Avigad, Heuele, Nawrocki, Logic and mechanized reasoning

Matteo Bianchetti

February 19, 2025

Contents

Preface

I solve some exercises and prove some statements from Avigad et al., *Logic and mechanized reasoning* (v 0.1). In the appendix, I list the errata that I have found.

Notation

Chapter 1

Introduction

The authors lists three ideas that, it seems, are jointly found for the first time in the work of Ramon Llull (1232?-1316):[1]

1. Symbols can stand for ideas.
2. One can generate complex ideas by combining simpler ones.
3. Mechanical devices can serve as aids to reasoning.

[1] The author spells the monk's last name as "Lull".

Chapter 2

Mathematical background

Key concepts:

1. proof by induction (p. 3)
2. definition by recursion (p. 4)
3. proof by complete induction (p. 5)
4. definition by course-of-values recursion (p. 5).
5. inductive definition (p. 6).

On p. 5, the authors define the following function recursively:

$$f(n,\ k) = \begin{cases} 1 & \text{if } k = 0 \text{ or } k = n \\ f(n-1,\ k) + f(n-1,\ k-1) & \text{otherwise} \end{cases}$$

where n and k are natural numbers and $k \leq n$. One more usually write the above function as

$$\binom{n}{k} = \begin{cases} 1 & \text{if } k = 0 \text{ or } k = n \\ \binom{n-1}{k} + \binom{n-1}{k-1} & \text{otherwise.} \end{cases}$$

Here $\binom{n}{k}$ indicates the number of ways of choosing k objects out of n without repetition. The equation in the second case, i.e.

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

is called *Pascal's identity*. Its intuitive justification is as a follows. Let x be an object among the n-many objects that are given. Then, if you do not choose x, you have to choose k objects from the now $n-1$-many given objects. If you do choose x, then you have to continue by selecting $k-1$ objects from the now $n-1$-many objects. Since every selection of k objects from the given n objects either include or does not include x, then the total number of ways of choosing k objects out of n without repetition is the sum of the ways of selecting k objects from $n-1$ objects (when you do not choose x) and the number of ways of selecting $k-1$ objects from $n-1$ objects (when you choose x).

Theorem 2.1. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Proof. I reason by induction. The statement is true for $n = 0$. Now, suppose that it holds for $n-1$. I show that it holds for n too. The following equalities hold:

$$\begin{aligned}
\binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1} && \text{[by definition]}\\
&= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} && \text{[by induction]}\\
&= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-k+1)!}\\
&= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!}\\
&= \frac{(n-1)!}{k(k-1)!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)(n-1-k)!}\\
&= \frac{(n-1)!}{(k-1)!(n-1-k)!}\left[\frac{1}{k} + \frac{1}{(n-k)}\right]\\
&= \frac{(n-1)!}{(k-1)!(n-1-k)!}\left[\frac{n-k+k}{k(n-k)}\right]\\
&= \frac{(n-1)!}{(k-1)!(n-1-k)!}\left[\frac{n}{k(n-k)}\right]\\
&= \frac{n(n-1)!}{k(k-1)!(n-k)(n-1-k)!}\\
&= \frac{n!}{k!(n-k)!}
\end{aligned}$$

□

Given two lists ℓ and m, I write

$$\ell + m$$

as a shortcut for

$$append(\ell,\ m).$$

Theorem 2.2. *For every list ℓ, $\ell + [] = \ell$.*

Theorem 2.3. *The operation append is associative.*[1]

Proof. Given two lists, l_1 and l_2, I will write $l_1 + l_2$ to indicate $append(l_1, l_2)$. I prove that, for every list l_1, l_2, l_3,

$$(l_1 + l_2) + l_3 = l_1 + (l_2 + l_3).$$

I reason by induction. For the base step, let $l_1 = []$. Therefore,

$$[] + (l_2 + l_3) = l_2 + l_3 = ([] + l_2) + l3.$$

Now, suppose that associativity holds for $l_1 = l$. I prove that it holds for $(a :: l)$, l_2, l_3. I will use the following property from the definition of :::[2]

$$(a :: m) + n = a :: (m + n)$$

[1] The authors define *append* on page 6.
[2] The authors define :: on page 6.

where a is an element and m and n are lists. The the proof continues as follow:

$$\begin{aligned}(a :: l) + (l_2 + l_3) &= a :: (l + (l_2 + l_3)) && \text{[by defin. of ::]}\\ &= a :: ((l + l_2) + l_3) && \text{[by induct. hyp.]}\\ &= (a :: (l + l_2)) + l_3 && \text{[by defin. of ::]}\\ &= ((a :: l) + l_2) + l_3 && \text{[by defin. of ::]}\end{aligned}$$

