Solutions for Week Four

Problem One: Concept Checks

i.   Give two examples of binary relations over the set $\mathbb{N}$.

> One option is the the = relation. Another is ≤. There are tons of other ones with nice names ($\equiv_2$, $\equiv_3$, the relation "divides," etc.), and lots more that you could only specify with a picture.

ii.   What three properties must a binary relation have to have in order to be an equivalence relation? Give the first-order definitions of each of those properties. For each definition of a property, explain how you would write a proof that a binary relation R has that property.

> An equivalence relation is a relation that's reflexive, symmetric, and transitive. A binary relation R over a set A is reflexive if
>
> $$\forall a \in A.\ aRa.$$
>
> To prove that R is reflexive, we can choose an arbitrary $a \in A$ and prove that aRa holds.
>
> The relation R is symmetric if
>
> $$\forall a \in A.\ \forall b \in A.\ (aRb \rightarrow bRa).$$
>
> To prove that R is symmetric, we can choose an arbitrary a and b in A where aRb, then prove that bRa also holds.
>
> The relation R is transitive if
>
> $$\forall a \in A.\ \forall b \in A.\ \forall c \in A.\ (aRb \wedge bRc \rightarrow aRc).$$
>
> To prove that R is transitive, we can choose an arbitrary a, b, and c in A where aRb and bRc, then prove that aRc also holds.

iii.   If R is an equivalence relation over a set A and a is an element of A, what does the notation $[a]_R$ mean? Intuitively, what does it represent?

> This is the equivalence class of a with respect to R. Formally, it's the set $\{\ b \in A \mid aRb\ \}$. Intuitively, it's the set of all elements that a relates to.

iv.   What does the notation $f : A \rightarrow B$ mean?

> This says that f is a function whose domain is A and whose codomain is B. In other words, f takes in as inputs objects from the set A and returns as output objects from the set B.

v.　　Let $f : A \to B$ be a function. Express, in first-order logic, what property f has to satisfy to be an injection. Then, based on the structure of that formula, explain how you would write a proof that f is injective.

There are two equivalent definitions for injectivity. First, there's this one:

$$\forall a_1 \in A. \ \forall a_2 \in A. \ (f(a_1) = f(a_2) \to a_1 = a_2).$$

Next, there's this one:

$$\forall a_1 \in A. \ \forall a_2 \in A. \ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)).$$

To prove injectivity using the first of these statements, we'd consider arbitrary $a_1, a_2 \in A$ where $f(a_1) = f(a_2)$, then prove that $a_1 = a_2$. For the second, we'd consider arbitrary $a_1, a_2 \in A$ where $a_1 \neq a_2$, then prove $f(a_1) \neq f(a_2)$.

vi.　　Negate your statement from part (vii) and simplify it as much as possible. Then, based on the structure of your formula, explain how you would write a proof that f is not injective.

The negation of both statements boil down to

$$\exists a_1 \in A. \ \exists a_2 \in A. \ (a_1 \neq a_2 \land f(a_1) = f(a_2)).$$

To prove that a function f is not injective, we'd find specific choices of a_1 and a_2 in A where $a_1 \neq a_2$ but $f(a_1) = f(a_2)$, then briefly justify why these choices work.

vii.　　Let $f : A \to B$ be a function. Express, in first-order logic, what property f has to satisfy to be a surjection. Then, based on the structure of that formula, explain how you would write a proof that f is surjective.

The formal definition of surjectivity is

$$\forall b \in B. \ \exists a \in A. \ f(a) = b.$$

To prove that a function is surjective, we'd consider an arbitrary $b \in B$, then find $a \in A$ where $f(a) = b$.

viii.　　Negate your statement from part (ix) and simplify it as much as possible. Then, based on the structure of your formula, explain how you would write a proof that f is not surjective.

The negation of the above statement is

$$\exists b \in B. \ \forall a \in A. \ f(a) \neq b.$$

To prove this, we'd show that there is a specific choice of b (which we pick) where $f(a) \neq b$ for any $a \in A$.

ix.　　Let $f : A \to B$ be a function. What properties must f have to be a bijection? How would you write a proof that f is bijective?

f would need to be injective and surjective. To prove f is a bijection, we'd prove that f is injective and surjective.

x.　　What would you need to prove to show that f is not a bijection?

