) Always finish your proof with something like: $P(k+1)$ is true when $P(k)$ is true, and therefore $P(n)$ is true for all natural numbers.

NOTE: On problem sets and exams, it is important to present your proof in the proper form. You must *always* write out steps 1-6 as given above. Form is important in inductive proofs.

Example 3: $P(n)$ denotes $1 + 3 + 5 + \dots + (2n-1) = n^2$, i.e., the sum of the first n odd integers is n^2

i) base case: prove that $P(1)$ is true $1 = 1^2 = 1$

ii) induction hypothesis is to assume $P(k)$: $1 + 3 + 5 + \dots + (2k-1) = k^2$

and show: $P(k+1)$: $1 + 3 + 5 + \dots + (2k-1) + (2k+1) = (k+1)^2$

PROOF:

Simulate adding another term to both sides of the induction hypothesis:

$$\begin{aligned} 1 + 3 + 5 + \dots + (2k-1) + (2k+1) &= k^2 + (2k+1) \\ &= k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

$P(k+1)$ is true when $P(k)$ is true, and therefore $P(n)$ is true for all natural numbers.

The following example illustrates that the basis of induction does not have to be 1:

Example 4: $P(n)$ denotes $1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$ for all nonnegative integers (this includes 0).

i) base case: prove that $P(0)$ is true: $2^0 = 1 = 2^1 - 1$

ii) induction hypothesis is to assume $P(k)$: $1 + 2 + 2^2 + \dots + 2^k = 2^{k+1} - 1$
and show: $P(k+1)$: $1 + 2 + 2^2 + \dots + 2^k + 2^{k+1} = 2^{((k+1)+1)} - 1 = 2^{k+2} - 1$

PROOF:

add 2^{k+1} to both sides of the inductive hypothesis:

$$\begin{aligned} (1 + 2 + 2^2 + \dots + 2^k) + 2^{k+1} &= (2^{k+1} - 1) + 2^{k+1} \\ &= (2 * 2^{k+1}) - 1 && \text{factoring} \\ &= 2^{k+2} - 1 && \text{exponent defin} \end{aligned}$$

$P(k+1)$ is true when $P(k)$ is true, and therefore $P(n)$ is true for all nonnegative numbers.

An example with two variables (but only one induction variable):

Example 5: $P(n)$ denotes that for any real number r except 1 and any integer $n \geq 0$,

the summation of r^i for $i = 0$ to n equals $(r^{(n+1)} - 1) / r - 1$

i) base case: prove that $P(0)$ is true $(r^{(0+1)} - 1) / r - 1 = 1$ and $r^0 = 1$.

ii) induction hypothesis is to assume $P(k)$: the summation of r^i for $i = 0$ to k equals $(r^{(k+1)} - 1) / r - 1$

and show: $P(k+1)$: the summation of r^i for $i = 0$ to $k+1$ equals $(r^{(k+2)} - 1) / r - 1$

PROOF:

the summation of r^i for $i = 0$ to $k+1$ equals the summation of r^i for $i = 0$ to k + $r^{(k+1)}$

$$\begin{aligned} &= (r^{(k+1)} - 1) / r - 1 + r^{(k+1)} \\ &= (r^{(k+1)} - 1) / r - 1 + (r^{(k+1)} * (r-1)) / r-1 \\ &= ((r^{(k+1)} - 1) + (r^{(k+1)} * (r-1))) / r-1 \\ &= ((r^{(k+1)} - 1) + (r^{(k+1)} * r) - r^{(k+1)}) / r-1 \\ &= ((r^{(k+1)} * r) - 1) / r - 1 \\ &= r^{(k+2)} - 1 / r - 1 \end{aligned}$$

$P(k+1)$ is true when $P(k)$ is true, and therefore $P(n)$ is true for all natural numbers.

Thus far, we have been using **weak** induction in our proofs. There is a variation called **strong** induction. Rather than assume that $P(k)$ is true to prove that $P(k+1)$ is true, we assume that $P(i)$ is true for all i where the (basis of induction) $\leq i \leq k$. From this assumption, we prove $P(k+1)$. It's stronger in the sense that we are allowed to come to the same conclusion while assuming more, but the assumption is a natural one based on our understanding of weak induction. In fact, weak induction is a special case of strong induction.

