Problem Set 6 Solutions

Problem 1. *There is a ferry boat which leaves from Boston Harbor. In order to board the boat, a person must go through several steps:*

- *Go to the ticket counter*
- *Purchase a ticket at the ticket counter*
- *Go to the boat*
- *Give the ticket to the conductor and get on*

(Tickets purchased for a particular trip are not good for any other trips). Give a state machine that models this scenario, in which each of the above steps corresponds to one (separate) transition.

Suppose that initially there are only 60 tickets at the ticket counter. Add this fact to your state machine, and prove that there are never more than 60 passengers on the boat.

We want to keep track of the number of tickets in the system and who has them as well as information about the people in the system, specifically, where they are and whether they've got a ticket. Note that no one is allowed to buy a second ticket it they haven't used the first (for simplicity).

Variables:
t: the number of tickets at the counter
b: the number of people on the boat (which is the same as the number of tickets the conductor has collected)
p: the number of tickets in people's hands Location(i): the location of the ith person. Ticket(i): true if the ith person has a ticket, false otherwise.

Initial conditions:
$t = 60$, $b = 0$, and $p = 0$

Transitions:
GoToCounter(i)
Precondition: (none)
Effect:
Location(i) = counter

PurchaseTicket(i)
Precondition:
$t > 0$, Ticket(i)=false, Location(i)=counter
Effect:
$t = t - 1$
$p = p + 1$
Ticket(i)=true

GoToBoat(i)
Precondition: (none)
Effect:
Location(i) = at boat

GetOnBoat(i)
Precondition:

Location(i) = at boat
Ticket(i)=true (and therefore $p > 0$)
Effect:
Location(i) = on boat
$b = b + 1$
$p = p - 1$
Ticket(i)=False

Prove the following: Invariant: $t + b + p = 60$ (essentially conservation of mass (tickets) in the system)

Initially, we have $t = 60$, $b = 0$, and $p = 0$, so $60 + 0 + 0 = 60$.

After each transition:
GoToCounter(i)
No effect

PurchaseTicket(i)
$t_{new} = t - 1$ and $p_{new} = p + 1$, so $t_{new} + b + p_{new} = t - 1 + b + p + 1 = t + b + p = 60$.

GoToBoat(i)
No effect

GetOnBoat(i)
$t_{new} = t + 1$ and $p_{new} = p - 1$, so $t_{new} + b + p_{new} = t + 1 + b + p - 1 = t + b + p = 60$.

So the invariant holds.

We can use this to show that $b \leq 60$.

Since $t + b + p = 60$, $b \leq 60$ if $p + t \geq 0$.
Invariant 2: $t \geq 0$, $p \geq 0$,

GoToCounter(i)
No effect

PurchaseTicket(i)
Since we enter with $t > 0$, $t_{new} = t - 1 \geq 0$

GoToBoat(i)
No effect

GetOnBoat(i)
Since we enter with $p > 0$, $p_{new} = p - 1 \geq 0$.

So, since $t + b + p = 60$, $60 - p - t = b$. So $60 \geq b$.

Problem 2. *Consider an array/permutation $A[]$. Show that it is impossible to implement a two-element swap (eg, exchange elements 1 and 2 without changing any of the other elements' positions) via any sequence of 3-element cyclic shifts (eg, $1 \to 2 \to 3 \to 1$)). Hint: an inversion in a permutation is a pair of elements i and j with $i < j$ but $A[i] > A[j]$. Study the number of inversions in the permutation as you perform swaps and shifts.*

The following lemma is the hammer needed for the problem:

Lemma 0.1 *Any two-element swap changes the number of inversions in a permutation by an odd amount.*

Proof. Suppose we swap elements $x = A[i]$ and $y = A[j]$. Which inversions change? Well, since only x and y move, the only inversions that change are those involving x or y (or both). Furthermore, elements preceding x or following y stay in the same order with respect to x and y before and after the swap, so only the elements between x and y see any change in the number of inversions they are involved in.

So consider any element $z = A[k]$ for $i < k < j$. Such pairs have their order changed by the swap (from (x, z) to (z, x). Thus, if the pair (x, z) was an inversion before the swap, it is not an inversion after. If it was not an inversion, it becomes one. Similarly, if (z, y) was an inversion before the swap, it is not an inversion after, and vice versa. In other words, the number of inversions involving z changes by one with respect to x and by one with respect to y, for a total change of 0 or 2 depending on whether the changes cancel or add. So the total number of inversions involving x or y and an element between them changes by a sum of even numbers, which is even.

