Avigad, Heuele, Nawrocki, Logic and mechanized reasoning

Matteo Bianchetti

February 22, 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)
6. invariant (p. 9)

2.1 Induction and recursion on the natural numbers

Theorem 2.1. *The solution to the Towers-of-Hanoi (ToH) problem given on page 4 (of Avigad's book) requires* $2^n - 1$ *moves.*

Proof. I call the three towers, from left to right, A, B, C. At the beginning, all the disks are on peg A. Let $T(n)$ be the number of moves that it takes to solve ToH with the given algorithm. The base case is $n = 0$ and the statement holds in this case: the solution requires 0 moves and $T(0) = 2^0 - 1 = 1 - 1 = 0$. For the induction hypothesis, suppose that the statement holds for n. For the inductive step, observes the following:

1. by induction hypothesis, it takes exactly $T(n)$ steps to move all the disks except the largest one to peg C using euxiliary peg B;
2. then, it takes 1 move to move the largest disk from peg A to peg B;
3. then, by induction hypothesis, it takes exactly $T(n)$ steps to move the disks from peg C to peg B using auxiliary peg A.

Therefore,

$$\begin{aligned} T(n+1) &= T(n) + 1 + T(n) \\ &= 2T(n) + 1 \\ &= 2(2^n - 1) + 1 \qquad \text{[by induct. hyp.]} \\ &= 2^{n+1} - 2 + 1 \\ &= 2^{n+1} - 1 \end{aligned}$$

□

2.2 Complete induction

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

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:

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

□

2.3 Generalized induction and recursion

Given two lists ℓ and m, I write

$$\ell + m$$

as a shortcut for

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

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, $\ell + [] = \ell$.*

Proof. For the base step, observe

$$[] + [][].$$

For the induction hypothesis, assume $\ell + [] = \ell$. For the inductive step, observe

$$\begin{aligned}(a :: \ell) + [] &= ([a] + \ell) + [] && \text{[by theorem 2.4]}\\ &= [a] + (\ell + []) && \text{[by assoc. of +]}\\ &= [a] + \ell && \text{[by induct. hyp.]}\\ &= a :: \ell && \text{[by theorem 2.4]}\end{aligned}$$

□

Theorem 2.6. *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 2.7. *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:

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

□

Theorem 2.8. *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:

$$\begin{aligned}
reverse(reverse(a :: \ell)) &= reverse(appendl(reverse(\ell), a)) && \text{[by defin. of } reverse\text{]}\\
&= reverse(reverse(\ell) + [a]) && \text{[by theorem 2.6]}\\
&= reverse([a]) + reverse(reverse(\ell)) && \text{[by theorem 2.7]}\\
&= reverse([a]) + \ell && \text{[by induct. hyp.]}\\
&= [a] + \ell && \text{[by property of } reverse\text{]}\\
&= a :: \ell && \text{[by defin. of ::]}
\end{aligned}$$

□

Theorem 2.9. *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

$$\begin{aligned}
reverse(a :: \ell) &= reverse(\ell) + reverse([a]) && \text{[by theorem 2.7]}\\
&= reverse(\ell) + [a] && \text{[by property of } reverse\text{]}\\
&= reverseAux(\ell, a :: []) && \text{[by defin. of } reverseAux\text{]}\\
&= reverseAux(a :: \ell, []) && \text{[by defin. of } reverseAux\text{]}\\
&= reverse'(a :: \ell) && \text{[by defin. of } reverse'\text{]}
\end{aligned}$$

□

2.4 Invariants

From p. 9:

> "The following puzzle, called the *MU puzzle*, comes from the book *Gödel, Escher, Bach* by Douglas Hofstadter. It concerns strings consisting of the letters M, I, and U. Starting with the string MI, we are allowed to apply any of the following rules:
>
> 1. Replace sI by sIU, that is, add a U to the end of any string that ends with I.
> 2. Replace Ms by Mss, that is, double the string after the initial M.
> 3. Replace $sIIIt$ by sUt, that is, replace any three consecutive Is with a U.
> 4. Replace $sUUt$ by st, that is, delete any consecutive pair of Us."

Theorem 2.10. *A string is derivable in Hofstadter'system if and only it consists of an M followed by any number of Is and Us as long as the number of Is is not divisible by 3.*

Proof. ($\Rightarrow$) First, I prove that if a string is derivable, then it consists of an M followed by any number of Is and Us as long as the number of Is is not divisible by 3. I reason by induction. The base case is MI and the statement is true for this case. Now, suppose that the statement is true after n applications of the rules. I show that the statement remains true after we apply any of the rules above.

1. Rule 1 does not change the number of I in the string. So the statement remains true.

2. Rule 2 doubles the number of I in the string. Since the number of strings before the application of rule 2 was either $1 \mod 3$ or $2 \mod 3$. In the first case, the number of I becomes $2 \mod 3$ and in the second case it becomes $1 \mod 3$. In both cases the statement remains true.

