

## Module 3: Proofs

Reading from Textbook (Johnsonbaugh): Chapter 2 Proofs

### Introduction

In previous modules, we saw several proof techniques, including algebraic proof, counter-example proof, direct proof, contrapositive proof, and proof of if-and-only-if statements.

In this module, we discuss enumeration proof, provide some more examples of contrapositive proof, and then discuss a similar proof by **contradiction**. We will compare/contrast the two methods contrapositive/contradiction. We then study a very important proof technique, called **induction**. This proof method has wide applicability in computer science. For example, proof by induction may be used to prove the correctness of program loops, algorithms, and recursive algorithms.

### Contents

1. Enumeration Proof (Exhaustive Proof)
2. Proof by Contrapositive: More Examples
3. Proof by Contradiction
4. Induction
5. Strong Induction

## Enumeration Proof

This is a proof that involves several cases, and the proof is made for each case exhaustively.

**Example:** Let the domain of  $m$  and  $n$  be positive integers. Prove that there are no values of  $m$  and  $n$  to satisfy

$$5m + 8n = 24$$

**Proof:** We first limit the range for  $m$  and  $n$ . Clearly,  $m \in \{1,2,3,4\}$  and  $n \in \{1,2,3\}$ .

(If  $m \geq 5$ , then  $5m \geq 25$ . Similarly, if  $n \geq 4$ , then  $8n \geq 32$ .)

We compute  $5m + 8n$  for each case and see that the sum will not equal 24.

	$n = 1$	$n = 2$	$n = 3$
$m = 1, \quad 5m = 5$	13	21	29
$m = 2, \quad 5m = 10$	18	26	34
$m = 3, \quad 5m = 15$	23	31	39
$m = 4, \quad 5m = 20$	28	36	44



**Example:** Let the domain of  $n$  be positive integers. Prove that

If  $n$  is not divisible by 5, then  $n^2$  is not divisible by 5.

**Proof:** Suppose  $n$  is not divisible by 5. Then  $n = 5k + r$ , for some integer  $k$  and some non-zero remainder  $r \in \{1,2,3,4\}$ . So,

$$n^2 = (5k + r)^2 = 25k^2 + 10kr + r^2 = 5(5k^2 + 2kr) + r^2.$$

So, dividing  $n^2$  by 5 will have a remainder:  $r^2 \bmod 5$ . Let us consider each value of  $r$  to show that the remainder will be non-zero in every case.

$r$	$r^2$	$r^2 \bmod 5$ (remainder)
1	1	1
2	4	4
3	9	4
4	16	1

The remainder is non-zero in every case. Therefore,  $n^2$  is not divisible by 5.



## Contrapositive Proof

Recall that if we need to prove

$$\underbrace{p}_{\text{hypothesis}} \rightarrow \underbrace{q}_{\text{conclusion}}$$

we turn it around and prove the equivalent contrapositive form:

$$\neg q \rightarrow \neg p.$$

We start by assuming that  $\neg q$  is true. (That is, the original conclusion  $q$  is false.)

Then we conclude that  $\neg p$  is true. (That is, the original hypothesis  $p$  is false.)

We saw this method of proof earlier (module 2 logic). Here we give a few additional examples of it, and then later compare/contrast it with proof by contradiction.

**Example:** Prove that for any two positive integers  $x$  and  $y$ ,

If  $xy \geq 65$ , then at least one of the two numbers must be  $\geq 9$ .

The contrapositive equivalent form of the above statement is:

If neither number is  $\geq 9$ , then the product will not be  $\geq 65$ .


Suppose neither number is  $\geq 9$ . That is,  $x \leq 8$  and  $y \leq 8$ . Then,  $xy \leq 64$ . 

**Example:** Prove that for any positive integer  $n$ ,

If  $n^2$  is not divisible by 5, then  $n$  is not divisible by 5.

A direct proof of this is difficult. That is, suppose we start by assuming that  $n^2$  is not divisible by 5. Then, it is hard to conclude that  $n$  is not divisible by 5. When a direct proof is not possible (or convenient), we try contrapositive proof. That is, we prove

If  $n$  is divisible by 5, then  $n^2$  is divisible by 5.