To prove that f is not a bijection, we need to show either that f is not injective or that f is not surjective.

xi.   Let $f : A \to B$ and $g: B \to C$ be functions. What does the notation $f \circ g$ mean? How would you evaluate $(f \circ g)(x)$?

f ∘ g denotes the composition of functions, and *(f ∘ g)(x) = f(g(x))*. Note: I accidentally switched the order of f and g here, so the domains and co-domains don't match—it should say *f : B → C* and *g: A → B*. Thanks to everyone who caught this in class!

Problem Two: Equivalence Relations

i.   In lecture, we proved that the binary relation ~ over $\mathbb{Z}$ defined as follows is an equivalence relation:

$$a{\sim}b \qquad \text{if } a{+}b \text{ is even.}$$

Consider this new relation # defined over $\mathbb{Z}$:

$$a\#b \qquad \text{if } a{+}b \text{ is odd.}$$

Is # an equivalence relation? If so, prove it. If not, disprove it.

No, this is not an equivalence relation. It's neither reflexive nor transitive.

Using the first-order definitions above, we can see that to prove that # is not reflexive, we need to prove that

$$\exists a \in \mathbb{Z}. \ \neg(a\#a).$$

Here's a proof of that:

Claim: The # relation over $\mathbb{Z}$ is an equivalence relation.

Disproof 1: We will prove that # is not reflexive. To see this, consider the number 1. Since $1{+}1 = 2$, which is even, we see that 1#1 does not hold. Therefore, the relation # is not reflexive, so it's not an equivalence relation. ∎

We could also prove that # is not transitive. To prove that, we'd need to prove that

$$\exists a \in \mathbb{Z}. \ \exists b \in \mathbb{Z}. \ \exists c \in \mathbb{Z}. \ (a\#b \land b\#c \land \neg(a\#c)).$$

In other words, we need to find a choice of integers a, b, and c where $a{+}b$ is odd, $b{+}c$ is odd, but $a{+}c$ is not odd. Here's a way to do that:

Claim: The # relation over $\mathbb{Z}$ is an equivalence relation.

Disproof 2: We will prove that # is not transitive. To do so, consider the numbers 0, 1, and 2. Then $0{+}1 = 1$, which is odd, and $1{+}2 = 3$, which is odd. However, $0{+}2 = 2$, which is not odd. Therefore, we have that 0#1 and 1#2, but we see that 0#2 does not hold. Therefore, # is not transitive, so it is not an equivalence relation. ∎

ii.   How many equivalence classes are there for the ~ relation defined above? What are they?

There are two equivalence classes. First, look at the equivalence class $[0]_\sim$. This is the set

$$\{ x \in \mathbb{Z} \mid 0{\sim}x \},$$

which after expanding out the definition of ~ can be seen to be the set

$$\{ x \in \mathbb{Z} \mid 0 + x \text{ is even } \}.$$

Equivalently, this is the set

$$\{ x \in \mathbb{Z} \mid x \text{ is even } \},$$

which is the set of all even integers.

Now, look at the equivalence class $[1]_\sim$. This is the set

$$\{ x \in \mathbb{Z} \mid 1{\sim}x \} = \{ x \in \mathbb{Z} \mid 1 + x \text{ is even } \}.$$

With some thought we see that

$$\{ x \in \mathbb{Z} \mid 1 + x \text{ is even } \} = \{ x \in \mathbb{Z} \mid x \text{ is odd } \},$$

which is the set of all odd integers.

These two equivalence classes ($[0]_\sim$ and $[1]_\sim$) collectively contain all integers, so they are the only two equivalence classes for ~.

Why we asked this question: Part (i) of this problem was designed to give you practice exploring whether a given relation was an equivalence relation. This requires you to play around with the relation, get a feel for how it works, where it applies, where it doesn't, and ultimately to use that information to decide whether it meets all three of the requisite criteria for an equivalence relation. From there, you'd then need to prove that your answer was correct. We hoped that this end-to-end process – getting a relation, exploring its properties, then formalizing your reasoning – would serve as a good model for PS3 and beyond.

Part (ii) was designed to get you to think about what equivalence relations are by presenting a concrete relation and, along the lines of part (i), asking you to play around with it to see what properties you can discover.