3. Rule 3 reduces the number of I by 3. Since we start with the number of I being $k \not\equiv 0 \mod 3$, also $k - 3 \not\equiv \mod 3$ and the statement remains true.

4. Rule 4 does not affect the number of I in the string. Therefore, the statement remains true.

($\Leftarrow$) Now, I prove that if a string

(C1) consists of an M

(C2) followed by any number of Is and Us

(C3) as long as the number of Is is not divisible by 3,

then that string is derivable.

To be continued.

□

2.5 Exercises

Exercise 1. For $n \geq 1$, prove that

$$\sum_{i<n} ar^i = \frac{a(r^n - 1)}{r - 1}.$$

Proof. I reason by induction. For $n = 1$,

$$\sum_{i<1} ar^0 = a = \frac{a(r^1 - 1)}{r - 1}.$$

By induction hypothesis, suppose that the statement holds for n. Now, consider the following

$$\begin{aligned}
\sum_{i<n+1} ar^i &= \left(\sum_{i<n} ar^i\right) + ar^n \\
&= \frac{a(r^n - 1)}{r - 1} + ar^n \qquad \text{[by induct. hyp.]} \\
&= \frac{a(r^n - 1) + ar^n(r - 1)}{r - 1} \\
&= \frac{ar^n - a + ar^{n+1} - ar^n}{r - 1} \\
&= \frac{a(r^{n+1} - 1)}{r - 1}
\end{aligned}$$

□

Exercise 2.

Proof. I reason by induction. The base case is n=5:

$$5! = 120 > 32 = 2^5.$$

As the induction hypothesis, suppose that the statement is true for n. For the inductive step, consider

$$\begin{aligned}
(n + 1)! &= (n + 1)n! \\
&> 2(2^n) \qquad \text{[because } n + 1 > 2 \text{ and, by induct. hyp., } n! > 2^n\text{]} \\
&= 2^{n+1}
\end{aligned}$$

□

Exercise 3.

Proof. Using summation notation, the expression to prove is the following:

$$\sum_{i=1}^{n} \frac{1}{n(n+1)} = \frac{n}{n+1}$$

The base case is $n = 1$ and the statement holds:

$$\sum_{i=1}^{1} \frac{1}{1 \cdot 2} = \frac{1}{2}.$$

For the inductive hypothesis, suppose that the statements holds for n. For the inductive step, consider

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{n(n+1)} &= \sum_{i=1}^{n} \frac{1}{n(n+1)} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} && \text{[by induct. hyp.]} \\
&= \frac{n(n+2)}{(n+1)(n+2)} \\
&= \frac{n^2+2n+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} \\
&= \frac{n+1}{n+2}
\end{aligned}$$

□

Exercise 4.

Proof. See the proof of theorem 2.1 for the notation. The statement holds for the base case $n = 0$: $2^0 - 1 = 1 - 1 == 0$. For the inductive hypothesis, suppose that the statement holds for n. For the inductive step, I show that the statement holds for $n + 1$. I reason as follows:

1. to move n disks (i.e. all the disks except the largest one) from peg A to peg C requires at least $2^n - 1$ steps (by induction hypothesis);
2. to move the largest disk from peg A to peg B requires 1 step;
3. to move the n disks on peg C to peg B requires at least $2^n - 1$ steps (by induction hypothesis).

Therefore, the entire process requires

$$2^n - 1 + 1 + 2^n - 1$$

steps, which is equal to $2^{n+1} - 1$, i.e. equal to $T(n + 1)$ (see proof of theorem 2.1). Therefore, the algorithm given in the book is optimal. □

Exercise 5.

Proof. □

Exercise 6.

Proof. □

Exercise 7.

Proof. The principle of complete induction (PCI) says that every natural number n has a property P if the following condition is true:

(C) for every n, for every $i < n$, $P(i)$.

I prove by ordinary (weak) induction that, if (C) holds, then, for all natural numbers, $P(n)$ holds. Let Q be a property on the natural numbers. Let us define, for all n,

$$Q(n) \text{ iff } \bigwedge_{i=1}^{n-1} P(i).$$

In words, $Q(n)$ holds if and only if $P(i)$ holds for all $i < n$. As the base case, $Q(0)$ holds because there are no natural numbers strictly below 0. Therefore, $P(0)$ holds. Now, suppose that $Q(n)$ holds. Therefore, $\bigwedge_{i=1}^{n-1} P(i)$. By (C), also $P(n)$ holds. Therefore, $Q(n+1)$ holds as well. Therefore, by ordinary induction, $Q(n)$ holds for every natural number n. Therefore, $P(n)$ also holds for every n. $\square$

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