Homework 4

Discrete Structures
Due Tuesday, February 2, 2021

Submit each question separately in .pdf format only

1. Consider the sets $X_{1,1} = \{1\}$, $X_{2,1} = \{1,2\}$, $X_{2,2} = \{1,2\} \times \{1,2\}$, and in general,

$$X_{n,m} = \underbrace{\{1,2,\dots,n\} \times \cdots \times \{1,2,\dots,n\}}_{m \text{ times}}.$$

Recall that $\mathbf{N} = \{1,2,\dots,\}$, and let $\mathbf{N}' = \mathbf{N} \cup \{0\} = \{0,1,2,\dots\}$.

(a) How many elements are there in $X_{n,m}$? Justify your answer.

There are n^m elements. This follows from the properties of the Cartesian product. That is,

$$\begin{aligned} |X_{n,m}| &= |\{1,\dots,n\} \times \cdots \times \{1,\dots,n\}| \\ &= |\{1,\dots,n\}| \cdots |\{1,\dots,n\}| \\ &= |\{1,\dots,n\}|^m \\ &= n^m. \end{aligned}$$

□

(b) Let rem: $\mathbf{N} \times \mathbf{N} \to \mathbf{N}'$ be the remainder function. That is, $f(n,m)$ is the remainder when n is divided by m. Prove that rem is surjective by finding at least one element in the preimage $f^{-1}(n)$, for any $n \in \mathbf{N}'$.

The preimage $f^{-1}(n)$ has many elements, one of which is $(n, n+1)$. If $n = 0$, then $(1,1) \in f^{-1}(0)$. □

(c) Using rem, define a surjective function $f\colon \mathbf{N} \to X_{2,2}$ for which the preimages $f^{-1}(b)$ all have infinitely many elements, for every $b \in X_{2,2}$.

There are many such functions, one is

$$f(n) = \begin{cases} (1,1) & \text{if } \mathrm{rem}(n,4) = 0, \\ (1,2) & \text{if } \mathrm{rem}(n,4) = 1, \\ (2,1) & \text{if } \mathrm{rem}(n,4) = 2, \\ (2,2) & \text{if } \mathrm{rem}(n,4) = 3. \end{cases}$$

□

(d) What is the range of $g\colon X_{n,2} \to \mathbf{N}'$, given by $g(b_1,b_2) = \mathrm{rem}(b_1,b_2)$?

The range is $\{0,\dots,n-1\}$, because $g(1,1) = 0$ and $g(k,k+1) = k$ for every $k = 1,\dots,n-1$. There can be no value $g(b_0,b_1) = n$, because dividing a number by another number must leave a remainder strictly smaller than the number being divided. □

(e) What is the range of $h\colon X_{n,3} \to \mathbf{N}'$, given by $h(b_1, b_2, b_3) = \mathrm{rem}(\mathrm{rem}(b_1, b_2), b_3)$?

The range is $\{0, \ldots, n-2\}$ for the same reasons as above. □

2. Let $\mathcal{M}$ be the set of all 2×2 matrices filled with real numbers. Define a function $f\colon \mathcal{M} \to \mathbf{R}$ for which $f\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = a \cdot d - b \cdot c$.

(a) Is the function f surjective? Justify your answer.

Function $f(M) = a \cdot d - b \cdot c$ is surjective, because any real number $x \in \mathbf{R}$ is a determinant for some matrix. Consider, for example, matrix $f\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) = x \cdot 1 - 0 \cdot 0 = x$. □

(b) Is the function f injective? Justify your answer.

This particular function from $\mathcal{M}$ to $\mathbf{R}$ is not injective, since there are many matrices with the same determinant. For example, let $x, y \in \mathbf{R}$ be any real numbers. In this case

$$f\begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix} = x \cdot 1 - 0 \cdot y = x.$$

We can see that regardless of y, we always get the same determinant x; so multiple matrixes $M_1 \neq M_2$ can satisfy $f(M_1) = f(M_2)$. It is a collision, but injective functions do not have collisions.

