

The Natural Numbers, Induction and Numeric Recursion

Luke Hunsberger

February 16, 2010

1 The Natural Numbers

We casually think of the *natural numbers* as the set

$$N = \{0, 1, 2, 3, \dots\}$$

The only problem is that it is not clear what “...” means.

⇒ We shall take it as given that the set, N , exists and is the unique set that satisfies the *Peano axioms*:¹

(P_1) There is a natural number 0.

(P_2) Every natural number a has a natural number successor, denoted by $Succ(a)$.

(P_3) There is no natural number whose successor is 0.

(P_4) Distinct natural numbers have distinct successors: if $a \neq b$, then $Succ(a) \neq Succ(b)$.

(P_5) If a property is possessed by 0 and also by the successor of every natural number which possesses it, then it is possessed by all natural numbers.

We can restate Axiom P_5 as follows:

¹This presentation of the Peano axioms is courtesy of Wikipedia:
http://en.wikipedia.org/wiki/Natural_number.

(P'_5) Let P be some property such that:

- $P(0)$ holds; and
- for every $a \in N$, if $P(a)$ holds, then so does $P(\text{Succ}(a))$.

Then $P(n)$ holds for all $n \in N$.

It is important to understand what Axiom P'_5 —or, equivalently, Axiom P_5 —is saying. If both of the bulleted conditions hold, then we can conclude that $P(n)$ holds for all $n \in N$. The first condition is easy: it simply says that $P(0)$ holds. The second condition is more complicated: it is a statement about *all* of the numbers, a , for which $P(a)$ holds. It says that *whenever* $P(a)$ holds, so does $P(\text{Succ}(a))$, where $\text{Succ}(a)$ is the successor of a .

Suppose P is some property for which both of the bulleted conditions hold. Since the first condition holds, we have that $P(0)$ holds. But then the second condition implies that $P(\text{Succ}(0))$ holds (i.e., that $P(1)$ holds). But then the second condition implies that $P(\text{Succ}(1))$ holds (i.e., that $P(2)$ holds). *And so on* (i.e., ...)!

2 Induction and Numeric Recursion

Axiom P'_5 forms the basis for a proof method known as *induction*. This section contains several examples of inductive proofs and demonstrates the close link between a certain class of recursively defined functions and induction.

Theorem 1. Every natural number, n , has one of two forms: either $n = 0$ or $n = \text{Succ}(m)$ for some $m \in N$.

Proof. We'll prove the theorem using induction (i.e., using Axiom P'_5). Therefore, we first need to state the theorem in terms of a property:

Let $P(n)$ be the property that “either $n = 0$ or $n = \text{Succ}(m)$ for some $m \in N$ ”.

The statement of the theorem is then: $P(n)$ holds for all $n \in N$.

We prove the theorem by showing that both of the bulleted conditions in Axiom P'_5 hold:

- $P(0)$ is the property that “either $0 = 0$ or $0 = \text{Succ}(m)$ for some $m \in N$ ”. Since $0 = 0$, we have that $P(0)$ holds.

- Next, suppose k is any one of the natural numbers for which $P(k)$ holds. We want to show that for such a k , $P(\text{Succ}(k))$ also holds. But $P(\text{Succ}(k))$ says “either $\text{Succ}(k) = 0$ or $\text{Succ}(k) = \text{Succ}(m)$ for some m ”. There is indeed a number, m , such that $\text{Succ}(k) = \text{Succ}(m)$. In particular, we can choose $m = k$, in which case we have: $\text{Succ}(k) = \text{Succ}(k)$.

Since both of the bulleted conditions hold, Axiom P'_5 tells us that we can conclude that $P(n)$ holds for all $n \in N$.

Theorem 1 tells us that a natural number, n , can only have one of two forms: either $n = 0$ or $n = \text{Succ}(m)$ for some $m \in N$. There are no other possibilities (i.e., there are no other kinds of elements in N).

A Recursively Defined Function: Factorial. Let f be the factorial function. It is typically defined recursively, as follows:

- $f(0) = 1$
- For $n > 0$, $f(n) = n * f(n - 1)$

Equivalently, we can write the definition of f in the following form, which more closely mirrors the preceding discussion:

(Case 1: $n = 0$) $f(0) = 1$

(Case 2: $n = \text{Succ}(m)$) $f(\text{Succ}(m)) = \text{Succ}(m) * f(m)$

Theorem 2. The above cases define $f(n)$ for every natural number, n .

