1 Propositions, Theorems and Proofs

In computer science we prove statements. Such statements need to be expressed/stated precisely.

A proposition is a statement that is either true or false.

A theorem is a proposition along with a proof of its correctness.

Every proposition is true or false with reference to a space we first define axiomatically and then build on by establishing more theorems.

An axiom is a proposition that is assumed to be true (no proof is required).

For example, Peano's axioms, on whose inductive proofs are based define natural (non negative) numbers. The set of natural (or non-negative integers) numbers is also denoted by N.

Axiom 1 (Peano). 0 is a natural number.
Axiom 2 (Peano). If n is a natural number, then its successor $s(n)$, which we prefer to write as $n+1$ is also a natural number.

Theorems in mathematics are true because the space these theorems apply to are based on simple axioms that are usually true.

The $\forall$ quantifier is also called the **universal quantifier**. It means **"for all"**. The $\exists$ quantifier is also called the **existential quantifier** and it means **there exist(s)**.

Proposition 1 *$\forall n \in N$, n^2+7 is prime.*

Symbol $\in$ is the **belongs to** set membership symbol. N is the set of natural (non negative integer) numbers.

This proposition states that for all natural (non-negative) numbers $n = 0, 1, \ldots$, the number n^2+7 is a prime number, i.e. it is a number divisible only by 1 and itself. This proposition can be easily shown to be false by counterexample. For $n = 3$, $n^2 + 7 = 3^2 + 7 = 16$ and one divisor of 16 other than 1 and 16, is 2. Therefore 16 is not a prime number, it is in fact a composite number and therefore this simple counterexample shows that Proposition 1 is false because it is not true for $n = 3$.

Proposition 2 *$\exists n \in N$ such that n^2+7 is prime.*

In order to prove that Proposition 2 is true, we only need prove it for a single value of n. For $n = 2$, we can easily establish that $2^2 + 7 = 11$ is a prime number. Proposition 2 is not, however, very interesting.
$X \Rightarrow Y$ is also known as implication and can be stated otherwise as "X implies Y".

2 How to use induction

Peano's axioms defined earlier cannot be used to prove that any property holds for all (natural) integers n. Induction is a principle (or proof technique) that can be used to prove theorems that depend on a variable that runs through the natural numbers (non-negative integers).

(Base Case) If you can prove that some property is true for 0,

(Inductive Step) and you can prove that "if this property is true for any (natural number) i, then it is also true for $i + 1$"

(Conclusion) then, **you have proved that the property is true for all the natural numbers** $n = 0, 1, 2, \ldots$.

This is summarized in the following axiom.

Axiom 3 (Induction). For any predicate P, if

- $P(0)$
- and $\forall n \in N\ P(n) \Rightarrow P(n+1)$,
- then $\forall n \in N$, $P(n)$.

Showing $P(0)$, i.e. that $P(0)$ is true, is the **base case**. The proof that $P(n)$ implies $P(n+1)$ is the **inductive step**. In the inductive step we assume that $P(n)$ is true. The assumption that $P(n)$ is true is called **inductive hypothesis**.

Axiom 3 in other words states the following, quite reasonable, observation.

- If I can prove $P(0)$ i.e. that $P(0)$ is true (BASE CASE),
- and show that $P(n)$ implies $P(n+1)$ for all n (INDUCTIVE STEP),
- then I have shown that $P(n)$ is true for all n.

2.1 Setting-up induction

The first step in induction is to identify in a proposition a predicate that depends on a natural-valued variable and also that same natural-valued variable). An example proposition is given below. Let $S_k = 0^k + 1^k + 2^k + \ldots + n^k$ for any integer $k > 0$. We also write $S_k = \sum_{i=0}^{n} i^k$. The latter term $\sum_{i=0}^{n} i^k$ indicates a sum that runs from $i = 0$ through (inclusive) $i = n$. Each term of the sum is a function of i. In our case the i-th term of the sum is i^k. We shall show that $S_1 = 0 + 1 + \ldots + n = n(n+1)/2$.

Proposition 3 *For all natural integers $n \geq 0$, we have that $0 + 1 + 2 + \ldots + n = n(n+1)/2$.*

In this particular example the natural-valued variable is n. In Proposition 3, the statement/predicate that is either true or false is "$0 + 1 + 2 + \ldots + n = n(n+1)/2$". Let us call this predicate $P(n)$ i.e a predicate P that depends on natural-valued n. Identifying $P(n)$ from a proposition may sometimes be not such an easy task.