Suppose  $n$  is divisible by 5, so  $n = 5k$ , for some integer  $k$ . Then,  $n^2 = 25k^2 = 5(5k^2)$ . This means  $n^2$  is divisible by 5. 

## Proof by Contradiction

Suppose we have a number of facts, and want to prove some conclusion  $S$  is true. We start by supposing to the contrary that  $S$  is false. That is,  $\neg S$  is true. Then, we show this will lead to a *contradiction*. (That is, it will negate some earlier known facts.) Therefore, we conclude  $S$  must be true.

**Definition:** A *rational* number  $x$  is a number that may be expressed as the ratio of two integers  $i$  and  $j$ ,  $x = \frac{i}{j}$ . A number that cannot be expressed in such a way is *irrational*.

**Example:** Given a rational number  $x$  and an irrational number  $y$ . Prove that  $(x + y)$  is irrational.

Proof: Suppose, to the contrary, that  $(x + y)$  is rational. Then, there are integers  $p$  and  $q$  such that

$$x + y = \frac{p}{q}$$

And we know from earlier given fact that  $x$  is rational. So,  $x = \frac{i}{j}$  for some integers  $i$  and  $j$ . Then,

$$y = (x + y) - x = \left(\frac{p}{q}\right) - \left(\frac{i}{j}\right) = \frac{pj - iq}{qj} = \text{rational}.$$

This contradicts the earlier fact that  $y$  is irrational. Therefore,  $(x + y)$  must be irrational. ■

**Example (Pigeonhole Principle):** Suppose  $n$  pigeons fly into  $k$  pigeonholes, where  $k < n$ . Prove that some holes must have more than one pigeon.

**Proof:** Suppose, to the contrary, that no hole has more than one pigeon. Since there are  $k$  holes, then there are at most  $k$  pigeons. And we know  $k < n$ . This contradicts the fact that there are  $n$  pigeons. Therefore, there must be some holes with more than one pigeon. ■

### Comparison of Contrapositive versus Contradiction Methods:

The contrapositive proof and contradiction proof are similar in that they both start with negation of conclusion. But proof by contradiction has two new characteristics:

1. We are free to use some of the earlier facts, in addition to negation of conclusion.
2. Proof by contradiction does not necessarily deal with If-Then type of statement, as illustrated by the next example.

**Example:** Prove  $\sqrt{2}$  is irrational.

**Proof:** Suppose to the contrary, that  $\sqrt{2}$  is rational. This means there are integers  $i$  and  $j$  such that

$$\sqrt{2} = \frac{i}{j}$$

We may assume that  $i$  and  $j$  are reduced so they have no common factor. (For example, if the ratio is  $4/6$ , then it can be reduced to  $2/3$ .) Then,

$$2 = \frac{i^2}{j^2}$$
$$i^2 = 2j^2 = \text{Even integer}$$

Earlier, we proved that if  $i^2$  is even, then  $i$  is even. So,  $i$  is even, which means

$$i = 2k, \text{ for some integer } k.$$

Then

$$j^2 = \frac{i^2}{2} = \frac{(2k)^2}{2} = 2k^2 = \text{Even integer}.$$

Again, since  $j^2$  is even, then  $j$  is even. That is,

$$j = 2m, \text{ for some integer } m.$$

So we conclude that both  $i$  and  $j$  are even. This contradicts the earlier fact the  $i$  and  $j$  have no common factor.

Therefore,  $\sqrt{2}$  is irrational.



**Example:** Let  $x_1, x_2, \dots, x_n$  be  $n$  real numbers, and let the average be

$$A = \frac{x_1 + x_2 + \dots + x_n}{n}$$

Use contradiction to prove that

$$S: (\exists i, (x_i \leq A)) \wedge (\exists j, (x_j \geq A))$$

(This is an exercise in formal proof, although it may appear obvious! We want to formally prove that at least one  $x$  value is  $\leq A$  and at least one  $x$  value is  $\geq A$ .)