□

Theorem 2.4. *For every element a and list ℓ,*

$$a :: \ell = [a] + \ell.$$

Proof. For the base case, observe

$$a :: [] = [a] = [a] + [].$$

For the inductive hypothesis, assume

$$a :: \ell = [a] + \ell.$$

For the inductive step, let b be an element:

$$\begin{aligned}a :: (b :: \ell) &= a :: ([b + \ell]) && \text{[by induct. hyp.]}\\ &= (a :: [b]) + \ell && \text{[by defin. of +]}\\ &= ([a] + [b]) + \ell && \text{[by induct. hyp.]}\\ &= [a] + ([b] + \ell) && \text{[by assoc. of +]}\end{aligned}$$

□

Theorem 2.5. *For every list ℓ and element a, $appendl(\ell,\ a) = \ell + [a]$.*

Proof. I reason by induction. For the base case,

$$appendl([],\ a) = [a] = [] + [a].$$

Now, as the induction hypothesis, suppose that $appendl(\ell,\ a) = \ell + [a]$. Then, let b to be an element and consider the following equalities:

$$\begin{aligned}appendl((b :: \ell),\ a) &= b :: appendl(\ell,\ a) && \text{[by defin. of } appendl\text{]}\\ &= b :: (\ell + [a]) && \text{[by induct. hyp.]}\\ &= (b :: \ell) + [a] && \text{[by defin. of +]}\end{aligned}$$

□

Theorem 2.6. *For every list ℓ and m,*

$$reverse(\ell + m) = reverse(m) + reverse(\ell).$$

Proof. I reason by induction. Let $\ell = []$. Therefore

$$reverse([] + m) = reverse(m) = reverse(m) + reverse(\ell).$$

Now, as the inductive step, suppose that, for l and m,

$$reverse(\ell + m) = reverse(m) + reverse(\ell).$$

Let a be an element. The following equalities hold:

$$\begin{aligned}
reverse((a :: l) + m)) &= reverse(a :: (\ell + m)) && \text{[by defin. of } +] \\
&= appendl(reverse(\ell + m),\ a) && \text{[by defin. of } reverse] \\
&= append(reverse(m) + reverse(\ell),\ a) && \text{[by induct. hyp.]} \\
&= (reverse(m) + reverse(\ell)) + [a] && \text{[by theorem 2.5]} \\
&= reverse(m) + (reverse(\ell) + [a]) && \text{[by assoc. of } +] \\
&= reverse(m) + appendl(a,\ reverse(\ell)) && \text{[by theorem 2.5]} \\
&= reverse(m) + reverse(a :: \ell) && \text{[by defin. of } reverse]
\end{aligned}$$

□

Theorem 2.7. *For every list ℓ, $reverse(reverse(\ell)) = \ell$.*

Proof. I reason by induction. For the base step, obverse:

$$reverse(reverse([])) = reverse([]) = [].$$

For the induction hypothesis, assume that $reverse(reverse(\ell))$. For the inductive step, observe:

$$\begin{aligned}
reverse(reverse(a :: \ell)) &= reverse(appendl(reverse(\ell), a)) && \text{[by defin. of } reverse] \\
&= reverse(reverse(\ell) + [a]) && \text{[by theorem 2.5]} \\
&= reverse([a]) + reverse(reverse(\ell)) && \text{[by theorem 2.6]} \\
&= reverse([a]) + \ell && \text{[by induct. hyp.]} \\
&= [a] + \ell && \text{[by property of } reverse] \\
&= a :: \ell && \text{[by defin. of } ::]
\end{aligned}$$

□

Theorem 2.8. *For every list ℓ, $reverse(\ell) = reverse'(\ell)$.*

Proof. For the base case, observe

$$reverse([]) = [] = reverseAux([],\ []) = reverse'([]).$$

For the inductive hypothesis, assume

$$reverse(\ell) = reverse'(\ell)/$$

For the inductive step, observer

$$\begin{aligned}
reverse(a :: \ell) &= reverse(\ell) + reverse([a]) && \text{[by theorem 2.6]} \\
&= reverse(\ell) + [a] && \text{[by property of } reverse] \\
&= reverseAux(\ell, a :: []) && \text{[by defin. of } reverseAux] \\
&= reverseAux(a :: \ell, []) && \text{[by defin. of } reverseAux] \\
&= reverse'(a :: \ell) && \text{[by defin. of } reverse']
\end{aligned}$$

□

Appendix A

Errata

page	errata	corrige
6	we principles	we apply the principles
7	there is part	there is a part

Table A.1: Errata