

Avigad, Heuele, Nawrocki, Logic and mechanized reasoning

Matteo Bianchetti

February 26, 2025

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Mathematical background</b>	<b>3</b>
2.1	Induction and recursion on the natural numbers . . . . .	3
2.2	Complete induction . . . . .	4
2.3	Generalized induction and recursion . . . . .	5
2.4	Invariants . . . . .	8
2.5	Exercises . . . . .	9
<b>A</b>	<b>Errata</b>	<b>18</b>

# 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):<sup>1</sup>

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.

---

<sup>1</sup>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, observe 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 auxiliary 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,

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

□

## 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 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  $\ell$  and  $m$ , I write

$$\ell + m$$

as a shortcut for

$$\text{append}(\ell, m).$$

**Theorem 2.3.** *The operation  $\text{append}$  is associative.*<sup>1</sup>

*Proof.* Given two lists,  $l_1$  and  $l_2$ , I will write  $l_1 + l_2$  to indicate  $\text{append}(l_1, l_2)$ . 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,

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

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  $::$ :<sup>2</sup>

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

---

<sup>1</sup> The authors define  $\text{append}$  on page 6.

<sup>2</sup> 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  $\ell$ ,*

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

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

*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  $\ell$  and element  $a$ ,  $\text{appendl}(\ell, a) = \ell + [a]$ .*

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

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

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

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

□



**Theorem 2.7.** *For every list  $\ell$  and  $m$ ,*

$$\text{reverse}(\ell + m) = \text{reverse}(m) + \text{reverse}(\ell).$$

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

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

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

$$\text{reverse}(\ell + m) = \text{reverse}(m) + \text{reverse}(\ell).$$

Let  $a$  be an element. The following equalities hold:

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

□

**Theorem 2.8.** *For every list  $\ell$ ,  $\text{reverse}(\text{reverse}(\ell)) = \ell$ .*

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

$$\text{reverse}(\text{reverse}([])) = \text{reverse}([]) = [].$$

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

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

□

**Theorem 2.9.** *For every list  $\ell$ ,  $\text{reverse}(\ell) = \text{reverse}'(\ell)$ .*

*Proof.* For the base case, observe

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

For the inductive hypothesis, assume

$$\text{reverse}(\ell) = \text{reverse}'(\ell)/$$

For the inductive step, observe

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

□

## 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 *sIII* by *sUt*, that is, replace any three consecutive *I*s with a *U*.
4. Replace *sUUt* by *st*, that is, delete any consecutive pair of *U*s.”

**Theorem 2.10.** *A string is derivable in Hofstadter’s system if and only if it consists of an *M* followed by any number of *I*s and *U*s as long as the number of *I*s 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 *I*s and *U*s as long as the number of *I*s 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  $1 \pmod 3$  or  $2 \pmod 3$ . In the first case, the number of *I* becomes  $2 \pmod 3$  and in the second case it becomes  $1 \pmod 3$ . 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  $k \not\equiv 0 \pmod 3$ , also  $k - 3 \not\equiv 0 \pmod 3$  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 *I*s and *U*s

(C3) as long as the number of *I*s 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

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

□

**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

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

□

**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

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

□

#### 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.** The goal of the modified ToH problem is to move the disks from peg  $A$  to peg  $C$ . The exercise requires the following:

1. recursive procedure for solving ToH
2. proof that the procedure requires  $3^n - 1$  moves
3. proof that the bound  $3^n - 1$  is optimal
4. proof that, as one carries out the sequence of moves from the initial configuration to the final configuration, they visit every legal arrangement of the  $n$  disks exactly once.

*Proof.* First, I provide the recursive procedure:

1. If  $n = 0$ , return

2. Else:

- (a) move  $n - 1$  disks (all but the one at the bottom on peg  $A$ ) from peg  $A$  to peg  $C$  using auxiliary peg  $B$ ;
- (b) move 1 disk (the one remained on peg  $A$ ) to peg  $B$ ;
- (c) move  $n - 1$  disks from peg  $C$  to peg  $A$  using auxiliary peg  $B$ ;
- (d) move 1 disk from peg  $B$  to peg  $C$ ;
- (e) move  $n - 1$  disks from peg  $A$  to peg  $C$ .