Suppose to the contrary that  $S$  is false. That is, suppose  $\neg S$  is true.

$$\neg S: (\forall i, (x_i > A)) \vee (\forall j, (x_j < A))$$

In words, this says that either all elements are greater than  $A$ , **or** all elements are smaller than  $A$ . Let us consider each of the two cases separately:

1. Suppose  $\forall i, (x_i > A)$ . Then,

$$A = \frac{x_1 + x_2 + \dots + x_n}{n} > \frac{A + A + \dots + A}{n} = \frac{nA}{n} = A$$

This says  $A > A$ , which is obviously a contradiction.

2. Suppose  $\forall j, (x_j < A)$ . Then,

$$A = \frac{x_1 + x_2 + \dots + x_n}{n} < \frac{A + A + \dots + A}{n} = \frac{nA}{n} = A$$

This says  $A < A$ , which is also a contradiction.

So both cases lead to a contradiction. Therefore,  $S$  must be true. ■

Next, we study induction, which is one of the most important proof methods in discrete mathematics.

## Proof by Induction

Let  $P(n)$  be a predicate. We need to prove that for all integer  $n \geq 1$ ,  $P(n)$  is true.

We accomplish the proof by induction as follows:

1. (Induction Base) Prove  $P(1)$  is true.
2. (Induction Step) Prove that  $\forall n \geq 1$ ,  
$$\underbrace{P(n)}_{\text{hypothesis}} \rightarrow \underbrace{P(n+1)}_{\text{conclusion}}$$

Here is the reasoning how induction works:

We first prove  $P(1)$ .

Then, once the induction step has been proved  $\forall n \geq 1$ , it means

$$\begin{aligned} P(1) &\rightarrow P(2) \\ \therefore P(2) \end{aligned}$$

Again, by the induction step,

$$\begin{aligned} P(2) &\rightarrow P(3) \\ \therefore P(3) \end{aligned}$$

And so on.

There is an interesting analogy with dominoes. Suppose we have an infinite number of domino blocks, numbered  $1, 2, 3, \dots$ . Suppose they are arranged in close spacing such that if block  $n$  is knocked down (to the right), it will knock down block  $n + 1$ . And suppose block 1 is knocked down. That will knock down block 2, which in turn will knock down block 3, and so on. This chain-reaction is called *domino effect*.

**Example:** Use induction to prove that all integers of the type

$$P(n) = 4^n - 1$$

are divisible by 3, for all integers  $n \geq 1$ .

**Proof:** For the base,  $P(1) = 4 - 1 = 3$ , which is divisible by 3.

Now suppose for some  $n \geq 1$ ,

$$P(n) = 4^n - 1 \text{ is divisible by 3. (This is the hypothesis.)}$$

We will prove that will imply that


$$P(n + 1) = 4^{n+1} - 1 \text{ is also divisible by 3. (This is the conclusion.)}$$

**Proof of conclusion:**

$$P(n + 1) = 4^{n+1} - 1 = 4 * 4^n - 1 = 4 * 4^n - 4 + 3 = 4 \left( \underbrace{4^n - 1}_{\text{hypothesis}} \right) + 3$$

By hypothesis,  $4^n - 1$  is divisible by 3. So,  $4^n - 1 = 3k$  for some integer  $k$ . So,

$$P(n + 1) = 4 * 3k + 3 = 3(4k + 1).$$


Therefore,  $P(n + 1)$  is divisible by 3. 

**Example:** Prove by induction that the number of  $n$ -bit integers is  $2^n$ , for  $n \geq 1$ .

**Proof:** For the base,  $n = 1$ , the number of 1-bit integers is obviously  $2^1 = 2$ .

Now, suppose for some  $n \geq 1$ , the number of  $n$ -bit integers is  $2^n$ .

Then we will prove the number of  $(n+1)$ -bit integers is  $2^{n+1}$ .