Let us go back to Proposition 3 and let's examine whether $P(n)$ is true for $n = 0$ and $n = 1$.

For $n = 0$, $P(0)$, is the sum $0 + \ldots + 0$ that includes no terms as its last term is $n = 0$ and so the sum contains no terms (i.e. it is 0). Then the left-hand side of the equality in Proposition 3 for $n = 0$ is zero. The right-hand size is $0(0+1)/2 = 0$, which is also zero. As $0 = 0$ is true we conclude that $P(0)$ is also true. Therefore we proved that $P(0)$ is true.

For $n = 1$, the sum $0 + \ldots + 1$ contains a single term and it is equal to 1, which is also equal to $1 \cdot (1+1)/2$, and therefore $P(1)$ is also true.

Therefore, $P(0)$ and $P(1)$ are both true.

2.2 Induction: From A to Z

A. We first make clear our intention to use induction, i.e. we state that **This proof will be by induction**.

B. We then identify the predicate $P(n)$ in a proposition that depends on a natural-valued variable n contained in the proposition. The assumption that $P(n)$ is true will be our **inductive hypothesis**.

C. The induction consists of the following:

C1. Base Case where we show $P(0)$ i.e. that $P(0)$ is true.

C2. Inductive Step where we show that $\forall n \in N\ P(n) \Rightarrow P(n+1)$, assuming that $P(n)$ is true (inductive hypothesis).

Comment 1. In many cases proving the base case is easy. For Proposition 3, $P(0)$ was straightforward to show, for example.

Comment 2. The base case need not be $P(0)$. In many instances it is $P(1)$. In fact it may be the case that the base case is $P(k)$ for some positive integer k. If this is, however, the case, we need to be careful with what we prove in the inductive step. We should show that $\forall n \geq k\ P(n) \Rightarrow P(n+1)$, rather than $\forall n \in N\ P(n) \Rightarrow P(n+1)$.

Comment 3. A very common confusion with induction is the use of the inductive hypothesis in the inductive step. In the inductive hypothesis we do not STATE/CLAIM that $P(n)$ is true. We ASSUME that $P(n)$ is true to complete the inductive step thus trying to show that 'If $P(n)$ is true then $P(n+1)$ is true". Thus in the inductive step ASSUMING the trueness of $P(n)$ we try to establish the trueness of $P(n+1)$. If $P(n)$ is false, however, the inductive step can not be completed and thus we cannot show that $P(n)$ is true (since we have already established that $P(n)$ was false).

Comment 4. What does $\forall n \in N\ P(n) \Rightarrow P(n+1)$ really mean? It means that if we show this implication and somehow we know that say $P(7)$ is true, then by substituting for $n = 7$ in the implication we also show that $P(8)$ is also true. Since $P(8)$ has proven true substituting for $n = 8$ in the implication we show that $P(9)$ is true and so on for $P(10), P(11), \ldots$. Therefore establishing (and NOT assuming) the trueness of $P(k)$ for some natural number k we have also established the trueness of an infinite other cases $P(k), P(k+1), P(k+2), \ldots$.

2.3 An example (Proposition 3)

A proof by induction of Proposition 3 can be found in the textbook. We summarize that proof below. The example that follows the proof is more extensive and detailed, however.

Proof of Proposition 3.

Let $S_1 = 0 + \ldots + n$. We are going to show that $0 + \ldots + n = n(n+1)/2$. We call equality $P(n)$. The proof is by induction.

1. Base case. We show that $P(0)$ is true. The left hand side sum of $P(0)$ is $0 + \ldots + 0$ which is 0. The right hand side of $P(0)$ is $0(0+1)/2$ which is also 0. Therefore $P(0)$ is true since the left and right hand side of $=$ are equal to zero and thus equal to each other.

2. Inductive Step. Show that $P(n) \Rightarrow P(n+1)$ for all $n \geq 0$.

Inductive hypothesis. Let us assume that $P(n)$ is true, i.e. $0 + 1 + 2 + \ldots + n = \sum_{i=0}^{n} i = n(n+1)/2$.

We need to prove that $0 + 1 + 2 + \ldots + (n+1) = \sum_{i=0}^{n+1} i = (n+1)(n+2)/2$.

