Staff Solutions to Problem Set 3

Reading: Chapter 5. on Induction and Chapter 6. on Recursive Data Types

Problem 1.
Let \( N \) be a number whose decimal expansion consists of \( 3^n \) identical digits. Show by induction that \( 3^n \mid N \).

For example:

\[
\begin{align*}
3^2 & \mid 777777777 \\
3^2 & = 9 \text{ digits}
\end{align*}
\]

Recall that 3 divides a number iff it divides the sum of its digits.

Solution. We proceed by induction on \( n \). Let \( P(n) \) be the proposition that \( 3^n \mid N \), where the decimal expansion of \( N \) consists of \( 3^n \) identical digits.

Base case. \( P(0) \) is true because \( 3^0 = 1 \) divides every number.

Inductive step. Now we show that, for all \( n \geq 0 \), \( P(n) \) implies \( P(n+1) \). Fix any \( n \geq 0 \) and assume \( P(n) \) is true. Consider a number whose decimal expansion consists of \( 3^{n+1} \) copies of the digit \( a \):

\[
\begin{align*}
\underbrace{aaaaa \ldots aaaaa}_{3^{n+1} \text{ digits}} &= \underbrace{aaa \ldots aaa}_{3^n \text{ digits}} \underbrace{aaa \ldots aaa}_{3^n \text{ digits}} \underbrace{aaa \ldots aaa}_{3^n \text{ digits}} \\
&= \frac{\underbrace{aaa \ldots aaa}_{3^n \text{ digits}}}{1000 \ldots 001} \underbrace{1000 \ldots 001}_{3^n \text{ digits}}
\end{align*}
\]

Now \( 3^n \) divides the first term by the assumption \( P(n) \), and 3 divides the second term since the digits sum to 3. Therefore, the whole expression is divisible by \( 3^{n+1} \). This proves \( P(n+1) \).

By the principle of induction \( P(n) \) is true for all \( n \geq 0 \).

Problem 2.
The Fibonacci numbers \( F_0, F_1, F_2, \ldots \) are defined as follows:

\[
F_n := \begin{cases} 
0 & \text{if } n = 0, \\
1 & \text{if } n = 1, \\
F_{n-1} + F_{n-2} & \text{if } n > 1.
\end{cases}
\]

Prove, using strong induction, the following closed-form formula for \( F_n \):

\[
F_n = \frac{p^n - q^n}{\sqrt{5}}
\]

where \( p = \frac{1+\sqrt{5}}{2} \) and \( q = \frac{1-\sqrt{5}}{2} \).

Hint: Note that \( p \) and \( q \) are the roots of \( x^2 - x - 1 = 0 \), and so \( p^2 = p + 1 \) and \( q^2 = q + 1 \).
Solution. Proof. We will proceed by strong induction on \( n \). Let the induction hypothesis, \( P(n) \), be that the given closed-form formula holds at \( n \), that is,

\[
F_n = \frac{p^n - q^n}{\sqrt{5}}.
\]

**Base case** \((n = 0)\): \( P(0) \) is true, since

\[
\frac{p^0 - q^0}{\sqrt{5}} = \frac{1 - 1}{\sqrt{5}} = 0 = F_0.
\]

**Base Case** \((n = 1)\): \( P(1) \) is true, since

\[
\frac{p^1 - q^1}{\sqrt{5}} = \frac{p - q}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = F_1.
\]

**Inductive Step** \((n > 1)\):

Since \( 0 \leq n - 1, n < n + 1 \), we may assume the strong induction hypothesis that \( P(n - 1) \) and \( P(n) \) are both true. We will use this to prove \( P(n + 1) \).

That is, we may assume

\[
F_{n-1} = \frac{p^{n-1} - q^{n-1}}{\sqrt{5}} \quad (1)
\]

\[
F_n = \frac{p^n - q^n}{\sqrt{5}} \quad (2)
\]

From the hint we have that \( p^2 = p + 1 \), which implies that \( p^2 p^{n-1} = (p + 1) p^{n-1} \) and so

\[
p^{n+1} = p^n + p^{n-1} \quad (4)
\]

Likewise \( q^2 = q + 1 \), and so

\[
q^{n+1} = q^n + q^{n-1} \quad (5)
\]

Subtracting (5) from (4) gives

\[
p^{n+1} - q^{n+1} = p^n - q^n + p^{n-1} - q^{n-1}
\]

and dividing by \( \sqrt{5} \) yields

\[
\frac{p^{n+1} - q^{n+1}}{\sqrt{5}} = \frac{p^n - q^n}{\sqrt{5}} + \frac{p^{n-1} - q^{n-1}}{\sqrt{5}} = F_n + F_{n-1} \quad \text{(by (1) and (2))} \quad (6)
\]

But \( F_{n+1} = F_n + F_{n-1} \) for \( n > 1 \) by definition, so (6) implies

\[
F_{n+1} = \frac{p^{n+1} - q^{n+1}}{\sqrt{5}}.
\]

That is, \( P(n + 1) \) is true in this case as well.

We conclude by strong induction that \( P(n) \) holds for all \( n \in \mathbb{N} \).
Problem 3.
Suppose that you have a regular deck of cards arranged as follows, from top to bottom:

\[ A \heartsuit 2 \heartsuit \ldots K \heartsuit A \clubsuit 2 \clubsuit \ldots K \clubsuit A \spadesuit 2 \spadesuit \ldots K \spadesuit \]

Only two operations on the deck are allowed: *inshuffling* and *outshuffling*. In both, you begin by cutting the deck exactly in half, taking the top half into your right hand and the bottom into your left. Then you shuffle the two halves together so that the cards are perfectly interlaced; that is, the shuffled deck consists of one card from the left, one from the right, one from the left, one from the right, etc. The top card in the shuffled deck comes from the right hand in an outshuffle and from the left hand in an inshuffle.

