Exercises 5 — induction and recursion

1.

Show by simple induction that for every positive integer n, $5^n - 1$ is divisible by 4.
(SLAM Exercise 4.1)

Basis, n = 1:

Induction step from n to n+1:

2.

Let us use $\mathbb{P}$ as the name for the set of all prime numbers, that is positive integers greater than 1 that are only divisible by 1 and themselves, so $\mathbb{P} = \{2, 3, 5, 7, 11, 13, ...\}$. You can use $\mathbb{P}$ in answering the following questions, and also the "divides" relation, defined as $a|b$ iff $\exists k(k \in \mathbb{N}^+ \wedge ka = b)$.

1. The number *n primorial* is the product of all prime numbers less than or equal to n, i.e. $\prod\{p \in \mathbb{P} : p \leq n\}$. Let us call the function that computes n primorial P, so for example, $P(3) = 2 \cdot 3 = 6$, $P(4) = 2 \cdot 3 = 6$, $P(5) = 2 \cdot 3 \cdot 5 = 30$, $P(6) = 2 \cdot 3 \cdot 5 = 30$, $P(7) = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ and so forth. The first primorial number is defined to be $P(1) = 1$.
   Using **simple recursion**, give a definition of the function $P : \mathbb{N}^+ \longrightarrow \mathbb{N}^+$ computing n primorial for any $n \in \mathbb{N}^+$, as follows:

$$P : n \mapsto \begin{cases} 1 & \text{for } n = 1 \\ & \text{for } n > 1, n \notin \mathbb{P} \\ & \text{for } n > 1, n \in \mathbb{P} \end{cases}$$

2. Is the function $P : \mathbb{N}^+ \longrightarrow \mathbb{N}^+$… (circle the answer)

   (a) injective? YES NO

   (b) surjective? YES NO

3. Using **simple recursion**, define an **injective function** $Q : \mathbb{N}^+ \hookrightarrow \mathbb{P}$.
   Use the fact that for any $k \in \mathbb{N}^+$, the number $P(k) + 1$ is a prime number (a so-called *primorial prime*).
   Hint: It's NOT as simple as mapping n to $P(n) + 1$. (Make sure you understand why that is)

$$Q : n \mapsto \begin{cases} P(1) + 1 & \text{for } n = 1 \\ & \text{for } n > 1 \end{cases}$$

4. Prove that Q above is injective.
   You may use the fact that $n \leq P(n)$ for all $n \in \mathbb{N}^+$ without needing to prove it.
   Hint: Answering this might become easier if you use a result from a previous task.

3.

Recall that $\{0,1\}^*$ is the set of all finite sequences of 0s and 1s. Define an **injective** function $f : \{0,1\}^* \hookrightarrow \mathbb{N}$.

Keep in mind that sequences of 0s and 1s may start and end with any number of 0s, so interpreting the string simply as a binary number is not going to result in an injective function, because 00100100 and 100100 would be mapped to the same natural number.

Use recursion over the structure of the sequence, as follows. The first case deals with the empty sequence, the other two cases “peel off” the first element in the sequence and the rest of the sequence is called s'.

$$f : s \mapsto \begin{cases} & \text{for } s = \varepsilon \\ & \text{for } s = 0s', s' \in \{0,1\}^* \\ & \text{for } s = 1s', s' \in \{0,1\}^* \end{cases}$$

4.

As above, $\{0,1\}^*$ is the set of all finite sequences of 0s and 1s. Define an **injective** function $g : \mathbb{N} \hookrightarrow \{0,1\}^*$.

Use recursion over $\mathbb{N}$, as follows. The first case deals with 0, the other with positive numbers, where you can use the values for smaller numbers.

$$g : n \mapsto \begin{cases} & \text{for } n = 0 \\ & \text{for } n > 0 \end{cases}$$

5.

Let $A = \{a, b, c\}$ and $X = \{x, y\}$, and correspondingly A^* and X^* be the sets of finite sequences in A and X, respectively.

Using recursion over the structure of the sequence, define two **injections** $f : X^* \hookrightarrow A^*$ and $g : A^* \hookrightarrow X^*$, as follows. In both definitions, the first case deals with the empty sequence, the other cases “peel off” the first element in the sequence and the rest of the sequence is called s'.

$$f : s \mapsto \begin{cases} & \\ & \\ & \end{cases} \quad \begin{array}{l} \text{for } s = \varepsilon \\ \text{for } s = xs', s' \in X^* \\ \text{for } s = ys', s' \in X^* \end{array}$$

$$g : s \mapsto \begin{cases} & \\ & \\ & \\ & \end{cases} \quad \begin{array}{l} \text{for } s = \varepsilon \\ \text{for } s = as', s' \in A^* \\ \text{for } s = bs', s' \in A^* \\ \text{for } s = cs', s' \in A^* \end{array}$$

6.