We start from the left-hand side of the latter equality to derive the right-hand side utilizing the inductive hypothesis.

$$\begin{aligned} 0 + 1 + 2 + \ldots + (n+1) &= \sum_{i=0}^{n+1} i \\ &= \left(\sum_{i=0}^{n} i\right) + (n+1) \\ &= n(n+1)/2 + (n+1) \end{aligned}$$

$$\begin{aligned} &= n(n+1)/2 + 2(n+1)/2 \\ &= (n+1)(n+2)/2 \end{aligned}$$

We got the third equality from the second one by observing that the sum in the former equality is the one in the inductive hypothesis. □.

2.4 Another example

Below, we prove the following more elaborate theorem.

Theorem 1 *Show that for all integer $m \geq 0$, $1 + x + \ldots + x^m = \frac{x^{m+1}-1}{x-1}$, for any $x \neq 1$.*

We relabel the natural variable in this example m instead of n.

Proof. We prove the theorem **by induction**.

The natural variable in the theorem is m. The predicate $P(m)$ in the theorem that depends on m is $1 + x + \ldots + x^m = \frac{x^{m+1}-1}{x-1}$, for any $x \neq 1$. There are various ways to represent the sum; one is $1 + x + \ldots + x^m$, another one is $\sum_{i=0}^{i=m} x^i$ or

$$\sum_{i=0}^{i=m} x^i$$

We proceed to presenting the inductive proof.

Base case. We show that $P(0)$ is true. The series $1+x+\ldots+x^m$ for $m = 0$ has as its last term $x^m = x^0 = 1$, i.e. the first term of the sum is also the last one. This means that the series collapses into a single term. On the other hand the right hand side for $m = 0$ gives

$$\frac{x^{0+1} - 1}{x - 1} = \frac{x - 1}{x - 1} = 1$$

Therefore,

$$1 + \ldots + x^0 = 1 = \frac{x^{0+1} - 1}{x - 1} = \frac{x - 1}{x - 1}$$

which is obviously true for any $x \neq 1$ (this is required to avoid division be zero problems).

Inductive Step. We show that for all $m \geq 0$, if $P(m)$ is true, then $P(m + 1)$ is also true. Our **inductive hypothesis** is "$P(m)$ is true".

If $P(m)$ is true, then the following equality will hold.

$$1 + x + \ldots + x^m = \frac{x^{m+1} - 1}{x - 1}$$

We then need to prove that $P(m + 1)$ is also true, i.e. we need to prove that

$$1 + x + \ldots + x^{m+1} = \frac{x^{m+2} - 1}{x - 1}$$

To prove this we start from the left hand side of $P(m + 1)$ and we rewrite it so that we can use the fact that $P(m)$ is true.

$$\begin{aligned} 1 + x + \ldots + x^{m+1} &= 1 + x + \ldots + x^m + x^{m+1} \\ &= (1 + x + \ldots + x^m) + x^{m+1} \end{aligned}$$

We observe that the term $(1 + x + \ldots + x^m)$, by the trueness of $P(m)$, is known.

$$\begin{aligned} 1+x+\ldots+x^{m+1} &= 1+x+\ldots+x^m+x^{m+1} \\ &= (1+x+\ldots+x^m)+x^{m+1} \\ &= \frac{x^{m+1}-1}{x-1}+x^{m+1} \end{aligned}$$

By completing the calculations we get that

$$\begin{aligned} 1+x+\ldots+x^{m+1} &= \frac{x^{m+1}-1}{x-1}+x^{m+1} \\ &= \frac{(x^{m+1}-1)+x^{m+1}(x-1)}{x-1} \\ &= \frac{(x^{m+1}-1)+x^{m+2}-x^{m+1}}{x-1} \\ &= \frac{x^{m+2}-1}{x-1}, \end{aligned}$$

which proves that $P(m+1)$ is true.

Therefore we proved the following: (a) $P(0)$ is true (base case), (ii) assuming that $P(m)$ was true, we proved that $P(m+1)$ was true or equivalently for all $m \geq 0$, $P(m) \Rightarrow P(m+1)$. By Axiom 3, this shows that for all m, $P(m)$ is indeed true and the theorem has been proven.

2.5 Exercises

Do for practice the following examples.

Example 1. Show that for any $n \geq 0$

$$\sum_{i=0}^{i=n} i^2 = n(n+1)(2n+1)/6$$

Example 2. Show that for any $n \geq 1$, $n^2 - 1 > 0$.

Example 3. What is wrong with the proof of Theorem 2 below? Explain.

Theorem 2 *All horses of the world are of the same color.*

Proof. The proof is by induction on the number of horses n. Let $P(n)$ be the following predicate.

