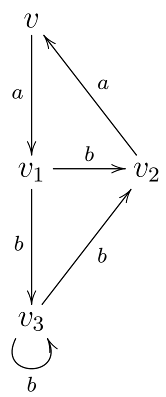
Exercise 1



Consider the labelled transition system above. Compute the relation $\sim$ of strong bisimilarity (union of all strong bisimulation relations) as a maximum fixed point.

Solution of Exercise 1

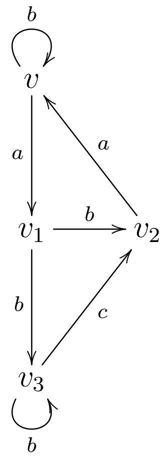
Let $Proc = \{v, v_1, v_2, v_3\}$ and let $I = \{(v, v), (v_1, v_1), (v_2, v_2), (v_3, v_3)\}$.

$$\begin{aligned}
X_0 &= Proc \times Proc \\
F(X_0) &= \{(v, v_2), (v_2, v), (v_1, v_3), (v_3, v_1)\} \cup I \\
F(F(X_0)) &= \{(v_1, v_3), (v_3, v_1)\} \cup I \\
F(F(F(X_0))) &= \{(v_1, v_3), (v_3, v_1)\} \cup I = F(F(X_0))\,.
\end{aligned}$$

As a conclusion $\sim\ = \{(v_1, v_3), (v_3, v_1)\} \cup I$. One should be able to argue, what is the reason why a given pair was removed or stayed in each iteration of the fixed-point computation. For example, the pair $(v, v_1) \in X_0$ was removed from $F(X_0)$ because e.g. $v_1 \xrightarrow{b} v_3$ but v cannot do any action b. Similarly, the pair (v, v_2) that belongs to $F(X_0)$ was removed from $F(F(X_0))$ because $v \xrightarrow{a} v_1$ and the only transition that can match this from the state v_2 is $v_2 \xrightarrow{a} v$ but the new pair (v_1, v) that we reached does not belong to $F(X_0)$. On the other hand, for example (v_1, v_3) can stay in $F(F(F(X_0)))$ because

- if $v_1 \xrightarrow{b} v_2$ then $v_3 \xrightarrow{b} v_2$ and $(v_2, v_2) \in F(F(X_0))$, and
- if $v_1 \xrightarrow{b} v_3$ then $v_3 \xrightarrow{b} v_3$ and $(v_3, v_3) \in F(F(X_0))$, and
- if $v_3 \xrightarrow{b} v_3$ then $v_1 \xrightarrow{b} v_3$ and $(v_3, v_3) \in F(F(X_0))$, and
- if $v_3 \xrightarrow{b} v_2$ then $v_1 \xrightarrow{b} v_2$ and $(v_2, v_2) \in F(F(X_0))$.

Exercise 2*



Determine (using both the fixed-point computation as well as using games) whether the following recursively defined variable X holds in a given state of the LTS above (note the added b loop in v and the new action c). Try to formulate the properties below intuitively and argue why a minimum or maximum fixed point was used.

1. $X \stackrel{min}{=} [a]ff \vee \langle a\rangle X, \quad v_2 \stackrel{?}{\models} X$
2. $X \stackrel{min}{=} (\langle a\rangle tt \wedge \langle b\rangle tt) \vee \langle a\rangle X \vee \langle b\rangle X, \quad v_1 \stackrel{?}{\models} X$
3. $X \stackrel{min}{=} [a]ff \vee (\langle a\rangle X \wedge [b]ff), \quad v_2 \stackrel{?}{\models} X$
4. $X \stackrel{max}{=} \langle b\rangle X \wedge [c]ff, \quad v \stackrel{?}{\models} X$
5. $X \stackrel{max}{=} ([a]ff \vee [b]ff) \wedge [a]X \wedge [b]X, \quad v_1 \stackrel{?}{\models} X$

Solution of Exercise 2

1. The property X says "we can reach a state (by performing the actions a) such that the action a becomes disabled" and it holds in the state v_2. It is a minimum fixed point because there is a finite evidence for this fact (in our case the evidence is the path $v_2 \xrightarrow{a} v \xrightarrow{a} v_1$ that ends in a state v_1 where a is disabled).

   Fixed-point computation, starting from the bottom (empty set), where

$$X_{i+1} = [\cdot a\cdot]\emptyset \cup \langle\cdot a\cdot\rangle X_i \ .$$

$$
\begin{aligned}
X_0 &= \emptyset \\
X_1 &= \{v_1, v_3\} \\
X_2 &= \{v_1, v_3, v\} \\
X_3 &= \{v_1, v_3, v, v_2\} \\
X_4 &= X_3
\end{aligned}
$$

Because $v_2 \in X_3$ we know that $v_2 \models X$.

