

S.E. Theory: SOFTENG211 Assignment #3

Nisarag Bhatt

Problem 1

Question:

Let A be a set with exactly n elements.

Consider the following two sets: $X = \{f \mid f : A \rightarrow \{0, 1\}\}$ and $Y = \{u \mid u \text{ is a binary string of length } n\}$.

Show that there is a bijection from X onto Y .

Answer:

Since X, Y are both finite sets then the existence of a bijection means they have the same number of elements.

We seek to prove $|X| = |Y|$ for there to exist a bijection from X onto Y .

Proof. First we consider the cardinality of $|X|$. By definition A has n elements and for every element in A you can choose 2 options either 0, 1 so we conclude there are $\underbrace{2 \cdot 2 \cdot \dots \cdot 2}_{n \text{ times}} = 2^n$ functions in the set X that map $A \rightarrow \{0, 1\}$ hence $|X| = 2^n$.

Now we consider the cardinality of $|Y|$. Y is simply all the possible binary strings of length n .

One may notice that for $n = 0$ we have that there is $2^0 = 1$ binary string (the empty string), for $n = 1$ we have that there is $2^1 = 2$ binary strings (0, 1) and so forth.

Consider the statement $P(n) = \text{"There are } 2^n \text{ binary strings of length } n\text{"}$. We continue to prove $P(n)$ by induction.

Base Case: $n = 0$: If $n = 0$ then $P(0) = \text{empty string}$. ✓

Inductive Hypothesis: Suppose for an arbitrary n , assume $P(n)$ is true.

Inductive Step: Want to show $P(n) \implies P(n+1)$: Consider the set of all binary strings of length $n+1$ (Call this set ϕ). Note that all binary strings either end in 1 or 0.

Split ϕ up into two sets α, β :

- α consists of all binary strings of length $n+1$ that end with 0
- β consists of all binary strings of length $n+1$ that end with 1

One may also notice that α consists of arbitrary binary strings with length n that end with 0 so by Inductive Hypothesis there are 2^n of these strings.

Similarly β consists of arbitrary binary strings with length n that end with 1 so by Inductive Hypothesis there are 2^n of these strings.

We can now see that $|\phi| = |\alpha| + |\beta| = 2^n + 2^n = 2^n(1+1) = 2^{n+1}$. So there are exactly 2^{n+1} binary strings of length $n+1$ so $P(n+1)$ holds.

So $P(n) \implies P(n+1)$, Hence $P(n)$ is true for all $n \in \mathbb{N}$.

From the proof by induction we now know that $|Y| = 2^n$.

Since $|X| = |Y|$, this must mean there is a bijection from X onto Y . (See proof of this in Question 2 Part 1 (if $n = m$ then there is a bijection from A onto B)) \square

Problem 2

Question:

Let A and B be two finite sets with exactly n and m elements, respectively.

Show the following:

Answer:

1. There is a bijection from A onto B if and only if $n = m$

• \Rightarrow

Proof. If there is a bijection from A onto B then there exists a bijective function $f : A \rightarrow B$

For the sake of contradiction assume that $n \neq m$.

Case 1: $n > m$ - Let $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$. If $n > m$ then there exists elements $a_i, a_j \in A$ such that a_i, a_j are mapped to an element $b_i \in B$. This means f is not injective (since $f(x) = f(y)$ does not imply $x = y$) and hence not bijective. Contradiction.

Case 2: $n < m$ - Let $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$. If $n < m$, then there exists an element in $b_i \in B$ such that $f(a_i) \neq b_i$. However this contradicts the fact that f is surjective which further contradicts the fact that f is bijective.

Since in both cases we get a contradiction, we have that if there is a bijection from A onto B then $n = m$. □

• \Leftarrow

Proof. If $n = m$ then consider the sets $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_n\}$.

Suppose there exists a function $f : A \rightarrow B$ such that f maps $a_1 \rightarrow b_1, a_2 \rightarrow b_2$ and so forth until $a_n \rightarrow b_n$.

This function is injective if $f(x) = f(y) \Rightarrow x = y$. For this function, if $f(a_i) = f(a_j)$, then it is necessary that $i = j$, since if $i \neq j$, $b_i \neq b_j$ by definition (of the way we defined the function). Therefore f is injective.