Consider the domino analogy. We still need to prove that the $n+1$ domino will fall, but instead of just assuming the previous one has fallen, we can assume that all the previous ones have fallen, which is correct - they did all fall.

Strong or Complete Induction:

- i) Prove $P(\text{base})$ is true
- ii) Assume $P(\text{base}), P(\text{base}+1) \dots P(k)$ is true, and prove that $P(k+1)$ is true.

Example 6: $P(n)$ denotes that all positive integers n have a prime factorization, i.e., n can be written as the product of primes.

- i) base case: prove that $P(1)$ is true $1 = 1 * 1$
- ii) induction hypothesis is to assume $P(i)$: for all positive integers i where $1 < i \leq k$, i has a prime factorization;

and show $P(k+1)$: $k+1$ has a prime factorization.

PROOF:

If $k+1$ is a prime, then it has the obvious prime factorization $k+1 * 1$. If $k+1$ is not a prime, then by the definition of primality, it must be true that for some a & b , $a * b = k+1$. Clearly, $a \leq k$ and $b \leq k$. But by the inductive hypothesis, both a and b have a prime factorization too. Thus $k+1$ is the product of prime factors a & b , proving that $k+1$ has a prime factorization.

$P(k+1)$ is true when $P(i)$ is true, where $i \leq k$, and therefore $P(n)$ is true for all natural numbers.

Strong induction is often used to prove that a sequence of numbers has a particular property.

Example 7:

$P(n)$ denotes the following: If b_1, b_2, b_3, \dots is a sequence defined by the following:
 $b_0 = 1, b_1 = 2, b_2 = 3, b_k = b_{k-3} + b_{k-2} + b_{k-1}$ for all integers $k \geq 3$; then, b_n is
 $\leq 3^n$ for all integers $n \geq 0$.

i) base case: prove that $P(0), P(1)$ and $P(2)$ are true. (Note: in sequence problems, you must prove all given base cases.)

$$b_0 = 1 \text{ which is } \leq 3^0$$

$$b_1 = 2 \text{ which is } \leq 3^1$$

$$b_2 = 3 \text{ which is } \leq 3^2$$

ii) induction hypothesis is to assume $P(i)$ for $k > 2$: for all positive integers i where
 $1 \leq i < k, b_i \leq 3^i$,

and show that $b_k \leq 3^k$.

PROOF:

The definition of the sequence tells us that $b_{k-3} + b_{k-2} + b_{k-1}$ for all integers $k \geq 3$.
Since $k > 2, 0 \leq k-3 \leq k$, and so by the inductive hypothesis, $b_{k-1} \leq 3^{k-1}, b_{k-2} \leq 3^{k-2}$
and $b_{k-3} \leq 3^{k-3}$. If we add these inequalities and apply the laws of basic algebra, we
get

$$b_{k-3} + b_{k-2} + b_{k-1} \leq 3^{k-1} + 3^{k-2} + 3^{k-3}$$

$$3^{k-1} + 3^{k-2} + 3^{k-3} \leq 3^{k-1} + 3^{k-1} + 3^{k-1}$$

$$3^{k-1} + 3^{k-1} + 3^{k-1} = 3 * 3^{k-1} = 3^k$$

And thus by substitution, $b_k \leq 3^k$ which is what we set out to prove.

$P(k)$ is true when $P(i)$ is true, where $i < k$, and therefore $P(n)$ is true for all natural numbers.

Now we look at an additional example presented to expand your conception of the application of induction:

Example 8: A jigsaw puzzle consists of a number of pieces. Two or more pieces with matched boundaries can be put together to form a "big" piece. To be more precise, we use the term *block* to refer to either a single piece or a number of pieces with matched boundaries that are put together to form a "big" piece. Thus, we can simply say that blocks with matched boundaries can be put together to form another block. Finally, when all pieces are put together as one single block, the jigsaw puzzle is solved. Putting 2 blocks together with matched boundaries is called one move. We shall prove (using strong induction) that for a jigsaw puzzle of n pieces, it will always take $n-1$ moves to solve the puzzle.

i) base case: prove that $P(1)$ is true: For a puzzle with 1 piece, it does not take any moves to solve it.

ii) induction hypothesis is to assume $P(i)$ where $1 \leq i \leq k$: for a puzzle with i pieces, it takes $i-1$ moves to solve the puzzle; and show that for a puzzle with $k+1$ pieces, it takes k moves to solve the puzzle.