To obtain  $(n+1)$ -bit integers, we can take each  $n$ -bit integer and extend it by one additional bit, which may be either 0 or 1. Therefore, the number of  $(n+1)$ -bit integers is twice the number of  $n$ -bit integers, thus  $2 * 2^n = 2^{n+1}$ . 



**Example:** Use induction to prove the *Arithmetic-Sum* formula:

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

Proof: For the base,  $n = 1$ ,

$$S(1) = 1 = \frac{1(2)}{2}$$

So the base is correct.

Suppose that for some  $n \geq 1$ , the formula is correct:

$$S(n) = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad (\text{Hypothesis})$$

We will prove that the formula is also correct for  $n+1$ :

$$S(n+1) = 1 + 2 + 3 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2} \quad (\text{Conclusion})$$

To prove the conclusion:

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



**Example:** A saving bank gives 5% yearly interest, compounded annually. Suppose initially, a deposit of \$1000 is made. Let  $F_n$  be the total amount accumulated after  $n$  years. To figure out the amount, it is convenient to first express  $F_n$  in terms of  $F_{n-1}$ , which is the amount at the end of the previous year.

$$F_n = \begin{cases} 1000, & n = 0 \\ 1.05 * F_{n-1}, & n \geq 1. \end{cases}$$

This recursive formulation is called a *recurrence equation*. (The first line is the base, and the second line is the recursive formula.)

We now need to solve this recurrence equation to find  $F_n$  directly in terms of  $n$ . One approach is to guess the solution, or claim what we believe the solution is, and then prove it correct by induction.

Let us prove by induction that the solution is

$$F_n = 1000 * (1.05)^n, \quad \forall n \geq 0.$$

(The student may wonder at this point how we guessed the solution in the first place. Later, we will see methods of finding the solution directly from the recurrence equation.)

**Proof:** For the base of induction,  $n = 0$ , the solution is  $F_0 = 1000 * (1.05)^0 = 1000$ . This is correct as given in the base of the recurrence equation.

Next, suppose the solution form is correct for some  $n \geq 0$ :


$$F_n = 1000 * (1.05)^n \quad (\text{hypothesis})$$

Then we will prove the solution will also be correct for  $n + 1$ :

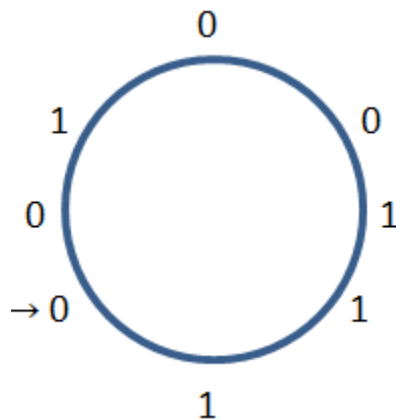
$$F_{n+1} = 1000 * (1.05)^{n+1} \quad (\text{conclusion})$$

To prove the conclusion:

$$\begin{aligned} F_{n+1} &= 1.05 * \underbrace{F_n}_{\text{hypothesis}} && (\text{from the recurrence equation}) \\ &= 1.05 * 1000 * (1.05)^n && (\text{from the hypothesis}) \\ &= 1000 * (1.05)^{n+1}. \end{aligned}$$

This completes the induction proof. 

**Example:** Suppose we have  $n$  0's and  $n$  1's distributed around a circle in any manner. (An example is shown in the following figure, for  $n = 4$ .) Prove by induction that it is always possible to find a starting point and make a complete cycle around the circle in clockwise direction while satisfying the following condition: **At any point during the cycle, the number of 0's that we have passed over will be at least as many as the number of 1's.** (A possible starting point is shown by an arrow in the figure.)



Note: This is not just a toy problem! It is similar to parenthesis-matching problem, which is applicable in parsing arithmetic expressions.

### Proof:

For induction base, problem of size  $n = 1$ , the circle has only one 0 and one 1. Obviously, we can start with the 0, and make the cycle to satisfy the required condition.

Now we will prove that for any  $n \geq 2$ , if it can be done for size  $n - 1$ , then it can also be done for size  $n$ .