This function is surjective if for every y in the codomain, there exists an x such that $f(x) = y$. In this case given a b_i , we have that there exists an a_i such that $f(a_i) = b_i$ for every i (where $0 < i \leq n$). Therefore f is surjective.

Since f is injective and surjective then by definition f must be bijective. Therefore if $n = m$, there exists a bijection from A onto B . □

2. Show that there is an injection from A into B if and only if $n \leq m$.

• \Rightarrow

Proof. Suppose there exists an injective function $f : A \rightarrow B$ where $\forall a_i, a_j \in A, f(a_i) = f(a_j) \Rightarrow a_i = a_j$.

For the sake of contradiction assume $n > m$.

Let $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$. If $n > m$ then there exists elements $a_i, a_j \in A$ such that a_i, a_j are mapped to an element $b_i \in B$. This means f is not injective (since $f(x) = f(y)$ does not imply $x = y$). Contradiction.

This must mean that if there is an injection from A into B then $n \leq m$. \square

• \Leftarrow

Proof. We will prove that if $n \leq m$ then there is an injection from A into B .

When $n = m$ trivially we have a bijection (see the proof for \Leftarrow for Part 1 of this question) and hence an injection from A into B .

So consider the case when $n < m$.

Let $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_n, \dots, b_m\}$

Pick a subset of B which contains n elements ($B' = \{b_1, \dots, b_n\}$).

Since A and B' both have n elements, consider an explicit bijection $f : A \rightarrow B'$.

f essentially maps $a_1 \rightarrow b_1$, $a_2 \rightarrow b_2$, until $a_n \rightarrow b_n$.

(see the proof for \Leftarrow for Part 1 of this question to see that f is a bijection). Since f is a bijection it must also be injection.

Now consider a function $g : B' \rightarrow B$ that sends every element to itself, note that B' has n elements and B has m elements.

g is injective because B has m elements and B' has n elements, since $n < m$ an injection exists since all elements in B' are mapped to themselves in B .

So for all $f(b_i) = f(b_j)$ we will have $b_i = b_j$ since each element maps to itself. Any left over are left unmapped so injectivity still exists since no element in B' maps to more than one element in B .

Since $f : A \rightarrow B'$ and $g : B' \rightarrow B$. We consider the composition $g \circ f : A \rightarrow B$. We are required to prove $g \circ f$ is an injection to complete this proof.

Proof. Since $f(a) = f(b) \implies a = b$ and $g(a) = g(b) \implies a = b$

So $g(f(a)) = g(f(b)) \implies f(a) = f(b) \implies a = b$ \square

Since $g \circ f : A \rightarrow B$ is an injection, there must exist an injection from A into B if $n \leq m$. \square

Problem 3

Question:

Let A be a set with exactly n elements.

Prove by induction that the number of bijective functions from A into A equals $n!$.

Clearly state your base case, inductive hypothesis, and present a clear inductive step.

Answer:

$\forall n \in \mathbb{N} P(n) =$ "The number of bijective functions from A into A equals $n!$ where A is a set with n elements"

Proof. Base Case: $n = 1$: If $n = 1$ then A has one element, trivially there only exists one function which maps that element to itself. ✓

Inductive Hypothesis: Suppose for an arbitrary n , assume $P(n)$ is true. This means there for a set with n elements we have that there exists $n!$ bijective functions to itself.

Inductive Step: Consider a set with $n + 1$ elements: $D = \{d_1, d_2, \dots, d_n, d_{n+1}\}$

Consider all the injective functions on this set. Split these functions into $n + 1$ sets K_i where the functions in K_i are the injective functions that send d_1 to d_i .

Note that the functions in K_1 send d_1 to d_1 , so are determined by what the function does on the set of n elements $\{d_2, \dots, d_{n+1}\}$. By our inductive hypothesis we have that there exist $n!$ functions that do this. By this logic, each set K_i has $n!$ elements. Since there $n + 1$ sets of these $n!$ elements.

We then have that $\underbrace{n! + n! + \dots + n!}_{n+1 \text{ times}} = (n+1)n! = (n+1)!$. This means there exists $(n+1)!$ different functions that map D into D .

