Solutions to Exercises 1, Part II: Transition Systems and Relations

1 Transition Systems and Invariants

Notation: $M = (S, I, r, A)$ is a transition system where S are the states, $I \subseteq S$ the set of initial states, $r \subseteq S \times A \times S$ and A is the input alphabet.

1.1 Special Invariants

Prove the following:

1. S is an inductive invariant. It is the largest among all invariants.

   Solution: We have $S \subseteq S$, $I \subseteq S$, and for every $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$, $s' \in S$. Therefore, S is an inductive invariant.

   Moreover, S is the largest among all invariants because any invariant needs to be a subset of S.

2. $Reach(M)$ is an inductive invariant.

   Solution: First, we have $Reach(M) \subseteq S$ and $I \subseteq Reach(M)$.

   Then, we want to show that for all $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$, if $s \in Reach(M)$, then $s' \in Reach(M)$

   Let $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$. Assume $s \in Reach(M)$. By definition of $Reach$, there exists a trace $(s_0, a_0, s_1, \ldots, a_n, s_n) \in Traces(M)$ such that $s_n = s$. By definition of $Traces$, we also have $(s_0, a_0, s_1, \ldots, a_n, s, a, s') \in Traces(M)$, which proves that $s' \in Reach(M)$.

3. $Reach(M)$ is the smallest of all possible invariants.

   Solution: By definition, any invariant is a superset of $Reach(M)$.

1.2 Closure of Invariants

A set of closed under an operation if applying the operation to elements of the set gives the result in the set. For example, the set of even natural numbers is closed under addition, whereas the set of odd natural numbers is not closed under addition.

Is the set of all invariants of M closed under the following operations:

1. union

   Solution: Let P_1 and P_2 be two invariants, i.e. $Reach(M) \subseteq P_1$, and $Reach(M) \subseteq P_2$. We have $Reach(M) \subseteq P_1 \cup P_2$, therefore $P_1 \cup P_2$ is also an invariant.

2. intersection

   Solution: Let P_1 and P_2 be two invariants, i.e. $Reach(M) \subseteq P_1$, and $Reach(M) \subseteq P_2$. We have $Reach(M) \subseteq P_1 \cap P_2$, because every state in $Reach(M)$ belongs to both P_1 and P_2 by assumption. Therefore $P_1 \cap P_2$ is also an invariant.

3. complement with respect to S

   Solution: Let P be an invariant, i.e. $Reach(M) \subseteq P$. We don't necessarily have $S \setminus Reach(M) \subseteq P$. For instance, we can make a machine where $Reach(M) = \emptyset$ (no initial states), with S a non-empty set of states, and define $P = \emptyset$.

4. operation $f : 2^S \to 2^S$ defined by $f(X) = Reach(M) \cup (S \setminus X)$

   Solution: For any set X (not just invariants), we have $Reach(M) \subseteq f(X)$, therefore $f(X)$ is an invariant.

Answer the same questions about all *inductive invariants* of M.

1. union

   Solution: Let P_1 and P_2 be two inductive invariants. We show that $P_1 \cup P_2$ is also an inductive invariant.

   First, we have $I \subseteq P_1 \cup P_2$ (because e.g. $I \subseteq P_1$).

   Second, let $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$. Assume $s \in P_1 \cup P_2$. We consider two cases. If $s \in P_1$, we use the fact that P_1 is an inductive invariant to conclude that $s' \in P_1$, and therefore $s' \in P_1 \cup P_2$. The second case is similar.

2. intersection

   Solution: Let P_1 and P_2 be two inductive invariants. We show that $P_1 \cap P_2$ is also an inductive invariant.

   First, we have $I \subseteq P_1 \cap P_2$ (because elements of I are both in P_1 and in P_2).

   Second, let $s, s' \in S$ and $a \in A$ such that $(s, a, s') \in r$. Assume $s \in P_1 \cap P_2$, i.e. $s \in P_1$, and $s \in P_2$. Since P_1 is an inductive invariant, we deduce that $s' \in P_1$, and similarly since P_2 is an inductive invariant, we deduce that $s' \in P_2$. Therefore $s' \in P_1 \cap P_2$.