□

(c) Is the function f bijective? Justify your answer.

Function f is not bijective, since it is not injective (see the previous item).

□

(d) Prove that $|\mathbf{R}| \leqslant |\mathcal{M}|$ by defining an injection $g\colon \mathbf{R} \to \mathcal{M}$.

It is quite simple to define a function from real numbers $\mathbf{R}$ to matrices $\mathcal{M}$ without collisions (the opposite direction is harder). We could take, for example,

$$g(x) = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

In this example every number $x \in \mathbf{R}$ maps to a matrix that contains the same number x four times. Clearly, different numbers $x_1 \neq x_2$ will get different matrices. We can also define another function (like the example above):

$$g_2(x) = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}.$$

This is also free of collisions; so it is injective.

□

(e) Prove or disprove that $|\mathbf{R}| = |\mathcal{M}|$.

First prove that $|\mathcal{M}| \leqslant |\mathbf{R}|$.
We want to find an injective function $h : \mathcal{M} \to \mathbf{R}$. The function h can be built as a composition of two injective functions.
Step 1. First "squeeze" all four numbers in a matrix $M \in \mathcal{M}$ into interval $(0; 1)$. We can use a one-to-one continuous function from $\mathbf{R}$ to $(0; 1)$:

$$\phi(x) = \frac{1}{\pi}\left(\arctan x + \frac{\pi}{2}\right).$$

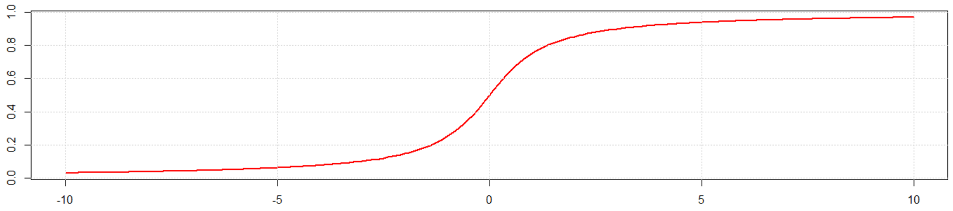

Figure 1: Mapping $\mathbf{R}$ to $(0; 1)$ using a bijection.

$\phi(x)$ is injective function, because it is a continuous and strictly growing one. Its derivative:

$$\phi'(x) = \frac{1}{\pi} \cdot \frac{1}{(x + \pi/2)^2 + 1} > 0, \quad \text{for all } x \in \mathbf{R}.$$

Therefore, for any $x_1 < x_2$ we have $\phi(x_1) < \phi(x_2)$; there will never be any collisions (equal values for different arguments $x_1 \neq x_2$), since one of them will be smaller than another one.
Note. Certainly, there are many other injective functions mapping $\mathbf{R}$ to $(0; 1)$.
We now apply the same function ϕ to all 4 numbers in a matrix.

Step 2. Once all 4 numbers of some matrix M are in the interval $(0, 1)$ write them as infinite decimal fractions:

$$\begin{array}{rcl} \phi(a) & = & 0.\mathtt{a}_1\mathtt{a}_2\mathtt{a}_3\mathtt{a}_4\mathtt{a}_5\mathtt{a}_6\ldots \\ \phi(b) & = & 0.\mathtt{b}_1\mathtt{b}_2\mathtt{b}_3\mathtt{b}_4\mathtt{b}_5\mathtt{b}_6\ldots \\ \phi(c) & = & 0.\mathtt{c}_1\mathtt{c}_2\mathtt{c}_3\mathtt{c}_4\mathtt{c}_5\mathtt{c}_6\ldots \\ \phi(d) & = & 0.\mathtt{d}_1\mathtt{d}_2\mathtt{d}_3\mathtt{d}_4\mathtt{d}_5\mathtt{d}_6\ldots \end{array} \tag{1}$$

Here all the digits $\mathtt{a}_i, \mathtt{b}_i, \mathtt{c}_i, \mathtt{d}_i$ are between 0 and 9.
Note. Some numbers might have multiple representations. For example, $1/4$ is both $0.250000\ldots$ and also $0.249999\ldots$. In these cases we never use 9-period. This is necessary just to ensure that our function is well-defined and injective; so there should be no chance that the same number will be mapped to two different values.