PROOF:

Consider the puzzle with $k+1$ pieces. For the last move that produces the solution to the puzzle, we have two blocks: one with n_1 pieces and the other with n_2 pieces, where $n_1 + n_2 = k + 1$. These two blocks will then be put together to solve the puzzle. According to the induction hypothesis, it took $n_1 - 1$ moves to put together the one block, and $n_2 - 1$ moves to put together the other block. Including the last move to unite the two blocks, the total number of moves is equal to $[(n_1 - 1) + (n_2 - 1)] + 1 = (k + 1) - 1 = k$

$P(k+1)$ is true when $P(i)$ is true, where $i \leq k$, and therefore $P(n)$ is true for any puzzle size.

The last topic to discuss concerning induction is:

The Law of Bad Proofs:

You can prove anything you want if your proof is wrong.

In some ways, induction seems like it can prove any property about anything. But you have to watch out for subtle flaws in your thinking. Consider the following:

$P(n)$ denotes that a set of n horses are all the same color.

base case: prove that $P(1)$ is true: If X is a set of 1 horse, then all the horses in X are the same color.

induction hypothesis is to assume $P(k)$ is true: every set of k horses are the same color. and show $P(k+1)$: every set of $k+1$ horses are the same color.

PROOF:

Suppose X is a set of $k+1$ horses. To show that all the horses in X are the same color, it's enough to show that if

h_1 is in X and h_2 is in X

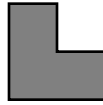
then h_1 is the same color as h_2 . If we can prove this, we are done because either h_1 or h_2 is in a set of k horses, and we know that a set of k horses are all the same color.

Let $X_1 = X - h_1$ and $X_2 = X - h_2$

X_1 and X_2 have k horses and by the inductive hypothesis, these k horses are all the same color. So, if we take a horse z which is a horse in the intersection of X_1 and X_2 (that being one of the horses that X_1 and X_2 have in common), we know that h_1 must be the same color as z , and h_2 must be the same color as z ; therefore, h_1 is the same color as h_2 . We have proven that all horses are the same color.

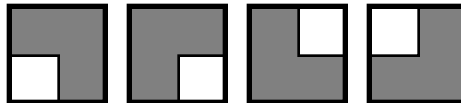
What's wrong with this?

Show that any 2^n by 2^n grid can be tiled using “L” shaped pieces (such as the one below) leaving any one square untiled.



Solution: Proof by induction on n .

Basis: It is easy to verify the case for $n = 1$ by exhaustively checking all possibilities:



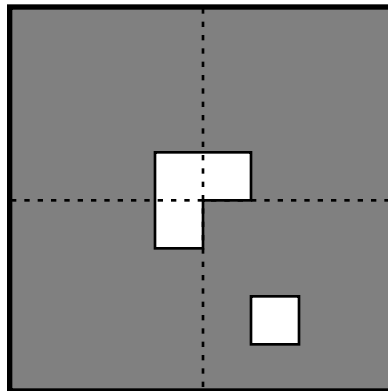
Induction:

Prove: A 2^{k+1} by 2^{k+1} grid can be tiled as described above.

Assuming: Any 2^k by 2^k grid can be tiled.

We begin with a 2^{k+1} by 2^{k+1} grid. Divide this grid into four sub-grids, each of size 2^k by 2^k . By the inductive hypothesis, each of these grids can be tiled leaving any one square empty.

Tile three of the four sub-grids so that the empty squares are adjacent and form an “L” shaped hole. The fourth sub-grid can be tiled however we please.



Now, simply fill the “L” shaped hole with another tile. Thus a 2^{k+1} by 2^{k+1} grid can be tiled, leaving any one square blank. This completes the proof.

Bibliography

G. Pólya, *Induction and Analogy in Mathematics*, Princeton, NJ: Princeton University Press: 1954.

D. Solow, *How to Read and Do Proofs*, New York: Wiley, 1982.

I.S. Sominskii, *Method of Mathematical Induction*, New York: Blaisdell, 1961.