We can also argue using the game characterization that Defender has a winning strategy from the pair (v_2, X). The strategy looks as follows

$$
\begin{aligned}
(v_2, X) \longrightarrow (v_2, [a]\mathit{ff} \vee \langle a\rangle X) \xrightarrow{D} (v_2, \langle a\rangle X) \xrightarrow{D} \\
(v, X) \longrightarrow (v, [a]\mathit{ff} \vee \langle a\rangle X) \xrightarrow{D} (v, \langle a\rangle X) \xrightarrow{D} \\
(v_1, X) \longrightarrow (v_1, [a]\mathit{ff} \vee \langle a\rangle X) \xrightarrow{D} (v_1, [a]\mathit{ff})
\end{aligned}
$$

and Attacker losses as he cannot pick any a-transition from the state v_1. Note that all moves in this strategy were done by Defender (annotated by the label D) and Attacker was never given an option to make a choice, hence this is a universal winning strategy for Defender.

2. The property X says ”there exists a path consisting of either the actions a or b to a state where both a and b and enabled at the same time”. This property X holds in v_1 and as before, there is a finite evidence if the property holds (the path), hence the minimum fixed point.

   Fixed-point computation, starting from the bottom (empty set), where

$$X_{i+1} = (\langle \cdot a \cdot \rangle \{v, v_1, v_2, v_3\} \cap \langle \cdot b \cdot \rangle \{v, v_1, v_2, v_3\}) \cup \langle \cdot a \cdot \rangle X_i \cup \langle \cdot b \cdot \rangle X_i \ .$$

$$
\begin{aligned}
X_0 &= \emptyset \\
X_1 &= \{v\} \\
X_2 &= \{v, v_2\} \\
X_3 &= \{v, v_2, v_1\} \\
X_4 &= X_3
\end{aligned}
$$

   Because $v_1 \in X_3$ we know that $v_1 \models X$. On the other hand, $v_3 \notin X_3$ and hence $v_3 \not\models X$.

   Defender’s universal winning strategy from (v_1, X) can be described in a very similar way as in the previous case so that the players end up in the pair $(v, (\langle a\rangle \mathit{tt} \wedge \langle b\rangle \mathit{tt}) \vee \langle a\rangle X \vee \langle b\rangle X)$ where Defender selects the first disjunct and the play continues from $(v, \langle a\rangle \mathit{tt} \wedge \langle b\rangle \mathit{tt})$. Now Attacker has two options how to play: $(v, \langle a\rangle \mathit{tt} \wedge \langle b\rangle \mathit{tt}) \xrightarrow{A} (v, \langle a\rangle \mathit{tt})$ or $(v, \langle a\rangle \mathit{tt} \wedge \langle b\rangle \mathit{tt}) \xrightarrow{A} (v, \langle b\rangle \mathit{tt})$ but in any case the defender can continue by executing the transition with label a resp. b and the formula becomes tt which is a winning configuration for Defender.

3. The property X says "there exists a path leading to a state where the action a is disabled but along this path the action b should be disabled". This property X does not hold in v_2. The property is a minimum fixed-point because if this property holds in some state then there is a finite path demonstrating this fact.

   Fixed-point computation, starting from the bottom (empty set), where

   $$X_{i+1} = [\cdot a\cdot]\emptyset \cup (\langle\cdot a\cdot\rangle X_i \cap [\cdot b\cdot]\emptyset) .$$

   $$\begin{aligned} X_0 &= \emptyset \\ X_1 &= \{v_1, v_3\} \\ X_2 &= X_1 \end{aligned}$$

   Because $v_2 \notin X_3$ we know that $v_2 \not\models X$. On the other hand, $v_1 \models X$ and $v_3 \models X$.

   We can argue that $v_2 \not\models X$ by finding Attacker's winning strategy from (v_2, X). After unfolding X we are in the configuration $(v_2, [a]\mathit{ff} \vee (\langle a\rangle X \wedge [b]\mathit{ff}))$. Clearly, if Defender chooses the first disjunct $[a]\mathit{ff}$, she will lose in the next round as the action a is enabled in v_2 and we end up in ff. So assume that Defender chooses to play $(v_2, [a]\mathit{ff} \vee (\langle a\rangle X \wedge [b]\mathit{ff})) \xrightarrow{D} (v_2, \langle a\rangle X \wedge [b]\mathit{ff})$. Attacker's strategy is to continue from $(v_2, \langle a\rangle X)$ and Defender can only enter the next configuration (v, X). As before X gets unfolded and Defender cannot win by choosing the disjunct $[a]\mathit{ff}$ as a is still enabled in v. Hence assume that Defender chooses to enter the configuration $(v, \langle a\rangle X \wedge [b]\mathit{ff})$. However, now attacker can play $(v, \langle a\rangle X \wedge [b]\mathit{ff}) \xrightarrow{A} (v, [b]\mathit{ff})$ and because b is enabled in v, Defender will lose also in this case. Hence Attacker has a universal wining strategy from (v_2, X).