Step 3. Finally, encode the digits found the 4 infinite numbers in (**??**) as one infinite number:

$$h(\phi(a), \phi(b), \phi(c), \phi(d)) = 0.\underbrace{a_1 b_1 c_1 d_1}\underbrace{a_2 b_2 c_2 d_2}\underbrace{a_3 b_3 c_3 d_3}\ldots. \tag{2}$$

The values of $h(\phi(a), \phi(b), \phi(c), \phi(d))$ in (**??**) are all in the interval $(0; 1)$, but some values are not used. For example $0.00090009\ldots = 1/1111$ is a number that is impossible to get, since we never use $0.999\ldots$ (9 period) to encode $\phi(d)$. Therefore the function h is an injection (different matrices are mapped to different numbers), but it is not a bijection.

In order to prove that $|\mathbf{R}| = |\mathcal{M}|$ we could do elaborate tricks (similar to Hilbert's Hotel reseatings) to ensure that there is a bijection. But there is a simpler way: $|\mathbf{R}| = |\mathcal{M}|$ follows from the two set inequalities $|\mathbf{R}| \leqslant |\mathcal{M}|$ and $|\mathbf{R}| \geqslant |\mathcal{M}|$ by Schröder–Bernstein theorem. So, whenever you have injections in both directions between two sets (in our case $\mathbf{R}$ and $\mathcal{M}$, you can also claim that there is a bijection between the two sets.

□

Note. The expression $a \cdot d - b \cdot c$ is called the determinant *of M.*

3. You may assume that there exists a bijection $f\colon (0,1) \to [0,1)$.

(a) Find a bijection between $(0,\infty)$ and $(0,1)$.

There are many such bijections, one is:

$$\begin{array}{rcl} g\colon (0,\infty) & \to & (0,1), \\ x & \mapsto & e^{-x}, \end{array} \qquad \begin{array}{rcl} g^{-1}\colon (0,1) & \to & (0,\infty), \\ y & \mapsto & -\ln(y). \end{array}$$

By the properties of the logarithm, $g^{-1}(g(x)) = x$ for all $x \in (0,\infty)$ and $g(g^{-1}(y))$ for all $y \in (0,1)$. □

(b) Find a bijection between $[0,\infty)$ and $[0,1)$.

There are many such bijections, one is:

$$\begin{array}{rcl} h\colon [0,\infty) & \to & [0,1), \\ x & \mapsto & \begin{cases} g(x) & x \neq 0 \\ 0 & x = 0 \end{cases} \end{array} \qquad \begin{array}{rcl} h^{-1}\colon [0,1) & \to & [0,\infty), \\ y & \mapsto & \begin{cases} g^{-1}(y) & y \neq 0 \\ 0 & y = 0 \end{cases} \end{array}$$

This is a bijection by the previous question. □

(c) Find a bijection between $(0,\infty)$ and $[0,\infty)$.

There are many such bijections, one is:

$$\begin{array}{rcl} k\colon (0,\infty) & \to & [0,\infty), \\ x & \mapsto & h^{-1}(f(g(x))) \end{array} \qquad \begin{array}{rcl} k^{-1}\colon [0,\infty) & \to & (0,\infty), \\ y & \mapsto & g^{-1}(f^{-1}(h(y))) \end{array}$$

□

(d) Find a bijection between $(0,\infty)$ and $\mathbf{R}$.

