Bucknell UNIVERSITY

Theory of Computation
CSCI 341, Fall 2016

Principles of Induction

Abstract

The principle of induction is a fundamental tool for proving the truth of a property for an infinite set of objects. The first infinite set encountered is the set of natural numbers, we introduce the basic and strong induction principle on natural numbers. Second we present its generalization to well-founded sets. The well-founded induction is a fundamental tool for applying induction on various set of objects arising in computer science. The application of these principles of induction are illustrated by showing the proof of termination of algorithms.

1 Principle of induction on natural numbers

We assume $P(n)$ being a property depending on n.

Principle induction 1:
If the two following conditions are true

1. (base case) $P(0)$
2. (induction case) $\forall i \in \mathbb{N}, (P(i) \Rightarrow P(i+1))$

then $\forall n \in \mathbb{N}, P(n)$.

Example 1. *For all $n \geq 0$, the following equality holds:*

$$0+1+\cdots+n = \frac{n(n+1)}{2}$$

Proof. Let $P(n)$ be the statement:

$$0+1+\cdots+n = \frac{n(n+1)}{2}$$

Let us prove it by induction.

- (base case) $0 = \frac{0(0+1)}{2}$, so $P(0)$ is true.
- (induction case) Let $i \in \mathbb{N}$, assuming H: $0+1+\cdots+i = \frac{i(i+1)}{2}$, we want to prove that $P(i+1)$ is true.

$$\begin{aligned}
0+1+\cdots+i+(i+1) &= (0+1+\cdots+i)+(i+1) \\
&= \frac{i(i+1)}{2}+(i+1) && \text{by induction hypothesis } H \\
&= \frac{i(i+1)}{2}+\frac{2(i+1)}{2} \\
&= \frac{(i+2)(i+1)}{2} \\
&= \frac{(i+1)(i+2)}{2} && \text{by commutativity}
\end{aligned}$$

□

Example 2. *Let us define the factorial function as follows:*

$$fact(n) = \begin{cases} 1 & \text{if } n \leq 0 \\ n \times fact(n-1) & \text{otherwise} \end{cases}$$

This definition is indeed a *valid* definition for a function because it terminates for any input natural number. In general, a function definition could be wrong if it corresponds to a circular computation with no termination. This is the reason why it is important to prove the termination of functions defined recursively.

Proposition 1. *For all natural number n, $fact(n)$ terminates.*

Proof. Let us prove by induction that the following proposition is true, $P(n)$: $fact(n)$ terminates.

- (base case) By definition $fact(0) = 0$ thus it terminates and $P(0)$ is true.
- (induction case) Let $i \in \mathbb{N}$, let us assume the induction hypothesis $H : fact(i)$ terminates. We want to prove that $f(i+1)$ terminates (also known as $P(i+1)$ is true). We know that $i+1$ is greater than 0, so we have $f(i+1) = i \times f(i)$ by definition of f. Using the induction hypothesis H we know that $f(i)$ terminates, finally we have that $f(i+1) = i \times f(i)$ terminates.

Both the base case and the induction case are true. Consequently, we have proven by induction that for all natural number n, $f(n)$ terminates.

□

Sometimes a property parametrized by a number n is true for all numbers except a few intial values. In this case, the induction principle seen before does not work and we need a variation of this induction principle.

Principle of induction 2:
Let $n_0 \in \mathbb{N}$. If the following two conditions are true:

1. *(base case)* $P(n_0)$
2. *(induction case)* $\forall n, [(n \geq n_0) \Rightarrow P(n)] \Rightarrow P(n+1)$

then $\forall n \geq n_0, P(n)$.

Example 3. *This principle of induction is adequate for proving that $2^n \leq n!$ for any $n \geq 4$.*

2 Principle of strong induction

Sometimes you need the induction hypothesis to be stronger in the sense that not only you need $P(i)$ to be true for proving $P(i+1)$ but you need all the $P(j)$ to be true for $j \leq i$. This variant of induction principle is called the principle of strong induction:

Principle of strong induction:
Let $n_0 \in \mathbb{N}$. If the following two conditions are true:

1. *(base case)* $P(n_0)$
2. *(induction case)* $\forall i, [\forall j, n_0 \leq j \leq i \Rightarrow P(j)] \Rightarrow P(i+1)$

then $\forall n \geq n_0, P(n)$.

Remark that the principle of strong induction allows to start the induction from a specific number n_0.