3. complement with respect to S

   Solution: Same counter-example as above.

4. operation $f : 2^S \to 2^S$ defined by $f(X) = Reach(M) \cup (S \setminus X)$

   Solution: When X is an inductive invariant, $f(X)$ is not necessarily an inductive invariant. Consider a machine with two states $S = \{s_1, s_2\}$ and no initial state. Let there be a transition from s_1 to s_2 (with some letter), and no other transitions. The set $X = \{s_2\}$ is an inductive invariant. However, $f(X) = \{s_1\}$ is not (because of the transition from s_1 to s_2).

2 Relations

We consider relations $r, s, t, r_1, r_2, r_1', \ldots \subseteq A \times A$ (where A is just arbitrary set, nothing to do with the input signals of the transition systems). Here $X \subseteq A$. Define:

$$\begin{array}{rcl} \Delta_X & = & \{(x,x) \mid x \in X\} \\ r^{-1} & = & \{(x,y) \mid (y,x) \in r\} \\ X \bullet r & = & r[X] \\ ran(r) & = & \{y \mid \exists x.(x,y) \in r\} \end{array}$$

2.1 Relation Identities

Prove the following or give a counterexample.

In the solutions, some equivalences are easier to read from bottom to top (and some from top to bottom).

1. $(X \bullet r_1) \bullet r_2 = X \bullet (r_1 \circ r_2)$

   Solution: Let $z \in A$. We have:

$$\begin{array}{rl} z \in (X \bullet r_1) \bullet r_2 \Leftrightarrow & \exists y \in X \bullet r_1.\ (y,z) \in r_2 \\ \Leftrightarrow & \exists y \in A.\ y \in X \bullet r_1 \wedge (y,z) \in r_2 \\ \Leftrightarrow & \exists y \in A.\ \exists x \in X.\ (x,y) \in r_1 \wedge (y,z) \in r_2 \\ \Leftrightarrow & \exists x \in X.\ \exists y \in A.\ (x,y) \in r_1 \wedge (y,z) \in r_2 \\ \Leftrightarrow & \exists x \in X.\ (x,z) \in r_1 \circ r_2 \\ \Leftrightarrow & z \in X \bullet (r_1 \circ r_2) \end{array}$$

2. $(r \cup s) \circ t = (r \circ t) \cup (s \circ t)$

   Solution: Let $x, z \in A$. We have:

$$\begin{array}{rl} (x,z) \in (r \cup s) \circ t \Leftrightarrow & \exists y \in A.\ (x,y) \in r \cup s \wedge (y,z) \in t \\ \Leftrightarrow & \exists y \in A.\ ((x,y) \in r \vee (x,y) \in s) \wedge (y,z) \in t \\ \Leftrightarrow & \exists y \in A.\ ((x,y) \in r \wedge (y,z) \in t) \vee ((x,y) \in s \wedge (y,z) \in t) \\ \Leftrightarrow & (\exists y \in A.\ (x,y) \in r \wedge (y,z) \in t) \vee (\exists y \in A.\ (x,y) \in s \wedge (y,z) \in t) \\ \Leftrightarrow & (x,z) \in r \circ t \vee (x,z) \in s \circ t \\ \Leftrightarrow & (x,z) \in (r \circ t) \cup (s \circ t) \end{array}$$

3. $(r \cap s) \circ t = (r \circ t) \cap (s \circ t)$

   Solution: A counterexample:
   $r = \{(0,1)\}$, $s = \{(0,2)\}$ and $t = \{(1,0),(2,0)\}$.

   We have $(r \cap s) \circ t = \emptyset$, while $(r \circ t) \cap (s \circ t) = \{(0,0)\}$.