Consider a circle with  $n$  0's and  $n$  1's. Find a 0 followed immediately by a 1 (in clockwise direction). Remove this 0-1 pair. Now we have a reduced problem with only  $(n - 1)$  0's and  $(n - 1)$  1's. By the hypothesis, we can find a starting point for this reduced circle. Now put back the 0-1 pair that was removed (in their original place). Obviously, the same starting point will still work for this original problem. (During the cycle, we will first hit the 0, and then immediately the 1, thus canceling each other.)



The reader is urged to apply this proof repeatedly to find the starting point on the above example. (The starting point is not always unique, although it is in this figure.)

**Question:** Will the proof still work if we simply find any 0 and any 1 (where 1 does not immediately follow 0) and remove this 0-1 pair to reduce the problem? The answer is no, the proof would not be valid anymore. Why? Explain.

**Example (Tiling Problem):** A *trominoe* is an L-shape piece with 3 squares, and in any orientation, as shown below.

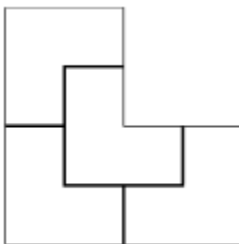


Consider a  $2^n \times 2^n$  board, with one of its quadrants missing. (We will call this a quad-deficient board.) That is, the board has only 3 quadrants, each of size  $2^{n-1} \times 2^{n-1}$ .

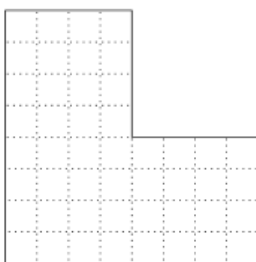
Prove by induction that a  $2^n \times 2^n$  quad-deficient board can be covered by some number of trominoe pieces. (By covering, we mean every cell is covered by a trominoe, and the trominoe pieces do not overlap.)

**Proof:** For  $n = 1$ , the board is the shape of a single trominoe and it can be covered by a single trominoe. So the base is proved.

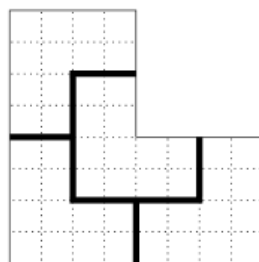
For  $n \geq 2$ , we will prove that if a  $2^{n-1} \times 2^{n-1}$  quad-deficient board can be covered, then a  $2^n \times 2^n$  quad-deficient board can also be covered. Consider a  $2^n \times 2^n$  board. The board can be divided into four quad-deficient boards of size  $2^{n-1} \times 2^{n-1}$ , as shown below. By the hypothesis, each of the four smaller boards can be covered. Therefore, the  $2^n \times 2^n$  board can also be covered. This completes the induction proof.



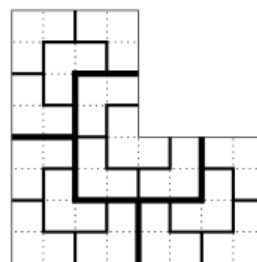
The algorithm suggested by this proof uses a strategy called *divide-and-conquer*, where a problem is solved by dividing it into a number of smaller problems of the same type. An illustration of the covering produced by this algorithm is shown below for a  $2^3 \times 2^3$  quad-deficient board.



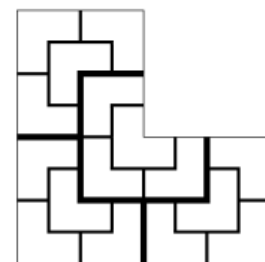
Initial Board



Top-Level Divide



Next-Level Divide



Polished Final Tiling

**Note:** The above tiling problem is similar in flavor to some real-world problems, such as VLSI layout problem. (VLSI stands for Very Large Scale Integration.) This problem is to pack as many components as possible on a wafer rectangle with certain area and with some additional constraints.