Proof. Let $P(n)$ be the proposition that $f(n)$ is defined. $P(0)$ holds since Case 1 defines $f(0)$. Next, suppose that $P(k)$ holds for some k (i.e., $f(k)$ is defined). We need to show that $P(\text{Succ}(k))$ holds (i.e., $f(\text{Succ}(k))$ is defined). Since Case 2 defines $f(\text{Succ}(k))$ in terms of $f(k)$, we have that $f(\text{Succ}(k))$ is defined. Thus, both bulleted conditions of Axiom P'_5 hold. Thus, we can conclude that $P(n)$ holds for all $n \in N$ (i.e., $f(n)$ is defined for all $n \in N$).

We can define the factorial function in Scheme as follows:

```
(define facty
  (lambda (n)
    (if (zero? n)
        1 ;; <--- f(0) = 1
        (* n (facty (- n 1)))))) ;; <--- f(Succ(m)) = Succ(m) * f(m)
```

Since there are only two cases to distinguish, an `if` special form is appropriate. Later on, we'll look at recursive data structures where there might be more than two cases. In such cases, a `cond` special form is more convenient. For the factorial function, the definition using a `cond` looks like this:

```
(define facty
  (lambda (n)
    (cond
      ;; BASE CASE: n = 0
      ((zero? n)
       1) ;; <--- f(0) = 1
      ;; RECURSIVE CASE: n = Succ(m)
      (else
       (* n (facty (- n 1)))))) ;; <--- f(Succ(m)) = Succ(m) * f(m)
```

Other Examples. Similar functions can be defined recursively using the same sorts of techniques:

- $1 + 2 + 3 + \dots + n$
- $1^2 + 2^2 + 3^2 + \dots + n^2$
- $1 - \frac{1}{2} + \frac{1}{3} - \dots \pm \frac{1}{n}$

In each case, the recursive definition defines a *base case* (for $n = 0$) and a *recursive case* (for $n = \text{Succ}(m)$). For example, summing the squares from 1 to n can be defined as follows:

```
(define sum-squares
  (lambda (n)
    (if (zero? n)
        0
        (+ (* n n) (sum-squares (n-1))))))
```

Alternatively, we could use $n = 1$ as a base case:

```
(define sum-squares
  (lambda (n)
    (if (= n 1)
        1
        (+ (* n n) (sum-squares (n-1))))))
```

However, if we do that, we need to keep in mind that this function is only defined for $n \geq 1$.

3 Proving Properties of Recursively Defined Functions

So far, we have only defined recursive functions and shown that they are defined for all natural numbers. We can also use induction to prove that certain recursive functions have certain properties.

Consider the following definition of the *addition* function:

- (1) For all $x \in N, z = 0$: $x + 0 = x$
- (2) For all $x \in N, z = S(y)$ for some $y \in N$: $x + S(y) = S(x + y)$

Since the above cases include $z = 0$ and $z = S(y)$ (for some y), the addition function is defined for all $z \in N$. Furthermore, since each case includes “for all $x \in N$ ”, the addition function is defined for all $x, z \in N$.

Theorem 3. The above-defined addition function is *associative* (i.e., $a + (b + c) = (a + b) + c$, for all $a, b, c \in N$).

Proof. Let $P(c)$ be the proposition $a + (b + c) = (a + b) + c$, for all $a, b \in N$. Notice that for each value of c , the proposition $P(c)$ is a statement about something “for all $a, b \in N$ ”. Thus, if we can show that $P(c)$ holds for all $c \in N$, then we will have shown that $a + (b + c) = (a + b) + c$, for all $a, b, c \in N$, as desired.

- ($c = 0$): $P(0)$ is the proposition that $a + (b + 0) = (a + b) + 0$ for all $a, b \in N$.

Left-hand side: $a + (b + 0)$
= $a + b$, by equation (1) of addition definition (with $x = b$)
= $(a + b) + 0$, by equation (1) of addition definition (with $x = b + c$)
= Right-hand side.

- $(c = S(m))$: $P(S(m))$ is the proposition that $a + (b + S(m)) = (a + b) + S(m)$. Want to show that *if* $P(m)$ holds, *then* $P(S(m))$ holds. So, we'll assume that $P(m)$ holds and try to show that then $P(S(m))$ holds.

$$\begin{aligned} & \text{Left-hand side of } P(S(m)): a + (b + S(m)) \\ &= a + S(b + m), \text{ by equation (2) of addition definition (with } x = b \text{ and } y = m) \\ &= S(a + (b + m)), \text{ by equation (2) of addition definition (with } x = a \text{ and } y = b + m) \\ &= S((a + b) + m), \text{ since } P(m) \text{ holds (by assumption)} \\ &= (a + b) + S(m), \text{ by equation (2) of addition def'n. (with } x = a + b \text{ and } y = m) \\ &= \text{Right-hand side of } P(S(m)). \end{aligned}$$

Thus, *if* $P(m)$ holds, then so does $P(S(m))$.

Thus, by induction, we conclude that $P(c)$ holds for all $c \in N$.