4. $(r_1 \circ r_2)^{-1} = (r_2^{-1} \circ r_1^{-1})$

Solution: Let $x, z \in A$. We have:

$$\begin{aligned}(z,x) \in (r_1 \circ r_2)^{-1} &\Leftrightarrow (x,z) \in r_1 \circ r_2 \\ &\Leftrightarrow \exists y \in A.\ (x,y) \in r_1 \wedge (y,z) \in r_2 \\ &\Leftrightarrow \exists y \in A.\ (y,x) \in r_1^{-1} \wedge (z,y) \in r_2^{-1} \\ &\Leftrightarrow \exists y \in A.\ (z,y) \in r_2^{-1} \wedge (y,x) \in r_1^{-1} \\ &\Leftrightarrow (z,x) \in r_2^{-1} \circ r_1^{-1}\end{aligned}$$

5. $X \bullet r = ran(\Delta_X \circ r)$

   Solution: Let $y \in A$. We have:

$$\begin{aligned}y \in X \bullet r &\Leftrightarrow \exists x \in X.\ (x,y) \in r \\ &\Leftrightarrow \exists x \in A.\ x \in X \wedge (x',y) \in r \\ &\Leftrightarrow \exists x \in A.\ \exists x' \in A.\ x = x' \wedge x \in X \wedge (x',y) \in r \\ &\Leftrightarrow \exists x \in A.\ \exists x' \in A.\ (x,x') \in \Delta_X \wedge (x',y) \in r \\ &\Leftrightarrow \exists x \in A.\ (x,y) \in \Delta_X \circ r \\ &\Leftrightarrow y \in ran(\Delta_X \circ r)\end{aligned}$$

6. If $r_1 \subseteq r_1'$ then $r_1 \circ r_2 \subseteq r_1' \circ r_2$ and $r_2 \circ r_1 \subseteq r_2 \circ r_1'$.

   Solution: Let $x, z \in A$. We have:

$$\begin{aligned}(x,z) \in r_1 \circ r_2 &\Leftrightarrow \exists y \in A.\ (x,y) \in r_1 \wedge (y,z) \in r_2 \\ &\Rightarrow \exists y \in A.\ (x,y) \in r_1' \wedge (y,z) \in r_2 \text{ because } r_1 \subseteq r_1' \\ &\Leftrightarrow (x,z) \in r_1' \circ r_2\end{aligned}$$

   Also,

$$\begin{aligned}(x,z) \in r_2 \circ r_1 &\Leftrightarrow \exists y \in A.\ (x,y) \in r_2 \wedge (y,z) \in r_1 \\ &\Rightarrow \exists y \in A.\ (x,y) \in r_2 \wedge (y,z) \in r_1' \text{ because } r_1 \subseteq r_1' \\ &\Leftrightarrow (x,z) \in r_2 \circ r_1'\end{aligned}$$

7. If $r_1 \subseteq r_1'$ then $r_1 \cup r_2 \subseteq r_1' \cup r_2$ and $r_2 \cup r_1 \subseteq r_2 \cup r_1'$.

   Solution: Let $x, y \in A$. We have:

$$\begin{aligned}(x,y) \in r_1 \cup r_2 &\Leftrightarrow (x,y) \in r_1 \vee (x,y) \in r_2 \\ &\Rightarrow (x,y) \in r_1' \vee (x,y) \in r_2 \text{ because } r_1 \subseteq r_1' \\ &\Leftrightarrow (x,y) \in r_1' \cup r_2\end{aligned}$$

Also,

$$\begin{aligned}(x,y) \in r_2 \cup r_1 &\Leftrightarrow (x,y) \in r_2 \vee (x,y) \in r_1 \\ &\Rightarrow (x,y) \in r_2 \vee (x,y) \in r_1' \text{ because } r_1 \subseteq r_1' \\ &\Leftrightarrow (x,y) \in r_2 \cup r_1'\end{aligned}$$

2.2 Transitive relations

Given a relation $r \subseteq A \times A$, prove that r is transitive if and only if $r \circ r \subseteq r$.