**Example:** Prove by induction that for all integers  $n \geq 1$ ,

$$2^n > n.$$

**Proof:** For the base,  $n = 1$ ,  $2^1 > 1$ , so the base is correct.

Now suppose for some  $n \geq 1$ ,

$$2^n > n. \quad (\text{Hypothesis})$$

Then we will prove

$$2^{n+1} > n + 1. \quad (\text{Conclusion})$$

Observe  $2^{n+1} = 2(2^n)$ , and use the hypothesis  $(2^n > n)$ , to get:


$$2^{n+1} = 2(\underbrace{2^n}_{\text{hypothesis}}) > 2(n)$$

And

$$2(n) \geq n + 1, \text{ when } n \geq 1.$$

Therefore,

$$2^{n+1} > n + 1.$$

This proves the conclusion. 

The next problem is a classic example of induction, found in many textbooks, which dates back to the time when the price of US domestic stamp was 8 cents! Suppose the post office wanted to maintain only two types of stamps: 5-cent stamps and 3-cent stamps, with the brilliant idea that this will work for any postage amount forever!

**Example (Stamps):** Prove by induction that any postage of  $n$  cents, for  $n \geq 8$ , may be achieved with only 5-cent stamps and 3-cent stamps. This may be expressed symbolically as follows, where  $n, A$ , and  $B$  are all integers.

$$\forall n \geq 8, \exists A \geq 0 \exists B \geq 0, \\ n = 5A + 3B.$$

Note  $A$  is the number of 5-cent stamps, and  $B$  is the number of 3-cent stamps. (Obviously,  $A$  and  $B$  must be non-negative.)

Proof: For the base,  $n = 8$ , we see it is correct:

$$8 = 5 + 3$$

Now suppose for some  $n \geq 8$ ,

$$n = 5A + 3B \quad (1)$$

for some non-negative integers  $A$  and  $B$ . Then, we will prove that by manipulating the postage for  $n$ , we can achieve  $n + 1$  postage. That is, we will prove

$$n + 1 = 5A' + 3B' \quad (2)$$

for some non-negative integers  $A'$  and  $B'$ . How do we get from  $n$  to  $n + 1$ ? We need to take away some stamps from the postage for  $n$  and put in some other stamps in such a way that the net change is  $+1$ . There are two transformations that come to mind:

- Case 1: If  $B \geq 3$ :  
Then take away three of 3-cent stamps and add two 5-cent stamps. That is,  
$$n + 1 = 5(A + 2) + 3(B - 3)$$
  
The net change is  $-9 + 10 = +1$ , therefore changing the postage amount from  $n$  to  $n + 1$ .
- Case 2: If  $A \geq 1$ :  
Take away one 5 cent-stamp and add two 3-cent stamps. That is,  
$$n + 1 = 5(A - 1) + 3(B + 2)$$
  
The net change is  $-5 + 6 = +1$ .

To complete the proof, we need to argue that one of the two cases will always apply. Suppose, to the contrary, that neither case applies for some  $n$ . If neither case applied, then  $(A = 0 \wedge B \leq 2)$ , thus  $n \leq 6$ . This contradicts the fact that  $n \geq 8$ . Therefore, one of the two cases must always apply. (The reader may note that the reasoning we just applied was a proof by contradiction!) ■

**Example:** We want to prove the following program computes and returns  $\log_2 n$ , assuming that the input parameter  $n$  is an integer power of 2.

```

Int Compute (int  $n$ ) {
 $p = 0$ ;  $m = n$ ;
while ( $m > 1$ ) {
     $p = p + 1$ ;  $m = \frac{m}{2}$ ;
}
return ( $p$ )
}

```

1. First use induction to prove that after the  $k^{th}$  iteration of the while loop,

$$p = k, \quad m = \frac{n}{2^k} \quad (\text{Loop Invariant})$$

(These relations are called loop-invariant.)

2. Then conclude that the return value of the program is  $\log_2 n$ .

**Proof:** The induction is on the number of iteration  $k$ . Since  $k = 1$  represents the results after the first iteration of the while loop, we will back-up and use  $k = 0$  to represent the situation after the initialization and just before the first iteration.