Now, I prove that the procedure requires exactly  $3^n - 1$  steps. The statement holds for  $n = 0$  because  $3^0 - 1 = 1 - 1 = 0$ . For the induction hypothesis, suppose that the statement holds for  $n - 1$ . For the inductive steps, consider the following:

- (a) moving  $n - 1$  disks from  $A$  to  $C$  requires exactly  $3^{n-1} - 1$  steps (by the induction hypothesis);
- (b) moving 1 disk from  $A$  to  $B$  requires exactly 1 step;
- (c) moving  $n - 1$  disks from  $C$  to  $A$  requires exactly  $3^{n-1} - 1$  steps (by the induction hypothesis);
- (d) moving 1 disk from  $B$  to  $C$  requires exactly 1 step;
- (e) moving  $n - 1$  disks from  $A$  to  $C$  requires exactly  $3^{n-1} - 1$  steps (by the induction hypothesis).

In sum, moving  $n$  disks from  $A$  to  $C$  using auxiliary  $B$ , requires exactly

$$(3^{n-1} - 1) + 1 + (3^{n-1} - 1) + 1 + (3^{n-1} - 1) = 3^{n-1} \cdot 3 - 1 = 3^n - 1$$

steps.

Now, I prove the bound  $3^n - 1$  is optimal. The statement holds for  $n = 0$ . As the induction hypothesis, suppose that the statement holds for  $n - 1$ . I show that it holds for  $n$ . I reason as follows:

- (a) to move  $n - 1$  disks from  $A$  to  $C$  using auxiliary  $B$  takes at least  $3^n - 1$  steps (by the induction hypothesis);
- (b) to move 1 disk from  $A$  to  $B$  requires 1 step;
- (c) to move  $n - 1$  disks from  $C$  to  $A$  using auxiliary  $B$  requires at least  $3^n - 1$  steps (by the induction hypothesis);
- (d) to move 1 disk from  $B$  to  $C$  requires 1 step;
- (e) to move  $n - 1$  disks from  $A$  to  $C$  using auxiliary  $B$  requires  $3^n - 1$  steps (by the induction hypothesis).

Therefore, moving  $n$  disks from  $A$  to  $C$  using auxiliary  $B$  requires at least  $3^n - 1$  steps.

Now, I prove that, while carrying out the steps, one goes through all the  $3^n$  legal positions of the disks exactly once. Notice that the statement says two things:

- 1. no legal arrangement is skipped;

2. no legal arrangement is repeated.

The statement holds for  $n = 0$ . Suppose that the statement holds for  $n - 1$ . For the inductive step, notice the following:

When the largest disk is on peg  $X$  (for  $X \in \{A, B, C\}$ ), the other  $n - 1$  disks goes through all the legal arrangements exactly once (by the induction hypothesis).

Therefore, the statement holds for  $n$ . □

**Exercise 6.** (The exercise does not clarify whether the goal is to move the disks to peg 2 or to peg 3.)

*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  $n$ . □

**Exercise 8.**

*Proof.* Part (1).

The solutions to  $x^2 = x + 1$  are  $\alpha = \frac{1+\sqrt{5}}{2}$  and  $\beta = \frac{1-\sqrt{5}}{2}$ . So, the statement holds for  $n = 0$  because

$$\frac{\alpha^0 - \beta^0}{\sqrt{5}} = 0$$

For the inductive hypothesis, suppose that the statement holds for  $n$ . For the inductive step,

consider:

$$\begin{aligned}
 \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} &= \frac{\alpha^{2+n-1} - \beta^{2+n-1}}{\sqrt{5}} \\
 &= \frac{\alpha^2 \alpha^{n-1} - \beta^2 \beta^{n-1}}{\sqrt{5}} \\
 &= \frac{(\alpha + 1)\alpha^{n-1} - (\beta + 1)\beta^{n-1}}{\sqrt{5}} \quad [\text{because } x^2 = x + 1] \\
 &= \frac{\alpha^n + \alpha^{n-1} - \beta^n - \beta^{n-1}}{\sqrt{5}} \\
 &= \frac{(\alpha^n - \beta^n) + (\alpha^{n-1} - \beta^{n-1})}{\sqrt{5}} \\
 &= \frac{\alpha^n - \beta^n}{\sqrt{5}} + \frac{\alpha^{n-1} - \beta^{n-1}}{\sqrt{5}} \\
 &= F_n + F_{n-1} \quad [\text{by induct. hyp.}] \\
 &= F_{n+1} \quad [\text{by defin. of } F_{n+1}]
 \end{aligned}$$

To conclude, I show that interchanging  $\alpha$  and  $\beta$  does not change the result. Let  $\alpha = \frac{1+\sqrt{5}}{2}$  and  $\beta = \frac{1-\sqrt{5}}{2}$ . Since the inductive step does not use the definitions of  $\alpha$  and  $\beta$ , it is enough to observe that, with the new definitions of  $\alpha$  and  $\beta$ , the statement holds for  $n = 0$ .