The last pair to consider is (x, y). This pair is exchanged by the swap, adding or removing one more inversion. Either way, this one more change makes the total change in inversions odd. ■

Corollary 0.2 *Any three-element cyclic shift changes the number of inversions in a permutation by an even amount.*

Proof. The 3-element shift $i \to j \to k \to i$ can be implemented as two swap, first of i and j, then of j and k. Since each of these swaps changes the number of inversions by an odd amount, doing them both changes the number of inversions by the sum of two odd amounts, which is even. ■

Now we can prove the claim of the problem. Let's assume we start with a permutation that has an even number of inversion (odd goes the same way). We claim the following invariant: every permutation reachable by a sequence of 3-element shifts has an even number of inversions. To see that this implies the problem claim, note that the permutation involving one swap has (by the above lemma) an odd number of inversions, implying that it is not a reachable permutation.

The proof of the invariant is by induction on the number of shifts we perform. Clearly it holds in the base case. Now suppose it applies to any permutation reachable after n shifts. Then consider a permutation reached after $n+1$ shifts. It was reached by a shift performed on an n-shift permutation, which by induction had an even number of inversion. The corollary tells us the last shift changed the even number of inversions by an even number, which means the new number of inversions is still even. This proves the inductive step.

Problem 3. *Let R_1 and R_2 be two equivalence relations on a set S. Show that $R_1 \cap R_2$ is an equivalence relation on S.*

An equivalence relation is reflexive, symmetric, and transitive. So, show these for $R_1 \cap R_2$.

Reflexive:
Since R_1 is reflexive, $\forall x \in S, (x, x) \in R_1$. Similarly, since R_2 is reflexive, $\forall x \in S, (x, x) \in R_2$. So, $\forall x \in S, (x, x) \in R_1 \cap R_2$

Symmetric:
If $(a, b) \in R_1$, then $(b, a) \in R_1$, and if $(a, b) \in R_2$, then $(b, a) \in R_2$, and $(a, b), (b, a) \in R_1 \cap R_2$. However, if $(a, b), (b, a) \notin R_1$, or $(a, b), (b, a) \notin R_2$, then $(a, b), (b, a) \notin R_1 \cap R_2$ and $R_1 \cap R_2$ is still symmetric.

Transitivity:
If $(a, b), (b, c) \in R_1$ then $(a, c) \in R_1$ and if $(a, b), (b, c) \in R_2$ then $(a, c) \in R_2$, and then $(a, b), (b, c), (a, c) \in R_1 \cap R_2$ and transitivity is maintained.

If however, (a, b) or $(b, c) \notin R_1$ or (a, b) or $(b, c) \notin R_2$, then said pair will not be in $R_1 \cap R_2$, so transitivity is still preserved.

Since $R_1 \cap R_2$ is reflexive, symmetric, and transitive, it is an equivalence relation.

Optional Problem 4. *Let A, B, and C be sets. Prove that $A - (B \cap C) = (A - B) \cup (A - C)$.*

First, let's define $A - B$ in terms of unions, intersections, and complements. $x \in A - B$ means that $x \in A \wedge x \notin B$, so $A - B = A \cap B^c$.

Rewriting $A - (B \cap C)$, and using set rules (which are exactly the same as the boolean algebra rules with $\wedge = \cap$, $\vee = \cup$, and $\neg = ^c$, we get:

$$\begin{aligned} A - (B \cap C) &= A \cap (B \cap C)^c \\ &= A \cap (B^c \cup C^c) \\ &= (A \cap B^c) \cup (A \cap C^c) \\ &= (A - B) \cup (A - C) \end{aligned}$$

Optional Problem 5. *Prove that for any relations Q, R and S*

$$Q \circ (R^c \circ S)^c \subseteq ((Q \circ R)^c \circ S)^c.$$

We want to prove that for any (a, d), if $(a, d) \in Q \circ (R^c \circ S)^c$ then $(a, d) \in ((Q \circ R)^c \circ S)^c$. Assume for contradiction this is not true, i.e., for some (a, d) we have $(a, d) \in Q \circ (R^c \circ S)^c$ and $(a, d) \in ((Q \circ R)^c \circ S)$. From the definition of composition we know there exist b and c such that $(a, b) \in (R^c \circ S)^c$, $(b, d) \in Q$, $(a, c) \in S$ and $(c, d) \in (Q \circ R)^c$.

We claim that $(c, b) \in R$. The proof is again for contradiction: assume $(c, b) \in R$ is false. We have $(c, b) \in R^c$ and we know that $(a, c) \in S$. From the definition of composition we get $(a, b) \in R^c \circ S$, which contradicts $(a, b) \in (R^c \circ S)^c$.