Some Useful Formulas

Here are some formulas for sequences that are great for practicing proofs by induction. You will also find these formulas useful later in the quarter when we discuss recursion and recurrence relations. The ones we have proven in this handout are included below.

- $1 + 2 + 3 + \dots + n = n(n+1) / 2$
- $1 + 3 + 5 + \dots + (2n-1) = n^2$
- $1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$
- $\sum_{i=0}^n r^i = (r^{n+1} - 1) / r - 1$
- $1^2 + 2^2 + 3^2 + \dots + n^2 = [n(n+1)(2n+1)] / 6$
- $1^3 + 2^3 + 3^3 + \dots + n^3 = [n(n+1) / 2]^2$
- $1*2 + 2*3 + \dots + n(n+1) = n(n+1)(n+2) / 3$
- $1/1*2 + 1/2*3 + \dots + 1/n(n+1) = n / (n+1)$
- $1^2 + 3^2 + 5^2 + \dots + (2n+1)^2 = (n+1)(2n+1)(2n+3) / 3$

Historical Notes

The first known use of mathematical induction was in the work of the 16th-century mathematician Francesco Maurolico (1494-1575). In his book *Arithmeticonum Libri Duo*, he presented a variety of properties of the integers together with proofs of these properties. He used induction to prove some of these properties, the first one being the proof that the sum of the first n odd integers is n^2 . The first formal explanation of mathematical induction was presented by Augustus DeMorgan (1806-1871) in 1838. This is also the first time the term "induction" was used in this context.

A Catalog of Proof Techniques

- 1.Proof by example: The author gives only the case $n=2$ and suggests that it contains most of the ideas of the general proof.
- 2.Proof by intimidation: "Trivial."
- 3.Proof by vigorous handwaving: Works well in a classroom or seminar setting.
- 4.Proof by cumbersome notation: Best done with at least four alphabets and numerous subscripts.
- 5.Proof by exhaustion: A long sequence of true and perhaps meaningless syntactically related statements.
- 6.Proof by omission: "The reader may easily supply the details;" "The other 47 cases are analogous;" etc.
- 7.Proof by obfuscation: A long sequence of true and perhaps meaningless syntactically related statements.
- 8.Proof by wishful citation: The author cites the negation, converse, or generalization of some theorem that appears in the literature.
- 9.Proof by funding: How could three different government agencies be wrong?
- 10.Proof by eminent authority: "I saw Knuth in the lounge and he said it

was probably NP-complete."

11.Proof by personal communication: "Eight-dimensional colored cycle stripping is NP-complete [Motwani, personal communication]."

12.Proof by reduction to the wrong problem: "To see that infinite dimensional colored cycle stripping is decidable, we reduce it to the halting problem."

13.Proof by reference to inaccessible literature: The author cites a simple corollary of a theorem to be found in a privately circulated memoir of the Slovenian Philological Society,1883.

14.Proof by importance: A large body of useful consequences all follow from the proposition in question.

15.Proof by accumulated evidence: Long and diligent search has not revealed a counterexample.

16.Proof by cosmology: The negation of the proposition is unimaginable or meaningless. Popular for proofs of the existence of God.

17.Proof by mutual reference: In reference A, Theorem 5 is said to follow from Theorem 3 in reference B, which is shown to follow from Corollary 6.2 in reference C, which is an easy consequence of Theorem 5 in reference A.

18.Proof by metaproof: A method is given to construct the desired proof. The correctness of the method is proved by any of the techniques on this page.

19.Proof by picture: A more convincing form of proof by example. Combines well with proof by omission.

20.Proof by vehement assertion: It is useful to have some kind of authority relation to the audience.

21.Proof by ghost reference: Nothing even remotely resembling the cited theorem appears in the reference given.

22.Proof by forward reference: Reference is usually to a forthcoming paper of the author, which is often not as forthcoming as the first paper.

23.Proof by semantic shift: Some of the mathematics' standard but inconvenient definitions are changed for the statement of the result.

24.Proof by appeal to intuition: Cloud-shaped drawings frequently help here.