Part (2).

I reason by induction. For  $n = 0$ ,  $\sum_{i=0}^0 F_i$  is an empty sum, which, by definition, is 0. So, the statement holds for  $n = 0$ . Now, as the inductive hypothesis, suppose that the statement holds for  $n$ . For the inductive step  $n + 1$ , consider:

$$\begin{aligned}
 \sum_{i < n} F_i &= \left( \sum_{i < n-1} F_i \right) + F_n \\
 &= F_{n+1} - 1 + F_n \quad [\text{by induct. hyp.}] \\
 &= F_{n+2} - 1 \quad [\text{by defin. of } F_n]
 \end{aligned}$$

Part(3).

I reason by induction. The statement holds for  $n = 0$ . As the inductive hypothesis, suppose that the statement holds for  $n$ . For the inductive step, consider:

$$\begin{aligned}
 \sum_{i \leq n+1} F_i &= \left( \sum_{i \leq n} F_i \right) + F_{n+1}^2 \\
 &= F_n F_{n+1} + F_{n+1}^2 \quad [\text{by induct. hyp.}] \\
 &= F_{n+1}(F_n + F_{n+1}) \\
 &= F_{n+1} F_{n+2} \quad [\text{by defin. of } F_n]
 \end{aligned}$$

□

### Exercise 9.

*Proof.* Identical to exercise 8 part (1).

□

**Exercise 10.** The exercise contains an oversight (I am using version 0.1). The correct formula is

$$\frac{n^2 + n + 2}{2}.$$

*Proof.* Part 1

First, I prove that the above formula provides an upper bound on the number of the regions of a plane. I reason by induction. Let  $R(n) = \frac{n^2+n+2}{2}$ . Another way of saying it is  $R(n) = \frac{n(n+1)}{2} + 1$ . For  $n = 0$ , there is exactly one partition of the plane (i.e. the plane itself) and  $R(0) = 1$ . Therefore, the statement holds. As the induction hypothesis, suppose that the statement holds for  $n$ . For the inductive step, notice that, at step  $n + 1$ , the plane contains exactly  $n$  straight lines. Therefore, by placing a new straight line on the plane, I can intersect at most  $n$  straight lines. I imagine to draw the new line  $l$  starting from a point and proceeding with equal velocity in both directions so that I intersect the other lines in the order  $l_1, l_2, \dots, l_n$ . For  $i \leq i \leq n$ , every time  $l$  intersects  $l_i$ , it generates a new region of the plane:

1. for  $i = 0$ , the new region is an angle having  $l$  and  $l_0$  as its sides;
2. for  $1 \leq i \leq n$ , the new region is a triangle whose sides are segments lying on  $l$ ,  $l_i$ , and  $l_{i-1}$ ).

Proceeding infinitely beyond  $l_n$ ,  $l$  generates an additional region which is an angle having  $l$  and  $l_n$  as its sides. Therefore, adding a new line to a plane with at most  $n$  regions adds at most  $n + 1$  new regions.<sup>3</sup> Therefore, by the induction hypothesis, at step  $n + 1$ , the total number of regions is at most  $R(n) + n + 1$ . Now, observe the following:

$$\begin{aligned} R(n) + n + 1 &= \frac{n(n+1)}{2} + 1 + n + 1 \\ &= \frac{n(n+1)}{2} + n + 2 \\ &= \frac{n^2 + n + 2n + 4}{2} \\ &= \frac{(n+1)(n+2) + 2}{2} \\ &= \frac{(n+1)(n+2)}{2} + 1 \\ &= R(n+1) \end{aligned}$$

Part 2.

Now, I prove that the upper bound is sharp, i.e. that, for some  $n$ , the number of regions of a plane is equal to  $R(n)$ . It suffices to notice that this is the case for  $n = 1$ .  $\square$

**Exercise 11.**

*Proof.* I reason by induction. Let  $D(n) = \frac{n(n-3)}{2}$ . The base case is  $n = 3$ . The statement holds for  $n = 3$  because a triangle has no diagonals and  $D(0) = 0$ . As the inductive hypothesis, suppose that the statement holds for  $n$ . For the inductive step  $n + 1$ , I use the following claim:

- (C) Let  $C_k$  be a convex  $k$ -gon. The difference between then number of diagonals of  $C_k$  and the number of diagonals of  $C_{k+1}$  is  $n - 1$ .