Consider the lower-case alphabet $A = \{"a", ..., "z"\}$ and the set
$C = A \cup \{"(", ")", "\neg", " \vee ", " \wedge "\}$ of characters.
We define a small language $\mathcal{L} \subseteq C^*$ of propositional formulae over the set of variable names $V = A^* \setminus \{\varepsilon\}$, and the following set of rules $R = \{R_1, R_2, R_3\}$ with

$$R_1 = \{(s, "\neg" s) : s \in C^*\}$$
$$R_2 = \{(s_1, s_2, "(" s_1 " \vee " s_2 ")") : s_1, s_2 \in C^*\}$$
$$R_3 = \{(s_1, s_2, "(" s_1 " \wedge " s_2 ")") : s_1, s_2 \in C^*\}$$

such that $\mathcal{L} = R[V]$.

1. Show that $\mathcal{L} \subset C^*$ by giving a string $s \in C^*$ such that $s \notin \mathcal{L}$:

   $s =$

2. Give three strings $s_1, s_2, s_3 \in C^* \setminus \mathcal{L}$ such that $(s_1, s_2, s_3) \in R_3$:

   $s_1 =$

   $s_2 =$

   $s_3 =$

3. Assume a function $E : V \longrightarrow \{0, 1\}$ that assigns every variable name a value in $\{0, 1\}$. Using **structural recursion**, define an evaluation function $\mathrm{eval}_E : \mathcal{L} \longrightarrow \{0, 1\}$ that interprets the formulae in $\mathcal{L}$ in a way consistent with the usual interpretation of the symbols $\neg$ (not), $\vee$ (or), and $\wedge$ (and) in propositional logic. **Use arithmetic operators (+, -, *, min, max) to compute with the values 0 and 1.**

$$\mathrm{eval}_E : s \mapsto \begin{cases} & \text{for } s \in V \\ & \text{for } s = \neg s' \\ & \text{for } s_1, s_2 \in \mathcal{L}, s = (s_1 \vee s_2) \\ & \text{for } s_1, s_2 \in \mathcal{L}, s = (s_1 \wedge s_2) \end{cases}$$

7.

Suppose we have a set of five characters $C = \{"a", "b", "(", ")", ",", "\}$, the set $S = \{"a", "b"\}$ consisting only of the letters a and b, and a relation $R = \{(s_1, s_2, "("s_1", "s_2")") : s_1, s_2 \in C^*\}$.

As you can see, R is a 3-place relation. Let us define a function $F : \mathcal{P}(C^*) \longrightarrow \mathcal{P}(C^*)$ such that

$$F : X \mapsto R(X \times X)$$

In other words, $F(X) = \{y : x_1, x_2 \in X, (x_1, x_2, y) \in R\}$.

Now let $F^n(X)$ be the set that results from applying F to some set $X \subseteq C^*$ n times in a row, with $F^0(X) = X$, $F^1(X) = F(X)$, $F^2 = F(F(X))$ and so forth, so that $F^{n+1}(X) = F(F^n(X))$.

1. Give an element in $F^0(S)$:

2. Give an element in $F^1(S)$:

3. Give an element in $F^2(S)$:

4. Suppose $U = \bigcup_{n \in \mathbb{N}} F^n(S)$.

   Give an element in $R[S] \setminus U$, or write “none” if no such element exists:

8.

Suppose we have a set A partially ordered by a strict order $<$. What would you need to show in order to demonstrate that $(A, <)$ is **not** well-founded? (in English/Swedish)

9.

1. Is the set $\mathcal{P}(\mathbb{Q})$ under strict set inclusion $\subset$ well-founded? (circle answer)

   YES NO

2. Prove it or provide a counterexample.

3. Is the set $\mathcal{P}(\mathbb{N})$ under strict set inclusion $\subset$ well-founded? (circle answer)

   YES NO

4. Prove it or provide a counterexample.

10.

Let the set $\mathbb{S}$ be the set of all finite strings consisting of lower-case characters from a to z, including the empty string “”. So, for example, “abc”, “string”, and “ordered” are all members of $\mathbb{S}$.
The *length* of a string is the number of characters in it. We shall use $\mathrm{len}(s)$ for the number of characters in s. Note that $\mathrm{len}(\text{“”}) = 0$.

Let < be the **strict prefix order** on $\mathbb{S}$. This means that for any two strings s and t, we have $s < t$ if and only if s is a proper prefix of t, i.e. t starts with s and then contains at least one more character. For example, $\text{“}abc\text{”} < \text{“}abcd\text{”}$ and $\text{“”} < \text{“}xyz\text{”}$, but $\text{“}abc\text{”} \not< \text{“}abc\text{”}$, $\text{“}ab\text{”} \not< \text{“}xyz\text{”}$ and of course $\text{“}xyz\text{”} \not< \text{“”}$.

Note that for any two strings s and t, it is always the case that $s < t \Rightarrow \mathrm{len}(s) < \mathrm{len}(t)$.

1. $(\mathbb{S}, <)$ is partially / totally ordered (circle the one that applies).

   (For the purposes of this question, “partially” should be understood as the opposite of “totally”, rather than as its generalization.)

2. Is $(\mathbb{S}, <)$ well-founded? (circle answer)

   YES NO