Problem Three: Inverse Relations

Let R be a binary relation over a set A. We can define a new relation over A called the ***inverse relation of R***, denoted R^{-1}, as follows:

$$xR^{-1}y \qquad \text{if} \qquad yRx$$

This question explores properties of inverse relations.

i. What is the inverse of the $<$ relation over $\mathbb{Z}$? Briefly justify your answer.

> The inverse of the $<$ relation over $\mathbb{Z}$ is the $>$ relation over $\mathbb{Z}$. This is because $x < y$ happens precisely when $y > x$.

ii. What is the inverse of the $=$ relation over $\mathbb{Z}$? Briefly justify your answer.

> The $=$ relation over $\mathbb{Z}$ is its own inverse. Note that $x = y$ happens precisely when $y = x$ happens.

iii. Prove or disprove: if R is an equivalence relation over A, then R^{-1} is an equivalence relation over A.

> ***Proof:*** Let R be an equivalence relation over a set A. We will prove that R^{-1} is also an equivalence relation over A by proving that R^{-1} is reflexive, symmetric, and transitive.
>
> To prove that R^{-1} is reflexive, consider any $a \in A$. We need to prove that $aR^{-1}a$. By definition, this means that we need to prove that aRa. Since R is reflexive, we know that aRa holds, as required.
>
> To prove that R^{-1} is symmetric, consider any $a, b \in A$ where $aR^{-1}b$. We need to prove that $bR^{-1}a$. Since $aR^{-1}b$ holds, we know that bRa holds. Since R is symmetric and bRa is true, we know that aRb is true. Therefore, by definition of R^{-1}, we know that $bR^{-1}a$ holds, as required.
>
> Finally, to prove that R^{-1} is transitive, consider any $a, b, c \in A$ where $aR^{-1}b$ and $bR^{-1}c$. We need to prove $aR^{-1}c$. Since $aR^{-1}b$ and $bR^{-1}c$, we know that bRa and that cRb. Since cRb and bRa, by transitivity of R we see that cRa. Thus by definition of R^{-1}, we know that $aR^{-1}c$ holds, as required. ∎

Why we asked this question: This question was designed for two main reasons. First, in parts (i) and (ii) of this problem, we wanted you to play around with a new first-order definition to get a feel for what it means and what it looks like in some concrete examples. For part (iii), we hoped that you'd use your results from part (ii) to recognize that these were probably going to be "prove" statements. We also hoped that these would be good practice problems for cases where you begin with arbitrary objects with a certain small set of prescribed properties and had to show that some new object defined from those original objects have another set of properties.

Problem Four: Monotone Functions

A function $f : \mathbb{R} \to \mathbb{R}$ is called ***monotone increasing*** if the following is true:

$$\forall x \in \mathbb{R}.\ \forall y \in \mathbb{R}.\ (x < y \to f(x) < f(y))$$

This problem explores properties of monotone increasing functions.

i.   Prove or disprove: every monotone increasing function is injective.

Proof: Let $f : \mathbb{R} \to \mathbb{R}$ be a monotone increasing function and consider any two real numbers x and y where $x \neq y$. We will prove that $f(x) \neq f(y)$. To see this, note that since $x \neq y$, either $x < y$ or $y < x$. Assume without loss of generality that $x < y$. Then since f is monotone, we see that $f(x) < f(y)$, and therefore that $f(x) \neq f(y)$. Therefore, f is injective, as required. ∎

ii.   Prove or disprove: every injective function from $\mathbb{R}$ to $\mathbb{R}$ is monotone increasing.

Disproof: Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = -x$. We claim that this function is injective but not monotone increasing.

To see that f is injective, consider any arbitrary $x, y \in \mathbb{R}$ where $f(x) = f(y)$. We will prove that $x = y$. To see this, notice that since $f(x) = f(y)$, we see that $-x = -y$, and therefore that $x = y$, as required.

However, this function is not monotone increasing. Notice that $103 < 137$, for example, but that $f(103) = -103$ is not less than $f(137) = -137$. ∎

Why we asked this question: Both parts of this question were framed as "prove or disprove," where you need to both assess whether each claim is true before you can start to write up the answer. This type of problem is extremely common in general mathematics, where you're working on a problem and have no idea whether some particular claim is correct or incorrect. We hoped that this would push you to search for some examples of injective functions and monotone increasing functions to see if you could spot a pattern.