So, $(c, b) \in R$ and since we know that $(b, d) \in Q$, we also have $(c, d) \in Q \circ R$. This is a contradiction because $(c, d) \in (Q \circ R)^c$.

Optional Problem 6. *Let X and Y be sets, and $f : X \rightarrow Y$ be a function. Recall that for a set X, $f(X) = \{f(x) \mid x \in X\}$. Prove or disprove the following.*

(a) *For any subsets A and B of X, $f(A) \cup f(B) = f(A \cup B)$*

(b) *For any subsets A and B of Y, $f^{-1}(A) \cap f^{-1}(B) = f^{-1}(A \cap B)$*

(a) To show $f(A) \cup f(B) = f(A \cup B)$, show $f(A) \cup f(B) \subseteq f(A \cup B)$ and $f(A \cup B) \subseteq f(A) \cup f(B)$
Show $f(A) \cup f(B) \subseteq f(A \cup B)$:

$$\begin{aligned} y \in f(A) \cup f(B) &\rightarrow y \in f(A) \vee y \in f(B) \\ &\rightarrow \exists x, (x \in A \vee x \in B) \wedge (y = f(x)) \\ &\rightarrow \exists x \in A \cup B \wedge y = f(x) \\ &\rightarrow y \in f(A \cup B) \end{aligned}$$

Show $f(A \cup B) \subseteq f(A) \cup f(B)$:

$$
\begin{aligned}
y \in f(A \cup B) &\rightarrow \exists x \in A \cup B \wedge y = f(x) \\
&\rightarrow \exists x \in A \vee x \in B \wedge y = f(x) \\
&\rightarrow y \in f(A) \vee y \in f(B) \\
&\rightarrow y \in f(A) \cup f(B)
\end{aligned}
$$

(b) Note that for $f^{-1}(y)$ to exist, $f(x)$ must be a bijection. We need to show that $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$ and $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$.
1. Show $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$

$$
\begin{aligned}
x \in f^{-1}(A) \cap f^{-1}(B) &\rightarrow x \in f^{-1}(A) \wedge x \in f^{-1}(B) \\
&\rightarrow f(x) \in A \wedge f(x) \in B \\
&\rightarrow f(x) \in A \cap B \\
&\rightarrow x \in f^{-1}(A \cap B)
\end{aligned}
$$

2. Show $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$

$$
\begin{aligned}
x \in f^{-1}(A \cap B) &\rightarrow x \in f^{-1}(A) \wedge x \in f{-1}(B) \\
&\rightarrow f(x) \in A \wedge f(x) \in B \\
&\rightarrow x \in f^{-1}(A) \wedge x \in f^{-1}(B) \\
&\rightarrow x \in f^{-1}(A) \cap f^{-1}(B)
\end{aligned}
$$

Optional Problem 7. *Determine which of the relation following relations R on all people is reflexive, symmetric, antisymmetric, and/or transitive, where $(a, b) \in R$ iff:*

(a) *a is taller than b* –antisymmetric and transitive

(b) *a and b were born on the same day of the week* –reflexive, symmetric and transitive

(c) *a and b were born less than 24 hours apart* –reflexive and symmetric

(d) *a has a different first name from b* –symmetric

(e) *a and b have a common grandparent* –reflexive and symmetric

Optional Problem 8. *Define a relation R on $\mathbb{N}$ by, $(a, b) \in R$ if $\exists c \in \mathbb{N}$ such that $a^2 = b^2 + c^2$.*

Decide whether R is reflexive, symmetric, antisymmetric, or transitive.

Reflexive:
$a^2 = a^2 + c^2$ is true when $c = 0$. So R is reflexive.

Symmetric:
$a^2 = b^2 + c_1^2 \leftrightarrow b^2 = a^2 + c_2^2$? No. Let $a = 5, b = 4, c_1 = 3$ but $4^2 = 5^2 + c_2^2$ has no solution in the natural (or even real) numbers.

Antisymmetric:
Yes. Show that $(a, b) \in R \wedge (b, a) \in R \rightarrow a = b$. $a^2 = b^2 + c_1^2$ rearranges to $b^2 = a^2 - c_1^2 = a^2 + c_2^2$. However, we cannot find any solution to $c_2^2 = -c_1^2$, unless $c_1 = c_2 = 0$, in which case $a = b$. Since there is no solution for $c_2 \in \mathbb{N}$, R is antisymmetric.

Transitive:
$(x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$? No. Case against:
$(13, 5) \in R \rightarrow 169 = 25 + 144$ and $(5, 4) \in R \rightarrow 25 = 16 + 9$, but $(13, 4) \notin R$ since $13^2 = 16 + c^2$, so $c^2 = 153$ and 153 is not a square, so there's no solution for c. R is not transitive.