For induction base,  $k = 0$ , the result after the initialization and just before the first iteration is  $p = 0$ ,  $m = \frac{n}{2^0} = n$ . So the base is correct.

Now suppose after iteration  $k$  of the while loop, for some  $k \geq 0$ ,

$$p = k, \quad m = \frac{n}{2^k}$$

Then the next iteration will increment  $p$  by 1, and divide  $m$  by 2. So the result after iteration  $k + 1$  will be:

$$p = k + 1, \quad m = n/2^{k+1}$$

This completes the induction proof. So, the Loop Invariant is proved for all  $k$ .

At the end, when the while loop terminates,  $m = 1$ . So,

$$p = k, \quad 1 = n/2^k$$

This means  $n = 2^k = 2^p$ . Therefore,  $p = \log_2 n$ . And this is the value returned by the program. ■

## Strong Induction:

The method of induction we used so far is called *simple induction* (or mathematical induction). Suppose we want to prove  $P(n)$  for all  $n \geq 1$ .

### **Simple Induction:**

1. Prove  $P(1)$  is true.
2. Prove that for any  $n \geq 2$ ,

$$\underbrace{P(n-1)}_{\text{hypothesis}} \rightarrow \underbrace{P(n)}_{\text{conclusion}}$$

In the induction step, we rely only on the truth of  $\underbrace{P(n-1)}_{\text{hypothesis}}$  to prove  $\underbrace{P(n)}_{\text{conclusion}}$ .

Now, let us examine the method of *strong induction*.

### **Strong Induction:**

First prove a number of bases cases.

Then, to prove  $P(n)$ , we are free to use the truth of any of the previous values:

$$P(1), P(2), \dots, P(n-1)$$

For our first example, we use the well-known Fibonacci sequence, which is a sequence  $F_1, F_2, F_3, \dots$  defined recursively as follows:

$$F_n = \begin{cases} 1, & n = 1, 2 \\ F_{n-1} + F_{n-2}, & n \geq 3. \end{cases}$$

Historically, Fibonacci introduced this sequence to study the birth rate of rabbits. (For simplicity, no death occurs!) Suppose a farm receives a pair of newly-born rabbits at the beginning. Suppose at the end of each month, each pair of rabbits that is at least 2-month old gives birth to a new pair of rabbits. Let  $F_n$  be the total number of pairs at the end of month  $n$ . Then, this number will equal to:

- The number of pairs at the end of the previous month,  $F_{n-1}$ ; plus:
- The number of newly born pairs, which equals the number of pairs that existed two months ago,  $F_{n-2}$ . (These are the rabbits that are now at least 2-month old).

Therefore,  $F_n = F_{n-1} + F_{n-2}$ .



To get a feel of how fast this function grows, let us use the recurrence equation to compute  $F_n$  for  $n = 1, 2, \dots, 12$ . (From this tabulation, observe the farm will have 144 pairs of rabbits at the end of one-year period!)

$n$	1	2	3	4	5	6	7	8	9	10	11	12
$F_n$	1	1	2	3	5	8	13	21	34	55	89	144

**Example:** Use induction to prove that the solution of Fibonacci sequence has the following upper bound:

$$F_n < 2^n, \quad \forall n \geq 1.$$

**Proof:** First we prove two base cases:

- $n = 1: F_1 = 1 < 2^1 = 2$
- $n = 2: F_2 = 1 < 2^2 = 4$

To prove the bound for  $F_n$  for any  $n \geq 3$ , suppose

$$F_m < 2^m \text{ for all } m < n.$$

In particular, suppose

$$\begin{aligned} F_{n-1} &< 2^{n-1} \\ F_{n-2} &< 2^{n-2} \end{aligned}$$

(This is why we needed two base cases.)

Then,

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &< 2^{n-1} + 2^{n-2} \end{aligned} \quad (\text{by hypothesis})$$

$$= 2^n \left( \frac{1}{2} + \frac{1}{2^2} \right)$$

$$= 2^n \left( \frac{1}{2} + \frac{1}{4} \right) = 2^n \left( \frac{3}{4} \right) < 2^n.$$



Next, let us use strong induction to prove the postage problem we saw earlier.