Since we have proved $P(1)$ and $\forall n \in \mathbb{N} : P(n) \implies P(n+1)$.

We can thus conclude $\forall n \in \mathbb{N} : P(n)$ holds.

□

Problem 4

Question:

Prove, using the induction principle, that $3^{2n} - 1$ is always divisible by 8 for all integers $n \geq 0$.

Clearly state your base case, inductive hypothesis, and present a clear inductive step.

Answer:

Proof. Consider " $P(n) = 8|3^{2n} - 1$ ", we seek to claim $P(n)$ holds for all integers $n \geq 0$

Base Case: $n = 0$: If $n = 0$ then $P(0) = 8|3^{2 \cdot 0} - 1 = 8|0$. Trivially $8|0$ hence $P(0)$ holds.

Inductive Hypothesis: Suppose for an arbitrary n , assume $P(n) = 8|3^{2n} - 1$ is true.

Inductive Step: By the Inductive Hypothesis we have that $8|3^{2n} - 1$ which means $3^{2n} - 1 = 8 \cdot m$ for some $m \in \mathbb{Z}$. So $3^{2n} = 8 \cdot m + 1$

We now consider the expression

$$\begin{aligned}
 & 3^{2(n+1)} - 1 \\
 &= 3^{2n+2} - 1 \\
 &= 3^{2n} 3^2 - 1 \\
 &= 3^{2n}(9) - 1 \\
 &= (8 \cdot m + 1) \cdot 9 - 1 \quad \text{By IH} \\
 &= 72m + 9 - 1 \\
 &= 72m + 8 \\
 &= 8(9m + 1)
 \end{aligned}$$

Note that $9m + 1$ is simply an integer hence $8|3^{2(n+1)} - 1$ so $P(n+1)$ is true.

Since we have proved $P(0)$ and \forall integers $n \geq 0 : P(n) \implies P(n+1)$

We can thus conclude \forall integers $n \geq 0 : P(n)$ holds. □

Problem 5

Question:

On the set \mathbb{Z} of integers consider the following relation E .

Pair (x, y) is in E if and only if either $(|x| \leq 10 \text{ and } |y| \leq 10 \text{ and } x \cdot y > 0)$ or $(x = y = 0)$ or $(|x| > 10 \text{ and } |y| > 10)$.

Do the following:

1. Prove that E is an equivalence relation.
2. Describe all equivalence classes of E .

Answer:

For E to be an equivalence relation it must satisfy 3 key properties:

• Reflexive

Required to prove: For all $x \in \mathbb{Z}$, xEx

Proof. Consider $x \in \mathbb{Z}$

- If $x = 0$ then $x = x = 0$ and hence $(x, x) \in E$.
- If $|x| \leq 10$ and $x \neq 0$ then note that $x \cdot x \neq 0$ which means $(x, x) \in E$.
- If $|x| > 10$ then it must be the case $(x, x) \in E$.

□

• Symmetric

Required to prove: For all $x, y \in \mathbb{Z}$, if xEy then yEx .

Proof. Suppose that xEy then it means $(x, y) \in E$; consider these cases:

- If $x, y = 0$
 - * If $x = y = 0$ then it follows that $y = x = 0$ therefore yEx
- $x, y \neq 0$
 - * If $|x|$ and $|y| > 10$ then it obviously follows $|y|, |x| > 10$ and hence yEx .
 - * If $|x| \leq 10$ and $|y| \leq 10$
 - If $0 < x, y \leq 10$ (both positive) then $(x, y) \in E$. Since $x \cdot y > 0$ is satisfied. This also means that $y \cdot x > 0$ so then yEx .
 - If $-10 \leq x, y < 0$ (both negative) then $(x, y) \in E$. Since $x \cdot y > 0$ is satisfied. This also means that $y \cdot x > 0$ so then yEx .

then $(x, y) \in E$ iff x, y are both positive or both negative.

□

- **Transitive**

Required to prove: For all $x, y, z \in \mathbb{Z}$, if xEy and yEz then xEz .

Proof. Suppose that xEy and yEz then it means $(x, y) \in E$ and $(y, z) \in E$.