There are many such bijections, one is:

$$\begin{array}{rcl} \varphi\colon (0,\infty) & \to & \mathbf{R}, \\ x & \mapsto & \begin{cases} g^{-1}(x) & x \in (0,1) \\ -k(x-1) & x \in (1,\infty) \end{cases} \end{array} \qquad \begin{array}{rcl} \varphi^{-1}\colon \mathbf{R} & \to & (0,\infty), \\ y & \mapsto & \begin{cases} g(y) & y > 0 \\ 1 + k^{-1}(-y) & y \leqslant 0 \end{cases} \end{array}$$

□

(e) Find a bijection between $\mathbf{R}$ and $\mathbf{R} \times \{0,1\}$.

There are many such bijections, one is:

$$\begin{aligned} \psi\colon \mathbf{R} &\to \mathbf{R} \times \{0,1\}, \\ x &\mapsto \begin{cases} (\varphi(x), 0) & x > 0, \\ (\varphi(k^{-1}(-x), 1) & x \leqslant 0 \end{cases} \end{aligned} \qquad \begin{aligned} \psi^{-1}\colon \mathbf{R} \times \{0,1\} &\to \mathbf{R}, \\ (a,b) &\mapsto \begin{cases} \varphi^{-1}(a) & b = 0, \\ -k(\varphi^{-1}(a)) & b = 1 \end{cases} \end{aligned}$$

□

4. In this question we consider infinite sequences of positive integers, $f(1), f(2), f(3), \ldots$. (Formally, they are functions from positive integers to positive integers $f : \mathbf{Z}^+ \to \mathbf{Z}^+$, where $\mathbf{Z}^+ = \{1,2,3,\ldots\}$.) Some student wrote various expressions involving quantifiers and the function f.

(a) $\exists a \in \mathbf{Z}^+ \; \exists b \in \mathbf{Z}^+ \; \forall c \in \mathbf{Z}^+ \; (c \geq a \;\to\; f(c+b) = f(c))$.

Answer: The corresponding class is $\mathcal{D}$.
This is precisely the definition of the *eventually periodic sequences*. Namely, starting from some place $a > 0$, the sequence $f(a), f(a+1), \ldots$ is periodic; and its period is b. □

(b) $\exists a \in \mathbf{Z}^+ \; \exists b \in \mathbf{Z}^+ \; \forall c \in \mathbf{Z}^+ \; (f(c+b) = f(c) \;\to\; c \geq a)$.

Answer: The corresponding class is $(\mathbf{Z}^+)^{\mathbf{Z}^+}$.
You can take $a = 1$. Then the conclusion $c \geq a$ is always true (regardless of the behavior of the function f). The expression describes the class of *all sequences of positive integers*.

□

(c) $\forall a \in \mathbf{Z}^+ \; \exists b \in \mathbf{Z}^+ \; \forall c \in \mathbf{Z}^+ \; (c \geq a \;\to\; f(c+b) = f(c))$.

Answer: The corresponding class is $\mathcal{C}$.
The implication $(c \geq a \;\to\; f(c+b) = f(c))$ is most "demanding", if $a = 1$, because in this case $c \geq a$ is always true, and therefore $f(c+b) = f(c)$ should be satisfied. Furthermore, if there exists a "universal" value b such that for all c we have $f(c+b) = f(c)$, it means that this is the class $\mathcal{C}$ of all *periodic sequences*. □

(d) $\forall a \in \mathbf{Z}^+ \; \forall c \in \mathbf{Z}^+ \; \exists b \in \mathbf{Z}^+ \; (c \geq a \;\to\; f(c+b) = f(c))$.

Answer: The corresponding class is $\mathcal{F}$.
Similar to the previous item: Making the expression true for value $a = 1$ would make it true for any other a. Therefore we start by selecting $a = 1$ and requiring that $f(c+b) = f(c)$.
Unlike the previous item, we can pick a different value b for every c. Yet, $c > 1$, so for every $f(c)$ we can find some $f(c+b) = f(c)$ somewhere later in the sequence. In other words, for any $f(c)$ we can find a value $f(c+b)$ which equals $f(c)$. Replacing c by $c+b$ and repeating, there must be yet another $f((c+b)+b')$ which also has the same value and so on.