**Example:** Prove by strong induction that any postage amount of  $n$  cents, for  $n \geq 8$ , may be achieved with only 5-cent stamps and 3-cent stamps. This may be expressed symbolically as follows, where  $n, A$ , and  $B$  are all integers.

$$\forall n \geq 8, \exists A \geq 0 \exists B \geq 0, \\ P(n): \quad n = 5A + 3B.$$

**Proof:** The basic idea is to first prove a number of base cases. Then, in the induction step for proving  $P(n)$ , we will use the truth of  $P(n - 5)$  and simply add a 5-cent stamp to the postage for  $n - 5$  to achieve the postage for  $n$ .

Bases Cases (5 cases):

$n = 8$	$8 = 1 * 5 + 1 * 3$
$n = 9$	$9 = 0 * 5 + 3 * 3$
$n = 10$	$10 = 2 * 5 + 0 * 3$
$n = 11$	$11 = 1 * 5 + 2 * 3$
$n = 12$	$12 = 0 * 5 + 4 * 3$

Now, to prove  $P(n)$  is true for any  $n \geq 13$ , suppose that

$$P(m) \text{ is true } \forall m < n, \quad 8 \leq m < n. \quad (\text{This is strong hypothesis.})$$

Since  $n \geq 13$ , then  $n - 5 \geq 8$ . So we know from the hypothesis that  $P(n - 5)$  is true. (This is why we needed 5 base cases.) So,

$$(n - 5) = 5A + 3B$$

for some non-negative integers  $A$ , and  $B$ .

Then, to achieve the postage for  $n$ , simply add a 5-cent stamp to the postage for  $(n - 5)$ . That is,

$$n = 5(A + 1) + 3B.$$

This completes the induction proof.

Note: An alternative proof is to first prove only 3 base cases (8, 9, 10). Then, for the induction step, simply add a 3-cent stamp to the postage for  $n - 3$  to achieve the postage for  $n$ .



**Illustration:** Let us see how the postage for  $n = 26$  is found by repeated application of the above induction proof.

To find the postage for $n = 26$	Add a 5-cent stamp to the postage for $n = 21$
To find the postage for $n = 21$	Add a 5-cent stamp to the postage for $n = 16$
To find the postage for $n = 16$	Add a 5-cent stamp to the postage for $n = 11$
To find the postage for $n = 11$	Use the base case: $11 = 1 * 5 + 2 * 3$

Therefore,  $26 = 4 * 5 + 2 * 3$ .



Example: Consider the following recurrence equation, where  $n$  is an integer power of 2.

$$F_n = \begin{cases} 4, & n = 1 \\ 8, & n = 2 \\ F_{\frac{n}{2}} + F_{\frac{n}{4}} + n, & n \geq 4 \end{cases}$$

First, use the recurrence equation to compute and tabulate  $F_n$  for  $n = 1, 2, 4, 8, 16, 32$ .

$n$	1	2	4	8	16	32
$F_n$	4	8	16	32	64	128

Prove by induction (strong induction) that the solution of the recurrence equation is:

$$F_n = 4n, \quad n \geq 1.$$

**Proof:** For the two base cases:

- $n = 1$ :  $F_1 = 4 = 4n$
- $n = 2$ :  $F_2 = 8 = 4n$ .

Now, to prove for any  $n \geq 4$ , we assume that

$$F_m = 4m, \quad \forall m < n. \quad (\text{strong hypothesis})$$

Then we will prove that  $F_n = 4n$ . (conclusion)

$$\begin{aligned} F_n &= F_{\frac{n}{2}} + F_{\frac{n}{4}} + n \\ &= 4\left(\frac{n}{2}\right) + 4\left(\frac{n}{4}\right) + n \quad (\text{by hypothesis}) \\ &= 2n + n + n = 4n. \end{aligned}$$