(a) Model this problem as a state machine.

Solution. Let the set of states \( Q \) be all the possible orderings of the deck of cards. Let the set of start states \( Q_0 \) consist of the single ordering listed above. For each state \((c_1, \ldots, c_{52}) \in Q\), there are two transitions in \( \delta \):

\[
(c_1, \ldots, c_{52}) \rightarrow (c_1, c_{27}, c_2, c_{28}, \ldots, c_{26}, c_{52})
\]
\[
(c_1, \ldots, c_{52}) \rightarrow (c_{27}, c_1, c_{28}, c_2, \ldots, c_{52}, c_{26})
\]

(b) Use the Invariant Principle to prove that you cannot make the entire first half of the deck black through a sequence of inshuffles and outshuffles.

Solution. Define two cards to be *opposites* if the sum of their positions is 53. For example, the top card is opposite the bottom card, the second card from the top is opposite the second from the bottom, etc.

Let \( P \) be the property that \( A \heartsuit \) is opposite \( K \spadesuit \), \( 2 \heartsuit \) is opposite \( Q \heartsuit \), etc., as in the initial configuration. We claim that \( P \) is a preserved invariant. Suppose that \( P \) holds for a given state and consider the two types of transition out of that state. Note that, for both types of transition, cards in opposite positions are mapped to opposite positions. Therefore, the property \( P \) still holds. Thus, \( P \) is preserved.

If the above explanation doesn’t convince you, consider this arithmetical justification: Consider two cards at positions \( i \) and \( j \) that are correctly paired in some configuration. Without loss of generality, let \( i \) be the earlier of the two positions. We know \( i + j = 53 \), so we can simply talk about positions \( i \) and \( 53 - i \). Considering the first of the transitions shown in part (a)’s solution, we can see that:

- A card at position \( k \) in the first half of the deck is moved to position \( 2k - 1 \)
- A card at position \( k \) in the second half of the deck is moved to position \( 2(k - 26) \)

Thus, the new position of the card from position \( i \) is \( 2i - 1 \), and the position of the other card is \( 2(j - 26) = 2(53 - i - 26) = 54 - 2i \). It is easy to see that the two new positions sum to 53, so the invariant is maintained for this pair of matched cards. Since we imposed no further conditions on the pair we chose, we see that any shuffle of this variety preserves the invariant; and the reasoning for the other sort of shuffle is analogous.

We finish by noting that \( P \) holds for the start state by definition. However, \( P \) cannot hold when all black cards are in the top half of the deck; in that case, every black card is opposite a red card, which was not true for any cards in the original configuration. Therefore, by the Invariant Principle, that state is not reachable.

Note: Discovering a suitable invariant can be difficult! The standard approach is to identify a bunch of reachable states and then look for a pattern, some feature that they all share.
Problem 4.

**Definition.** The set RAF of rational functions of one real variable is the set of functions defined recursively as follows:

**Base cases:**
- The identity function, id\(r\) := \(r\) for \(r \in \mathbb{R}\) (the real numbers), is an RAF,
- any constant function on \(\mathbb{R}\) is an RAF.

**Constructor cases:** If \(f, g\) are RAF’s, then so are

1. \(f + g\), \(fg\), and \(f/g\).

(a) Prove by structural induction that RAF is closed under composition. That is, using the induction hypothesis,

\[ P(h) ::= \forall g \in \text{RAF}. h \circ g \in \text{RAF}, \]

prove that \(P(h)\) holds for all \(h \in \text{RAF}\). Make sure to indicate explicitly

- each of the base cases, and
- each of the constructor cases.

**Solution.**

**Proof. base cases:** We must show \(P(id_{\mathbb{R}})\) and \(P(\text{constant-function})\). But this follows immediately from the fact that \(id_{\mathbb{R}} \circ g = g\) and the composition of a constant function with any function, \(g\), is constant.

**constructor cases:** Given \(e, f \in \text{RAF}\), we may assume by structural induction that \(P(e)\) and \(P(f)\) both hold, and must prove \(P(h)\) for \(h = e \circ f\) in the three cases where \(\circ = +, \cdot, \text{or } \div\). But the same proof works for all three cases:

\[ (e \circ f) \circ g = (e \circ g) \circ (f \circ g) \]

(by definition of composition), and since \((e \circ g), (f \circ g) \in \text{RAF}\) for all \(g \in \text{RAF}\) by hypothesis, so is their combination using the operator \(\circ\) – that is, their sum/product/quotient – by the constructor rule (1). This proves \(P(h)\) for all three of the constructor cases \(\circ = +, \cdot, \text{or } \div\).

This completes all the constructor cases, and so \(\forall h \in \text{RAF}. P(h)\) follows by structural induction.

(b) Briefly explain why a similar proof using the induction hypothesis

\[ Q(g) ::= \forall h \in \text{RAF}. h \circ g \in \text{RAF}, \]

would break down.

**Solution.** The problem is that the identity used in the induction step of the previous part, namely that composition distributes from the left over each constructor operation \(\circ\), breaks down for composition on the right. For example,

\[ h \circ (g_1 + g_2) = (h \circ g_1) + (h \circ g_2) \]

fails when \(h\) is nonlinear. For example, if \(h(x) := x^2\), and \(g_1 = g_2 = id_{\mathbb{R}}\), then

\[ [f \circ (g_1 + g_2)](r) = (2r)^2 = 4r^2 \]

\[ \neq 2r^2 = r^2 + r^2 \]

\[ = [(f \circ g_1) + (f \circ g_2)](r). \]
So even though the conclusion $\forall g. Q(g)$ is true, a direct proof using $Q(g)$ as the induction hypothesis quickly gets stuck.