- If $x = 0$ we have that $y = 0$, and since $y = 0$ we have that $z = 0$. This means that $x = z = 0$ and therefore xEz .
- If $|x| > 10$ and $|y| > 10$, and since $(y, z) \in E$ one may observe this only happens when $|z| > 10$. Hence $|x| > 10$ and $|z| > 10$ therefore $(x, z) \in E$.
- If $0 < x \leq 10$ and since $(x, y) \in E$ we have that $0 < y \leq 10$. Similarly since $(y, z) \in E$ one may notice that $0 < z \leq 10$. Since x, z are both positive, we have that $x \cdot z > 0$ and therefore xEz .
- If $-10 \leq x < 0$ and since $(x, y) \in E$ we have that $-10 \leq y < 0$. Similarly since $(y, z) \in E$ one may notice that $-10 \leq z < 0$. Since x, z are both negative, we have that $x \cdot z > 0$ and therefore xEz .

□

Since all 3 properties are satisfied we have that E is an equivalence relation.

Equivalence Classes of E

Notice that there are 4 equivalence classes for E .

1. $\{x \mid x = 0\}$
2. $\{x \mid 0 < x \leq 10\}$
3. $\{x \mid -10 \leq x < 0\}$
4. $\{x \mid |x| > 10\}$

Problem 6

Question:

A connected graph G is planar if you can draw the graph on the plane without any edges crossing. When you draw a graph in a such way, the plane is divided into regions. These regions are called faces of the graph. One of the faces is the exterior face. Let n, m , and f be the number of vertices, edges, and faces (including the exterior face) of G .

Prove by induction that $n - m + f = 2$

Clearly state your base case, inductive hypothesis, and present a clear inductive step.

Answer:

Without loss of generality, assume G is not a tree. This is because for a tree we have that $m = n - 1$ and $f = 1$ and hence $n - m + f = n - (n - 1) + 1 = 2$ so this formula always works for a tree.

$P(m) = \text{"For a connected planar graph } G \text{ with } n \text{ vertices, } m \text{ edges and } f \text{ faces then } n - m + f = 2\text{"}$

Proof. Base Case(s): Consider the case when G has no edges (i.e. $m = 0$), only one graph exists with this case and that is when there is only vertex so $n = 1$ and hence $f = 1$.

Therefore $n - m + f = 1 - 0 + 1 = 2$. ✓.

Inductive Hypothesis: Suppose for an arbitrary m , assume $P(m)$ is true. So this formula holds for any connected planar graph with m edges, n vertices and f faces.

Inductive Step: Consider a connected planar graph G with $m + 1$ edges, n vertices and f faces.

Since G is not a tree then it must have atleast one cycle.

Consider a cycle C in this graph G , remove an edge in this cycle to form G' .

The amount of faces is reduced by 1 because the cycle C separated the plane into two regions. The regions to either side of the edge we remove are distinct. When we remove the edge, these regions collapse together to become 1 therefore the amount of faces is reduced by 1.

G' has $m' = m - 1$ edges, $n' = n$ vertices and $f' = f - 1$ faces.

By the induction hypothesis we have that $n' - m' + f' = 2$, substituting the above expressions in we get that $n - m + 1 + f - 1 = n - m + f = 2$ which is what is required.

Therefore we conclude $P(m)$ holds for all $m \geq 0$. □

Problem 7

Question:

Prove that any integer $n \geq 12$ can be written as a sum of integers 4 and 5.

Clearly state your base case, inductive hypothesis, and present a clear inductive step.

Answer:

$$P(n) = \text{"Any integer } n \geq 12 \text{ can be written as a sum of integers 4 and 5"}$$

Proof. Base Case(s):

$$P(12) = 4(3) + 5(0) \checkmark$$

$$P(13) = 4(2) + 5(1) \checkmark$$

$$P(14) = 4(1) + 5(2) \checkmark$$

$$P(15) = 4(0) + 5(3) \checkmark$$

$$P(16) = 4(4) + 5(0) \checkmark$$

Inductive Hypothesis: Suppose for an arbitrary n , assume $P(n)$ is true. Which means $n = 4l + 5m$ where $l, m \in \mathbb{N} \cup \{0\}$