4. The property X says "there is an infinite path containing only b actions and along this path the action c is never enabled". This property X holds in v due to the loop with b. However, it does not hold e.g. in v_1 as we can explore a finite prefix of the LTS starting from v_1 and see that either that the action c becomes enabled (state v_3) or the action b is not enabled any more (state v_2). Hence there is a finite counter-example if the property does not hold and the property is defined as a maximum fixed point.

   Fixed-point computation, starting from the top (set of all processes), where

   $$X_{i+1} = \langle\cdot b\cdot\rangle X_i \cap [\cdot c\cdot]\emptyset .$$

   $$\begin{aligned} X_0 &= \{v, v_1, v_2, v_3\} \\ X_1 &= \{v, v_1\} \\ X_2 &= \{v\} \\ X_3 &= X_2 \end{aligned}$$

   Because $v \in X_2$ we know that $v \models X$ and this is the only state where X holds.

Defender's winning strategy from (v, X) is as follows. First, X gets unfolded and from $(v, \langle b \rangle X \wedge [c]\mathit{ff})$ Attacker has two choices. If he chooses to continue from $\langle b \rangle X$, Defender can perform the action b in v and reaches the configuration (v, X) that we have started from, meaning that the play can get infinite as long as Attacker keeps choosing the first conjuct (an infinite play is winning for Defender as we deal with a maximum fixed point). Hence at some point Attacker must choose to enter the configuration $(v, [c]\mathit{ff})$ but this is also loosing for Attacker as c is not enabled in the state v.

5. The property X says "every state that is reachable by performing the actions a and b never allows at the same time both the actions a and b". This property X holds only in v_3. If the property does not hold, there is a finite counter-example in a form of a path consisting of only labels a and b and ending in a state where both a and b are enabled. Hence it is defined as a maximum fixed point.

   Fixed-point computation, starting from the top (set of all processes), where

$$X_{i+1} = ([\cdot a \cdot]\emptyset \cup [\cdot b \cdot]\emptyset) \cap [\cdot a \cdot]X_i \cap [\cdot b \cdot]X_i \; .$$

$$\begin{aligned} X_0 &= \{v, v_1, v_2, v_3\} \\ X_1 &= \{v_1, v_2, v_3\} \\ X_2 &= \{v_1, v_3\} \\ X_3 &= \{v_3\} \\ X_4 &= X_3 \end{aligned}$$

   Because $v_1 \notin X_3$ we know that $v_1 \not\models X$ and the only state that satisfies X is v_3.

   Attacker has a universal winning strategy from (v_1, X) by playing:

$$(v_1, X) \longrightarrow (v_1, ([a]\mathit{ff} \vee [b]\mathit{ff}) \wedge [a]X \wedge [b]X) \xrightarrow{A} (v_1, [b]X) \xrightarrow{A}$$
$$(v_2, X) \longrightarrow (v_2, ([a]\mathit{ff} \vee [b]\mathit{ff}) \wedge [a]X \wedge [b]X) \xrightarrow{A} (v_2, [a]X) \xrightarrow{A}$$
$$(v, X) \longrightarrow (v, ([a]\mathit{ff} \vee [b]\mathit{ff}) \wedge [a]X \wedge [b]X) \xrightarrow{A} (v, [a]\mathit{ff} \vee [b]\mathit{ff}) \, .$$

   Notice that Defender didn't have any choice so far. However, whatever Defender chooses from the current configuration will be loosing for her as both a and b are enabled in v.

Exercise 3

Express the following properties as formulae in HML with one recursively defined variable and argue for the choice of minimum or maximum fixed point.

1. There is an infinite path consisting of only actions a and b.
2. There is an infinite path consisting of only actions a and b where the first action is a and where a and b alternate.
3. One can reach a state where the action sequence aba is enabled.
4. One can reach a state where the action sequence aba is enabled and before this happens, the action c is always enabled.

Solution of Exercise 3

1. $X \stackrel{max}{=} \langle a \rangle X \vee \langle b \rangle X$
   It is a maximum fixed point because there is no finite evidence for such an infinite path but there is a finite counter-example if such path does not exist.
2. $X \stackrel{max}{=} \langle a \rangle \langle b \rangle X$
   As before, this is a maximum fixed point.
3. $X \stackrel{min}{=} \langle a \rangle \langle b \rangle \langle a \rangle tt \vee \langle Act \rangle X$
   This is a minimum fixed point because there is a finite evidence if the property holds (the actual path that enables the sequence aba).
4. $X \stackrel{min}{=} \langle a \rangle \langle b \rangle \langle a \rangle tt \vee (\langle c \rangle tt \wedge \langle Act \rangle X)$
   As before, this is a minimum fixed point.