In any set of $n \geq 1$ horses, all the horses of the set are of the same color.

The base case is $P(1)$ and $P(1)$ is always true as in a set consisting of a single horse, all the horses (there is only one) of the set have the same color.

Let us assume (inductive hypothesis) that for any n, $P(n)$ is true. Since we assume $P(n)$ to be true, any set of n horses have the same color. Then we will prove that $P(n+1)$ is also true (inductive step). To show the inductive step, i.e. that $P(n+1)$ is true let us consider ANY set of $n+1$ horses $H_1, H_2, \ldots H_n, H_{n+1}$.

The set of horses $H_1, H_2, \ldots, H_n$, consists of n horses, and by the inductive hypothesis any set of n horses are of the same color. Therefore color(H_1) =color(H_2) = ... =color(H_n).

The set of horses $H_2, H_3, \ldots, H_{n+1}$, consists of n horses, and by the inductive hypothesis any set of n horses are of the same color. Therefore color(H_2) =color(H_3) = ... =color(H_{n+1}).

Since from the first set of horses color(H_2) =color(H_n), and from the second set color(H_2) =color(H_{n+1}), we conclude that the color of horse H_{n+1} is that of horse H_2, and since all horses $H_1, H_2, \ldots, H_n$ are of the same color, then all horses $H_1, H_2, \ldots, H_n, H_{n+1}$ have the same color. This proves the inductive step.

The induction is complete and we have thus proved that for any n, in any set of n horses all horses (in that set) are of the same color.

EndofProof.

(Hint: The key to this proof is the existence of horse H_2.)

3 Ordinary vs Strong Induction

The induction proof technique we have described is sometimes called ordinary induction. It is summarized by the inductive step $P(n) \Rightarrow P(n+1)$.

Sometimes this does not suffice to show that $P(n)$ is true. We can then use **strong induction**.

Axiom 4 (Strong Induction). For any predicate P, if

- $P(0)$
- and $\forall n \in N\ (P(0) \wedge P(1) \wedge \ldots \wedge P(n)) \Rightarrow P(n+1)$,
- then $\forall n \in N$, $P(n)$.

Therefore in strong induction, the trueness of $P(n+1)$ is a consequence of the trueness of all preceding predicates $P(1), P(2), \ldots, P(n)$, not just of $P(n)$.

3.1 An Example.

A **recursive function** is a function that invokes itself. In **direct recursion** a recursive function f invokes directly itself, whereas in **indirect recursion** function f invokes function g that invokes f. A quiet well-known recursive function from discrete mathematics is the Fibonacci function F_n. The Fibonacci function is defined as follows.

$$F_n = F_{n-1} + F_{n-2} \text{ if } n > 1$$

where

$$F_0 = 0 \text{ and } F_1 = 1$$

Proposition 4 *For any $n \geq 0$, we have that $F_n \leq 2^n$.*

Proof. Proof is by strong induction.

Base case. We show that $F_0 \leq 2^0 = 1$. Since $F_0 = 0$, and we have that $0 \leq 1$ the base case follows.

Inductive Step. We shall show that if $F_i \leq 2^i$ for all $i = 0, 1, \ldots, n-1$, then $F_n \leq 2^n$.

In order to prove the inductive step we assume the inductive hypothesis i.e. that for all $i < n$ we have indeed $F_i \leq 2^i$. Since $n-1$ and $n-2$ are less than n by the inductive hypothesis we thus have that $F_{n-1} \leq 2^{n-1}$ and $F_{n-2} \leq 2^{n-2}$. The inductive step is then shown by using the recurrence.

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &\leq 2^{n-1} + F_{n-2} \\ &\leq 2^{n-1} + 2^{n-2} \\ &\leq 2^{n-1} + 2^{n-1} \\ &= 2 \cdot 2^{n-1} \\ &= \cdot 2^n \end{aligned}$$

The second and third line are by the way of the inductive hypothesis for $n-1$ and $n-2$ respectively. Therefore we have shown that if $F_i \leq 2^i$ for all $i = 0, \ldots, n-1$, then $F_n \leq 2^n$. This completes the strong induction.

We have thus shown that $F_n \leq 2^n$ for all $n \geq 0$.

Example 1. Show that for any $n \geq 0$

$$F_n \leq 2^{n-1}.$$

Example 2. Show that for any $n \geq 1$

$$F_n \geq 2^{n/2-1}.$$