---

<sup>3</sup>Another way of grasping this is to realize that the already existing  $n$  lines cut the new line  $l$  at most into  $n$  distinct points. Therefore, the already existing lines cut  $l$  into at most  $n + 1$  distinct segments. Each of these segments of  $l$  partitions the plane into a new region. Therefore, adding  $l$  results in at most  $n + 1$  regions of the plane.



I will prove C later. Now, assuming C, I prove the inductive step as follows:

$$\begin{aligned}
 D(n+1) &= D(n) + n - 1 && \text{[by induct. hyp., C]} \\
 &= \frac{n(n-3)}{2} + n - 1 \\
 &= \frac{n^2 - 3n + 2n - 2}{2} \\
 &= \frac{n^2 - n - 2}{2} \\
 &= \frac{(n+1)(n-2)}{2} \\
 &= \frac{(n+1)(n+1-3)}{2}
 \end{aligned}$$

Now, I prove C. Consider a convex  $k$ -gon  $C_k$  and let  $V = \{V_1, \dots, V_k\}$  be the set of its vertices. Let the sides of  $C_k$  be  $V_1V_2, V_2V_3, \dots, V_{k-1}V_k, V_kV_1$ . Let  $C_{k+1}$  be a convex  $k+1$ -gon and let  $W = W_1, \dots, W_k, W_{k+1}$  be the set of vertices of  $C_{k+1}$ . Let the sides of  $C_{k+1}$  be  $W_1W_2, \dots, W_{k-1}W_k, W_kW_{k+1}, W_{k+1}W_1$ . Let  $\tau$  be an injective function that maps  $V_i$  to  $W_i$ . Therefore,  $\tau$  induces an injection  $T$  between the set  $Diag_k$  diagonals of  $C_k$  and the set  $Diag_{k+1}$  of diagonals of  $C_{k+1}$  according to the following formula:

$$T(V_iV_j) = \tau(V_i)\tau(V_j).$$

To prove C, it suffices to show that  $|T(Diag_k)| = k - 1$ . The vertex  $W_{k+1}$  of  $C_{k+1}$  is the only vertex of  $C_{k+1}$  that is not in  $\tau(V)$ . Therefore, every diagonal of  $C_{k+1}$  having  $W_{k+1}$  has one of its endpoints is not in  $T(Diag_k)$ . The diagonals having  $W_{k+1}$  as one of their endpoints are exactly the following:

$$W_{k+1}W_2, W_{k+1}W_3, \dots, W_{k+1}W_{k-1}.$$

These are exactly  $k - 2$  diagonals. Another diagonal that is not in  $T(Diag_k)$  is  $W_1W_k$  (because  $T^{-1}(W_1W_k) = V_1V_k$ , which is a side of  $C_k$ ). For every other segment  $W_iW_j$ , if  $W_iW_j$  is a diagonal of  $C_{k+1}$ , then both  $i \neq k+1, j \neq k+1$ , and  $i \neq j \pm 1$ . Therefore,  $T^{-1}(W_iW_j) = V_iV_j$ . It follows that  $W_iW_j \in T(Diag_k)$ . In sum, there exactly  $k - 1$  diagonals of  $C_{k+1}$  that are not in  $T(Diag_k)$ .  $\square$

### Exercise 12.

*Proof.* As the exercise indicates, in this proof,  $x$  and  $y$  always varies over the non-negative natural numbers. I do *not* use the hint that the exercise provides. I use the following lemma:

(L1) For every natural number  $x$  and  $y$ ,  $d$  divides  $x$  and  $y$  iff  $d$  divides  $\text{mod}(x, y)$  and  $y$ .

I prove (L1). Suppose that  $d \mid x$  and  $d \mid y$ . Therefore, for some  $a$  and  $b$ ,  $x = ad$  and  $y = bd$ . By definition,  $y \mid x - \text{mod}(x, y)$ . Therefore, for some  $c$ ,  $x - \text{mod}(x, y) = cy = cbd$ . Therefore,

$$x - cbd = ad - cbd = d(a - cb) = \text{mod}(x, y).$$

Therefore  $d \mid \text{mod}(x, y)$ . Now suppose that  $d \mid y$  and  $d \mid \text{mod}(x, y)$ . Therefore, for some  $a$  and  $b$ ,  $\text{mod}(x, y) = ad$  and  $y = bd$ . By definition,  $\text{mod}(x, y)$  is the least integer such that  $y \mid x - \text{mod}(x, y)$ . Therefore, for some  $c$ ,

$$\begin{aligned}
 x - \text{mod}(x, y) &= cy \\
 &= cbd.
 \end{aligned} \tag{2.1}$$

Therefore  $x = cbd - \text{mod}(x, y) = cbd - ad = d(cb - a)$ . Therefore,  $d \mid x$ .