Part (i) of this question was designed to see if you were comfortable writing a proof that a function is injective given very little information about that function. We also thought it was a nice place to give you practice with proofs involving "without loss of generality." Part (ii) of this problem was designed as an example of a disproof that actually has several parts to it, namely finding a function that's injective but not monotone increasing, then proving it has both properties.

Problem Five: Involutions

A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$.

i.   Find three different examples of involutions from $\mathbb{Z}$ to $\mathbb{Z}$. Briefly justify your answers.

Here are three involutions from $\mathbb{Z}$ to $\mathbb{Z}$:

1. $f(x) = x$. Then $f(f(x)) = f(x) = x$.

2. $f(x) = -x$. Then $f(f(x)) = f(-x) = -(-x) = x$

3. $f(x) = \begin{cases} x + 1 & \text{if } x \text{ is even} \\ x - 1 & \text{if } x \text{ is odd} \end{cases}$

To see why option (3) works, consider the following. If you take an even integer x, notice that $f(f(x)) = f(x+1)$. Since x is even, we know $x+1$ is odd, so $f(x+1) = (x+1) - 1 = x$. If you take an odd integer x, notice that $f(f(x)) = f(x-1)$. Since x is odd, then $x - 1$ is even, so we see that $f(x - 1) = (x - 1) + 1 = x$.

ii.   Prove that if f is an involution, then f is a bijection.

Proof: Let $f : A \to A$ be an involution. We will prove that f is a bijection by proving that it's both injective and surjective.

To prove that f is injective, consider any arbitrary $a_1, a_2 \in A$ where $f(a_1) = f(a_2)$. We will prove that $a_1 = a_2$. To see this, start with $f(a_1) = f(a_2)$ and apply f to both sides of this equality. This tells us that $f(f(a_1)) = f(f(a_2))$. Since f is an involution, we know that $f(f(a_1)) = a_1$ and also that $f(f(a_2)) = a_2$, so we conclude that $a_1 = a_2$, as required.

To prove that f is surjective, consider any $b \in A$. We need to show that there is some $a \in A$ such that $f(a) = b$. To do so, let $a = f(b)$. Then, since f is an involution, we see that $f(a) = f(f(b)) = b$, as required. ∎

Why we asked this question: This question was designed to get you playing around with inverse functions and bijections. Part (i) of this question was designed as a fun "scavenger hunt" type problem where we hoped you'd think of the first two functions rather quickly, then have to spend some time trying to figure out the last one. To the best of our knowledge, the only other function classes that work here are piecewise defined, so we hoped that you'd start playing around with piecewise functions. In part (ii) of this problem, we wanted you to prove that a function is injective and surjective given little knowledge about the function. This sort of reasoning is common in discrete math – we begin with an object of some particular type and prove it must have some auxiliary properties by leveraging the definition of that type of object. Hypothetically speaking, this style of reasoning might be relevant on Problem Set Three. ☺

Problem Six: Functions and Relations – Together!

Let $f : A \rightarrow B$ be an arbitrary function. Define a new binary relation ~ over A as follows:

$$x \sim y \quad \text{if} \quad f(x) = f(y)$$

Prove that ~ is an equivalence relation over A.

Proof: Let $f : A \rightarrow B$ be an arbitrary function and consider the relation ~ over A defined as

$$x \sim y \text{ if } f(x) = f(y).$$

We will prove that ~ is reflexive, symmetric, and transitive.

To show that ~ is reflexive, consider any $x \in A$. We need to prove that $x \sim x$. To do so, notice that since $=$ is reflexive, we know that $f(x) = f(x)$. Therefore, we see that $x \sim x$, as required.

To show that ~ is symmetric, consider any $x, y \in A$ where $x \sim y$. We need to prove that $y \sim x$ holds. To see this, note that since $x \sim y$, we know that $f(x) = f(y)$. Since $=$ is symmetric, we see that $f(y) = f(x)$, so $y \sim x$, as required.

To show that ~ is transitive, consider any $x, y, z \in A$ where $x \sim y$ and $y \sim z$. We need to prove that $x \sim z$ holds. To see this, note that since $x \sim y$ and $y \sim z$, we know that $f(x) = f(y)$ and $f(y) = f(z)$. Since $=$ is transitive, this tells us that $f(x) = f(z)$, so $x \sim z$, as required. ∎

Why we asked this question: Honestly, we just couldn't resist. We figured it would be fun to conclude with a problem that connects together the two major topics we've covered over the course of the past week. ☺