Solution:

$$\begin{aligned}r \circ r \subseteq r &\Leftrightarrow \forall x, z \in A.\ (x,z) \in r \circ r \Rightarrow (x,z) \in r \\ &\Leftrightarrow \forall x, z \in A.\ (\exists y \in A.(x,y) \in r \wedge (y,z) \in r) \Rightarrow (x,z) \in r \\ &\Leftrightarrow \forall x, z \in A.\ \forall y \in A.\ ((x,y) \in r \wedge (y,z) \in r) \Rightarrow (x,z) \in r \\ &\Leftrightarrow \forall x, y, z \in A.\ ((x,y) \in r \wedge (y,z) \in r) \Rightarrow (x,z) \in r \\ &\Leftrightarrow \text{r is transitive}\end{aligned}$$

2.3 Symmetric relations

Recall that a relation $r \subseteq A \times A$ is symmetric if $\forall x, y \in A.\ (x,y) \in r \Rightarrow (y,x) \in r$.
Now let r be an arbitrary relation. Prove that $r^{-1} \circ (r \cup r^{-1})^* \circ r$ is symmetric.

Solution: (Sketch)

First, since the composition of two symmetric relations is symmetric, we can show by induction on $n \geq 0$ that for any symmetric relation r, r^n is symmetric.

Second, taking the union of symmetric relations gives a symmetric relation, which means that for any symmetric relation r, r^* is also symmetric (using the previous point).

We can establish that $r \cup r^{-1}$ is a symmetric relation, and using the second point, that $(r \cup r^{-1})^*$ is also symmetric.

Finally, let $x, t \in A$. We have:

$$\begin{aligned}(x,t) \in r^{-1} \circ (r \cup r^{-1})^* \circ r &\Leftrightarrow \exists y \in A.\ \exists z \in A.\ (x,y) \in r^{-1} \wedge (y,z) \in (r \cup r^{-1})^* \wedge (z,t) \in r \\ &\Leftrightarrow \exists z \in A.\ \exists y \in A.\ (t,z) \in r^{-1} \wedge (z,y) \in (r \cup r^{-1})^* \wedge (y,x) \in r \\ &\Leftrightarrow (t,x) \in r^{-1} \circ (r \cup r^{-1})^* \circ r\end{aligned}$$

To go from the first to the second line, we use the fact that $(r \cup r^{-1})^*$ is symmetric.

2.4 Transitive closure

Recall that we define the powers of a relation $r \subseteq A \times A$ as follows:

$$r^0 = \triangle_A, \quad r^1 = r, \quad \text{and} \quad r^{n+1} = r^n \circ r$$

We showed that the *reflexive and transitive closure* $r^* = \bigcup_{n \geq 0} r^n$ is the smallest reflexive and transitive relation on A containing r. Show that for any relation r on a set A, $(r \cup r^{-1})^*$ is the least equivalence relation containing r. Precisely, show that

(i) $(r \cup r^{-1})^*$ is an equivalence relation, and

Solution: We have three things to prove:

1. (Reflexivity) Let $x \in A$. We have $(x, x) \in (r \cup r^{-1})^*$ because $\triangle_A \subseteq (r \cup r^{-1})^*$.
2. (Symmetry) As seen in the previous section, $(r \cup r^{-1})^*$ is symmetric.
3. (Transitive) Let $(x, y) \in (r \cup r^{-1})^*$ and $(y, z) \in (r \cup r^{-1})^*$. By definition, there exist $n, m \geq 0$ such that $(x, y) \in (r \cup r^{-1})^n$ and $(y, z) \in (r \cup r^{-1})^m$. Therefore $(x, z) \in (r \cup r^{-1})^n \circ (r \cup r^{-1})^m = (r \cup r^{-1})^{n+m}$. This shows that $(x, z) \in (r \cup r^{-1})^*$.

(ii) if s is an equivalence relation containing r, then $(r \cup r^{-1})^* \subseteq s$.

Solution: Let s be an equivalence relation containing r. We prove by induction over $n \in \mathbb{N}$ that $(r \cup r^{-1})^n \subseteq s$.

1. (Case $n = 0$) $(r \cup r^{-1})^0 = \triangle_A \subseteq s$ because s is reflexive.
2. (Case $n = n' + 1$) Assume by induction that $(r \cup r^{-1})^{n'} \subseteq s$. We know that $r \subseteq s$, and that s is symmetric, therefore $r^{-1} \subseteq s$. Thus, we also have: $r \cup r^{-1} \subseteq s$.
   Finally, we have $(r \cup r^{-1})^n = (r \cup r^{-1})^{n'} \circ (r \cup r^{-1}) \subseteq s \circ s \subseteq s$ (because s is transitive), which concludes the proof.