Optional Problem 9. *Show that the transitive closure of the symmetric closure of the reflexive closure of a relation R is the smallest equivalence relation that contains R.*

Let A be the set that R is a relation on. Let S be the transitive closure of the symmetric closure of the reflexive closure of a relation R. We need to prove that S is an equivalence relation, and then we need to prove that any equivalence relation that contains R also contains S and is therefore bigger than S.

To prove S is an equivalence relation, we need to prove it is reflexive, symmetric, and transitive.

Reflexivity is easy. Note that we got S by performing 3 "closure" operations on R, each of which adds (but does not remove) some pairs to the relation. The first, reflexive closure added all pairs (a, a) for $a \in A$, and neither of the symmetric or transitive closure operations remove these pairs. So S has them all, and is reflexive.

Now let T be the symmetric closure of the reflexive closure. Clearly T is reflexive and symmetric, and S is the transitive closure of T. We use this to prove S is symmetric. Suppose $(a, b) \in S$. Then by the definition of transitive closure of T, there's a path $(a = x_0, x_1, x_2, \ldots, x_n, b = x_{n+1})$ such that each $(x_i, x_{i+1}) \in T$. It follows from the symmetry of T that each $(x_{i+1}, x_i) \in T$, which implies (since S is a transitive closure) that $(x_{n+1}, x_0) = (b, a) \in S$. So S is symmetric.

Transitivity is also easy—since S is a transitive closure, it is transitive.

Now we have to prove that any equivalence relation containing R also contains S. Suppose we have an equivalence relation $P \supseteq R$. It follows that the reflexive closure of P contains the reflexive closure of R. but since P is reflexive, its reflexive closure is P—that is, P contains the reflexive closure of R. It follows that the symmetric closure of P contains the symmetric closure of the reflexive closure of R, namely T. But again, since P is an equivalence relation, its symmetric closure is P, meaning $P \supseteq T$. For similar reasons, $P \supseteq S$, as claimed.

Optional Problem 10. In the next problems, we are going to define the integers as a equivalence classes of pairs of natural numbers. For these problems, use only natural numbers and the properties of addition. Don't use negation or subtraction. You may use the fact that addition is associative, distributive, and commutative. You will also find it useful to use the following cancellation lemma: if $a + b = a + c$, then $b = c$ (this can be proved by induction from the Peano-axiom definition of plus, but you can take it as an axiom).

We define a relation $\equiv$ on $\mathbb{N} \times \mathbb{N}$ by $(a, b) \equiv (c, d)$ iff $a + d = b + c$. Prove that $\equiv$ is an equivalence relation.

Reflexive: $(a, b) \equiv (a, b)$ because $a + b = a + b$.
Symmetric: $(a, b) \equiv (c, d) \implies a + d = b + c \implies (c, d) \equiv (a, b)$.
Transitive $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$ means
$a + d = b + c$ and $c + f = d + e \implies a + d + c + f = b + c + d + e \implies a + f = b + e \implies (a, b) \equiv (e, f)$.

The solutions to the remaining problems will be handed out later

Optional Problem 11. Let $\mathbb{Z}$ be the set of equivalence classes of $\equiv$ (from the previous problem). We define a relation P from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$ by the following rule. $(X, Y) \sim_P Z$ iff $\exists a, b, c, d \in \mathbb{N}$ for which $(a, b) \in X$, $(c, d) \in Y$, and $(a + c, b + d) \in Z$. Note that $\sim_P$ is a binary relation, but its first argument is an ordered pair.

(a) Prove that $\sim_P$ is actually a function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$.

(b) Since P is a function, we will let $X + Y$ denote the (unique) Z for which $(X, Y) \sim_P Z$. We now define subtraction via a relation M as follows. $(X, Y) \sim_M Z$ if $X = Y + Z$. Prove that M is a function. Let $X - Y$ denote the Z for which $M((X, Y), Z)$.

Optional Problem 12. We now prove some properties of our plus and minus functions.

(a) Prove that there is an element Θ in $\mathbb{Z}$ such that $\forall X \in \mathbb{Z} \quad X + W = W + X = X$.

(b) Prove that for every element X in $\mathbb{Z}$, there is an element Y in $\mathbb{Z}$ such that $X + Y = \Theta$.

(c) Prove that $X - X = \Theta$.

(d) Give an injective function f from $\mathbb{N}$ to $\mathbb{Z}$ such that for any $x, y \in \mathbb{N}$, $f(x+y) = f(x) + f(y)$ (note that the right-hand side plus is operating on $\mathbb{Z}$). This function puts of "copy" of the natural numbers into the integers we've defined.