Example 4. *Consider the Fibonacci function defined as the following:*

$$fibo(n) = \begin{cases} 0 & \text{if } n \leq 0 \\ 1 & \text{if } n = 1 \\ fibo(n-1) + fibo(n-2) & \text{otherwise} \end{cases}$$

Proposition 2. *For all natural number n, $fibo(n)$ terminates.*

Proof. We prove by strong induction on n the following property:

$$P(n): \ fibo(n) \text{ terminates}$$

- (base case) $fibo(0) = 1$ so it terminates, and then $P(0)$ is true
- (induction case) Let $i \in \mathbb{N}$, let us assume the induction hypothesis $H : \forall j, j \leq i \Rightarrow P(j)$. We want to prove that $P(i+1)$ is true. By case on $i+1$,
  - $i+1 = 1$, then $fibo(1) = 1$, and then it terminates.
  - $i+1 > 1$, then $fibo(i+1) = fibo(i) + fibo(i-1)$, since i and $i-1$ are less then i, by the induction hypothesis H we know that $fibo(i)$ and $fibo(i-1)$ terminates, and so $fibo(i+1)$

  Finally we have proven that $P(i+1)$ is true.

The base case and the induction case are true. We can conclude, using the principle of strong induction that $\forall n$, $fibo(n)$ terminates. □

3 Principle of Well-founded induction

The principle of induction we have seen are valid for numbers. Its generalisation to arbitrary sets is the topic of this section. Remark that on numbers the notions involved in the definition of induction is the $<$ relation. This is where we have to start.

Let $\prec$ be a binary relation on a set A. The relation $\prec$ has an *infinite descending chain* if and only if there exists an element a_0 such that:

$$\cdots \prec a_n \prec a_{n-1} \prec \cdots \prec a_1 \prec a_0$$

Definition 1. *A relation with no infinite descending chain is called well-founded. A set A with a well-founded relation is called well-founded.*

Remark that the set of natural numbers with the strictly-less-than-equal relation $<$ form a well-founded set.

Principle of well-founded induction:
Assuming $(A, \prec)$ is a well-founded. If the following proposition holds:

$$\forall a \in A, [(\forall b \in A, b \prec a \Rightarrow P(b)) \Rightarrow P(a)]$$

then $\forall a \in A, P(a)$.

Example 5. *The Ackermann function is defined recursively as the following:*

$$ack(m,n) = \begin{cases} n+1 & \text{if } m = 0 \\ ack(m-1,1) & \text{if } m > 0 \text{ and } n = 0 \\ ack(m-1, ack(m,n-1)) & \text{if } m > 0 \text{ and } n > 0 \end{cases}$$

Proposition 3. *The Ackermann function terminates for any pair (m,n).*

Proof. Let us define the adequate well-founded relation. Consider the following relation $\prec$ on $\mathbb{N} \times \mathbb{N}$:

$$(a,b) \prec (c,d) \text{ iff } a < b \text{ or } a = b \text{ and } b < c$$

The relation $\prec$ is well-founded (convince yourself of that).

Let us prove using the well-founded induction that the Ackermann function terminates for any pair m,n. Let (m,n) be a pair of natural numbers, let us assume the induction hypothesis

$$H : \forall (a,b), [(a,b) \prec (m,n) \Rightarrow Ack(a,b) \text{ terminates}]$$

We prove by case on (m,n) that $Ack(m,n)$ terminates:

- $(m,n) = (0,0)$, in this case $Ack(0,0) = 1$ by definition, then it terminates.
- $(m,n) = (m,0)$, with $m > 0$, then we consider the pair $(m-1,1)$. We have that $(m-1,1) \prec (m,n)$ then we can use the induction hypothesis H and we have that $Ack(m-1,1)$ terminates. In this case $Ack(m,n) = Ack(m-1,1)$ and then it terminates.
- (m,n) is such that $m > 0$ and $n > 0$. First, we consider first the pair $(m,n-1)$, we know that $(m,n-1) \prec (m,n)$, then we can apply the induction hypothesis H and we obtain that $Ack(m,n-1)$ terminates. Second, we consider the pair $(m-1, Ack(m,n-1))$, we know that $(m-1, Ack(m,n-1)) \prec (m,n)$, applying again the induction hypothesis H and we obtain the $Ack(m-1, Ack(m,n-1))$ terminates, in this case this is equal to $Ack(m,n)$ and then it terminates.

Finally in all cases we have proven the $H \Rightarrow (Ack(m,n))$ terminates . We conclude that the Ackermann function terminates on any pair of natural numbers. □

We have seen an example of using the well-founded induction principle on pair of numbers. The same idea can be applied to many other structures, in particular the computational ones, like trees, graphs, expressions, lists, words. In each case, one has to define first a well-founded relation. For example on trees, it can be the relation *to be a subtree*, on expressions it can be the relation *to be a subexpression*, *etc.* And then one can use the well-founded induction principle to prove properties.