Therefore this is the class $\mathcal{F}$, the set of all sequences where, if a number appears, it reappears infinitely often. □

(e) $\exists a \in \mathbf{Z}^+\ \forall b \in \mathbf{Z}^+\ \forall c \in \mathbf{Z}^+\ (b \leq a \rightarrow f(c+b) = f(c))$.

Answer: The corresponding class is $\mathcal{A}$.
If we select $b = 1$, then $b \leq a$ is always true, and $f(c+b) = f(c)$ must also be true for all c. Therefore, $f(c+1) = f(c)$, so any two subsequent values in the sequence are the same. This can be true only for *constant sequences.* □

Please check what do these expressions actually say about the properties of the function f. Consider the following sets as possible answers.

- $(\mathbf{Z}^+)^{\mathbf{Z}^+}$ – the set of all infinite sequences of positive integers.
- $\varnothing$ – the *empty set* containing no sequences.
- $\mathcal{A}$ – the set of all *constant sequences.*
- $\mathcal{B}$ – the set of all *eventually constant sequences.*
- $\mathcal{C}$ – the set of all *periodic sequences.*
- $\mathcal{D}$ – the set of all *eventually periodic sequences.*
- $\mathcal{E}$ – the set of all *arithmetic progressions.*
- $\mathcal{F}$ – the set of sequences where, if a number appears, it reappears infinitely often.
- $\mathcal{I}$ – the set of all *injective sequences.*
- $\mathcal{S}$ – the set of all *surjective sequences.*

For every quantifier expression in the list (a)–(e) find the corresponding set ($\mathbf{N}^{\mathbf{N}}$, $\varnothing$, $\mathcal{A}$,...,$\mathcal{S}$). Give short explanations, why do you believe the quantifier expression describes the set of sequences. If it turns out that some expression does not match any of these sets, describe its meaning in plain English.

5. Complete the proofs in Coq notation (they mirror the statements from Homework 2).

See full solution in `https://bit.ly/3jHNbZD`, course homepage under *Discrete 2021: Assignments.*

□

```
Section traffic.

Inductive City : Type :=
  | A
  | B
  | C.

Variable Plane : City*City -> Prop.
Variable Rail: City*City -> Prop.

Hypothesis PlaneLinks: forall x y:City, x<>y <-> Plane(x,y).
Hypothesis RailLink1: Rail(A,B).
Hypothesis RailLink2: Rail(B,A).
Hypothesis RailLink3: Rail(B,C).
Hypothesis RailLink4: Rail(C,A).
Hypothesis RailLink5: ~Rail(A,A).
Hypothesis RailLink6: ~Rail(A,C).
Hypothesis RailLink7: ~Rail(B,B).
Hypothesis RailLink8: ~Rail(C,B).
Hypothesis RailLink9: ~Rail(C,C).


(* L1: From any city there is a direct plane-link to some other city. *)
Lemma L1: forall (x: City), exists (y: City), (x<>y /\ Plane(x,y)).
Proof.
  Admitted.

(* It is not true that from any city one can go to any other city
   in two steps like this:
   First take a plane-link and then take a rail-link. *)
Lemma L2: ~(forall (x:City) (y:City),
    exists (z:City), (Plane(x,z) /\ Rail(z,y))).
Proof.
  Admitted.

(* It is generally not true that, if it is possible to go from
   a city 'x' to some other city 'y' with two plane-links,
   then it is also possible to go from 'x' to 'y'
   using a single plane-link. *)
Lemma L3: ~(forall x y z:City, (Plane(x,z) /\ Plane(z,y) -> Plane(x,y))).
Proof.
  Admitted.

End traffic.
```