Inductive Step:

From the base cases, we only need to consider two cases:

1. $l \geq 1$ (n is not divisible by 5)
2. $l = 0$ (n is divisible by 5)

For the first case ($l \geq 1$), consider the inductive hypothesis $n = 4l + 5m$ then

$$\begin{aligned} n + 1 &= 4l + 5m + 1 \\ &= 4(l + 1 - 1) + 5m + 1 \\ &= 4l + 4 - 4 + 5m + 1 \\ &= 4l - 4 + 5m + 5 \\ &= 4(l - 1) + 5(m + 1) \end{aligned}$$

For the second case ($l = 0$), consider the inductive hypothesis again $n = 4l + 5m = 5m$ then for $m \geq 3$ we have that:

$$\begin{aligned} n + 1 &= 5m + 1 \\ &= 5(m - 3 + 3) + 1 \\ &= 5m - 15 + 15 + 1 \\ &= 5m - 15 + 16 \\ &= 5(m - 3) + 4(4) \end{aligned}$$

In both cases $P(n + 1)$ can be written as a sum of integers 4 and 5 so $P(n)$ holds for any integer ≥ 12 . \square

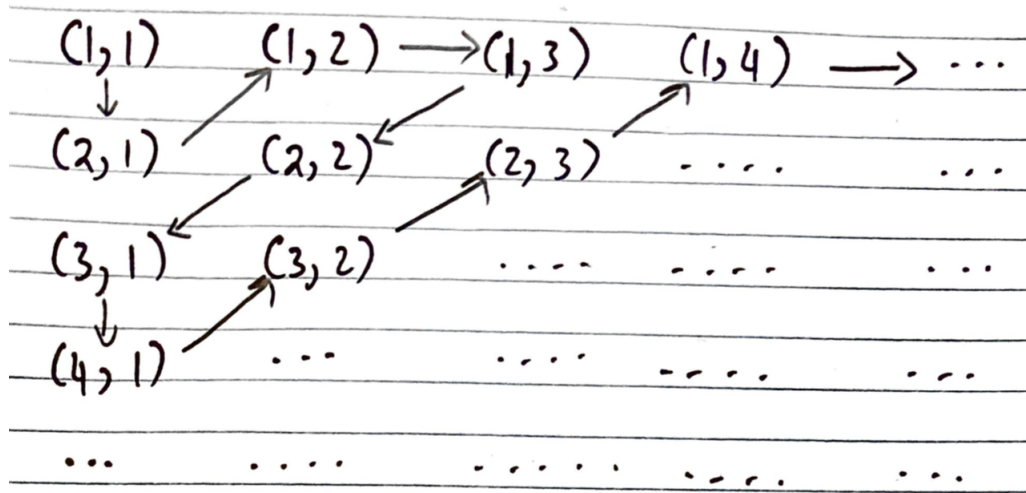
Problem 8

Question:

Explain why there is a bijection between \mathbb{N} and \mathbb{N}^2 .

Answer:

I will explain why there is a bijection between \mathbb{N} and \mathbb{N}^2 by drawing a picture:



This picture I have drawn is essentially \mathbb{N}^2 layed out in a grid format. We then traverse this grid in a zig-zag path.

We can then label each pair with how far down the path it is, so:

- 1 $\rightarrow (1, 1)$
- 2 $\rightarrow (2, 1)$
- 3 $\rightarrow (1, 2)$
- 4 $\rightarrow (1, 3)$
- 5 $\rightarrow (2, 1)$
- 6 $\rightarrow (3, 1)$
- 7 $\rightarrow (4, 1)$
- 8 $\rightarrow (3, 2)$
- 9 $\rightarrow (2, 3)$
- 10 $\rightarrow (1, 4)$

and so forth...

So since we can continue to draw more pairs of \mathbb{N}^2 in a grid format and zig zag through and map each natural number to a (x, y) pair in this zig zag path, we essentially create a bijection.

Another way of thinking about this picture is that we can imagine \mathbb{N} to be a number line. If we traverse this path shown above in my picture we create another line. Both of these are lines are continuous and never end.

Since both of them are a line there must exist a bijection between them.