Let  $\text{Div}(x, y)$  be the set of exactly all divisors of  $x$  and  $y$ . From (L1), it follows that  $\text{Div}(x, y) = \text{Div}(y, \text{mod}(x, y))$ .

Now, consider the definition of  $\text{gcd}(x, y)$ . When  $y = 0$ ,  $\text{gcd}(x, y) = x$ , which is the greatest integer dividing both  $x$  and  $y$ . When  $y > 0$ ,  $\text{gcd}(x, y) = \text{gcd}(y, \text{mod}(x, y))$ . Continuing the process, eventually, for some integer  $r$ , one reaches  $\text{gcd}(x, y) = \text{gcd}(r, 0)$ . By (L1) and the definition of  $\text{gcd}()$ ,  $\text{Div}(x, y) = \text{Div}(r, 0)$ .  $r$  is the greatest element in  $\text{Div}(r, 0)$  and, by definition of  $\text{gcd}()$ ,  $\text{gcd}(r, 0) = r$ . Therefore  $\text{gcd}(x, y)$  is the greatest divisor of  $x$  and  $y$ .  $\square$

Note. The exercise mentions a few more lemmas that are useful to solve the exercise in some other ways. I did not use these lemmata, which are the following:

(L1) For every natural numbers  $x, y$ ,  $\text{gcd}(x, y) = \text{gcd}(x + y, y)$ .

(L2) For every natural numbers  $x, y, k$ ,  $\text{gcd}(x, y) = \text{gcd}(x + ky, y)$ .

(L3) For every natural numbers  $x, y$ , if  $y > 0$ , then  $x = \left\lfloor \frac{x}{y} \right\rfloor y + \text{mod}(x, y)$ .

For completeness, I prove these lemmata here.

*Proof.* First, I prove (L1). Suppose that  $d = \text{gcd}(x, y)$ . Therefore, for some  $a$  and  $b$ ,  $x = ad$  and  $y = bd$ . Therefore,  $x + y = d(a + b)$  and  $d$  divides  $x + y$  too. Now, suppose that  $d = \text{gcd}(x + y, y)$ . Therefore, for some  $a$  and  $b$ ,  $x + y = ad$  and  $y = bd$ . Therefore,  $a = a + y - y = ad - bd = d(a - b)$  and  $d$  divides  $x + 1$  and  $y$  too.

Now, I prove (L2). I reason by induction. The statement holds for  $k = 0$ . As the induction hypothesis, suppose that the statement holds for  $k = n$ . For the inductive step, consider

$$\begin{aligned}
 \text{gcd}(x + (k + 1)y, y) &= \text{gcd}(x + kn + y, y) \\
 &= \text{gcd}((x + kn) + y, y) \\
 &= \text{gcd}(x + kn, y) && \text{[by (L1)]} \\
 &= \text{gcd}(x, y) && \text{[by induct. hyp.]}
 \end{aligned}
 \tag{2.2}$$

Now, I prove (L3). By definition,  $\text{mod}(x, y)$  is the unique integer  $r$  such that  $y \mid x - r$ . Therefore,

$$\left\lfloor \frac{x}{y} \right\rfloor y + \text{mod}(x, y) = \frac{x - \text{mod}(x, y)}{y} y + \text{mod}(x, y) = x - \text{mod}(x, y) + \text{mod}(x, y) = x.$$

$\square$

### Exercise 13.

*Proof.*

$\square$

### Exercise 14.

*Proof.* See the proof of theorem 2.7.

$\square$

### Exercise 15.

*Proof.* □

**Exercise 16.**

*Proof.* See the proof of theorem [2.8](#). □

**Exercise 17.**

*Proof.* See the proof of theorem [2.9](#). □

**Exercise 18.**

*Proof.* □

**Exercise 19.**

*Proof.* □

**Exercise 20.**

*Proof.* □

**Exercise 21.**

*Proof.* □

# Appendix A

## Errata

page	exercise	errata	corrigé
6	5	we principles	we apply the principles
7		there is part	there is a part
11		is requires	it requires

Table A.1: Errata

Comments:

1. The statement of exercise 5 in chapter 2 (p. 10) should include that the goal of the modified Hanoi is to move the disks from peg 1 to peg 3.
2. The statement of exercise 6 in chapter 2 (p. 10) should specify whether the goal is to move the disks to peg 2 or to peg 3.
3. Exercise 9 is identical to exercise 8.a.
4. The formula in exercise 10 should be

$$\frac{n^2 + n + 2}{2}.$$