3 Finite State Machines with Boolean Variables

We consider in this exercise finite-state machines enriched with boolean variables (FSM for short). Formally, an FSM is a pair (V, Q, δ) where:

- V is a finite set of (boolean) variable names,
- Q is a finite set of states,
- For every pair of states p and q, $\delta(p, q)$ is a propositional formula containing variables from V and V', where V' is a copy of V with primed variable names.

A configuration of the FSM is determined by a pair (q, m) where

- q is a state in Q, called the *control state*,
- $m : V \to \{\top, \bot\}$ is a mapping from variable names to true or false.

The FSM can move from a configuration (p, m) to (q, m') if the formula $\delta(p, q)$ is true when we interpret every variable from V using the mapping m, and every variable in V' using m'. We define the relation $r \subseteq (Q \times V \to \{\top, \bot\}) \times (Q \times V \to \{\top, \bot\})$ to contain all such pairs of configurations (p, m) and (q, m').

Consider now the FSM in Figure **??**, inspired from Peterson's algorithm (we recommend reading this page before the exercise). We made use of two conventions when drawing the figure:

- When there is no transition drawn from a state p to a state q, we mean that $\delta(p, q) = \bot$ in the FSM.
- When a primed variable X' does not appear in a transition, we leave the variable unchanged, meaning that there is an implicit conjunct $X' \leftrightarrow X$ in the transition.

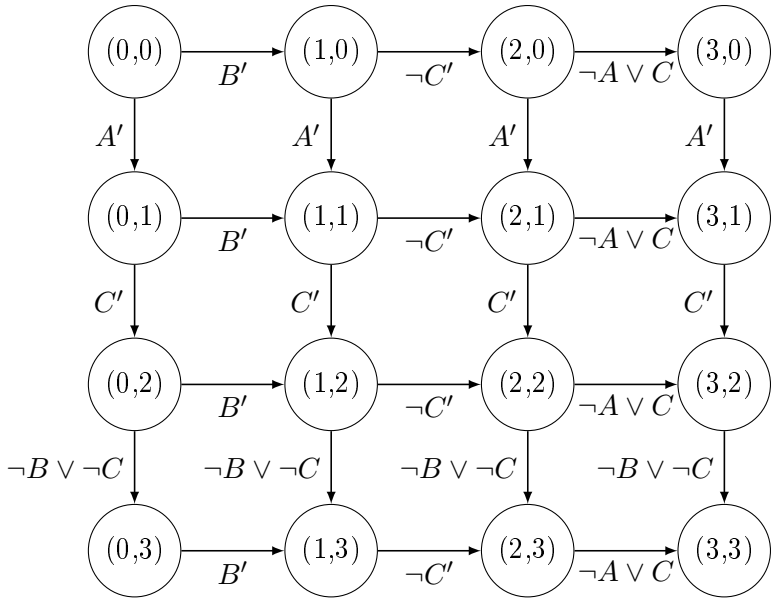

Figure 1: A finite-state machine with boolean variables $\{A, B, C\}$.

For example, the transition from $(0, 0)$ to $(0, 1)$ can be taken regardless of the initial mapping of boolean variables. It changes variable A to $\top$, and leaves the variables B and C unchanged. The transition from $(2, 0)$ to $(3, 0)$ can only be taken when the mapping of boolean variables respects $\neg A \vee C$, and leaves all variables unchanged.

Does there exist mappings m and m' such that the FSM can move (using multiple steps) from configuration $((0, 0), m)$ to $((3, 3), m')$, i.e. such that $(((0, 0), m), ((3, 3), m')) \in r^*$?

Solution: No. We can establish the following inductive invariant of the configurations of the FSM:

$$\begin{aligned} P = \{((x, y), m) \mid & (x \geq 1 \Rightarrow m(B)) \wedge \\ & (y \geq 1 \Rightarrow m(A)) \wedge \\ & ((x, y) = (3, 2) \Rightarrow m(C)) \wedge \\ & ((x, y) = (2, 3) \Rightarrow \neg m(C) \wedge \\ & (x, y) \neq (3, 3)\} \end{aligned}$$