Exercises with (Some) Solutions

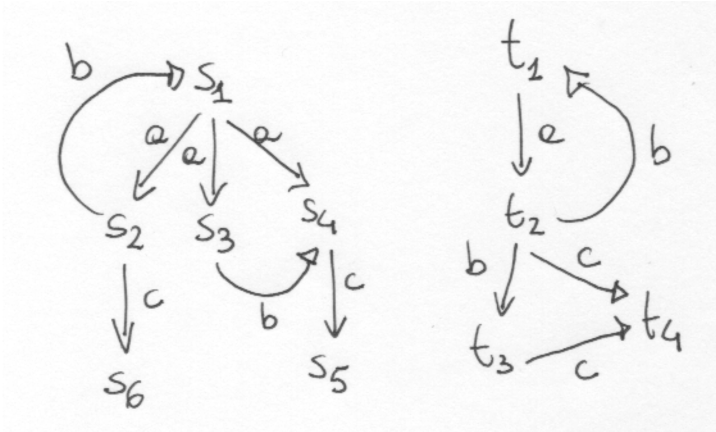
Teacher: Luca Tesei

Master of Science in Computer Science - University of Camerino

Contents

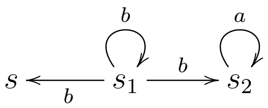
1 Strong Bisimulation and HML

Exercise 1.1 *Consider the following LTS:*



1. *Tell whether or not s_1 is strongly bisimilar to t_1. Justify your answer formally.*
2. *Determine all the states of the LTS that satisfy the following formulas:*
   - $[a]\langle b\rangle tt \wedge [a]\langle c\rangle tt$
   - $\langle a\rangle\langle b\rangle tt \vee \langle c\rangle\langle b\rangle[c] ff$
   - $[a][b]\langle c\rangle tt$

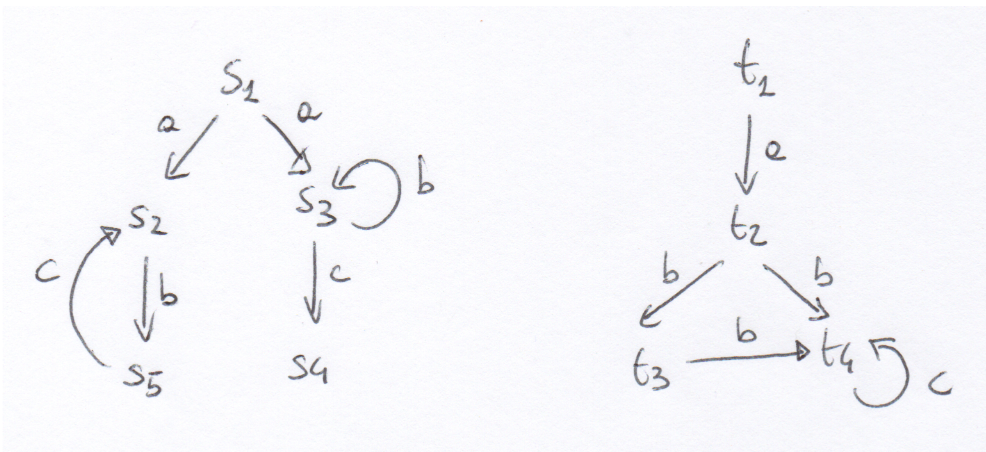
Exercise 1.2 *Consider the following labelled transition system.*



Compute for which sets of states $[\![X]\!] \subseteq \{s, s_1, s_2\}$ the following formulae are true.

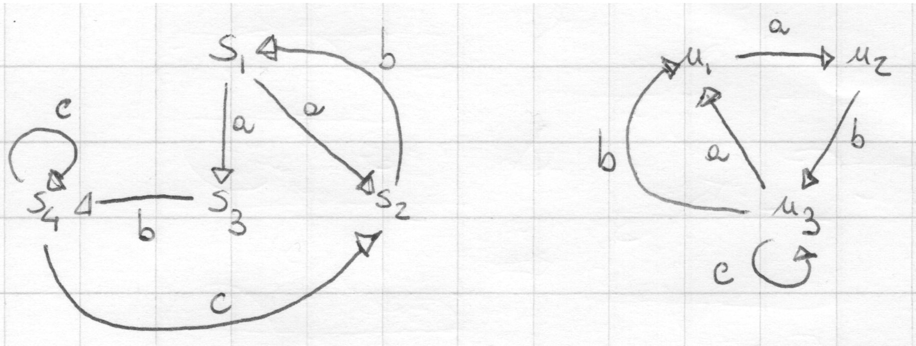
- $X = \langle a\rangle tt \vee [b]X$
- $X = \langle a\rangle tt \vee ([b]X \wedge \langle b\rangle tt)$

Exercise 1.3 *Consider the following LTS:*



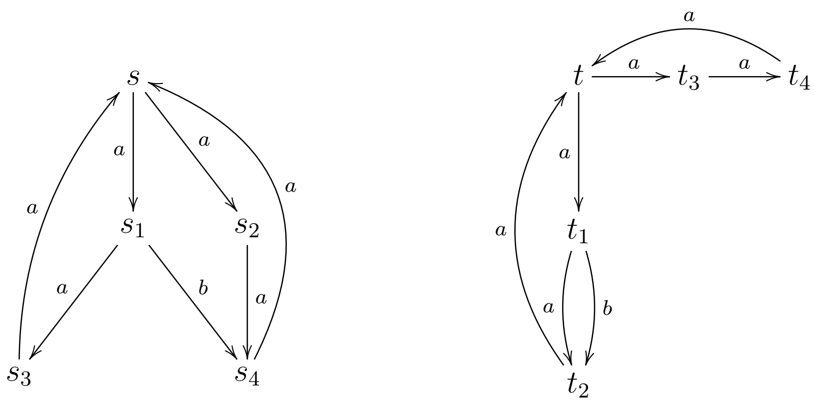
1. *Tell whether or not s_1 is strongly bisimilar to t_1. Justify your answer formally.*
2. *Determine all the states of the LTS that satisfy the following formulas:*
   - $[a]\langle b\rangle tt$
   - $\langle a\rangle(\langle b\rangle tt \vee \langle c\rangle tt)$
   - $\langle b\rangle[b][c]ff$

Exercise 1.4 *Consider the following LTS:*



1. *Tell whether or not s_1 is strongly bisimilar to u_1. Justify your answer formally.*
2. *Determine all the states of the LTS that satisfy the following formulas:*
   - $\varphi_1 = [a]\langle b\rangle\langle c\rangle tt$
   - $\varphi_2 = \langle a\rangle\langle b\rangle\langle c\rangle tt$
   - $\varphi_3 = [a]\langle b\rangle[c]ff$
   - $\varphi_4 = \langle a\rangle\langle b\rangle[c]ff$

Exercise 1.5 *Consider the following labelled transition system.*



Show that $s \sim t$ by finding a strong bisimulation R containing the pair (s, t).

Exercise 1.6 *Consider the CCS processes P and Q defined by:*

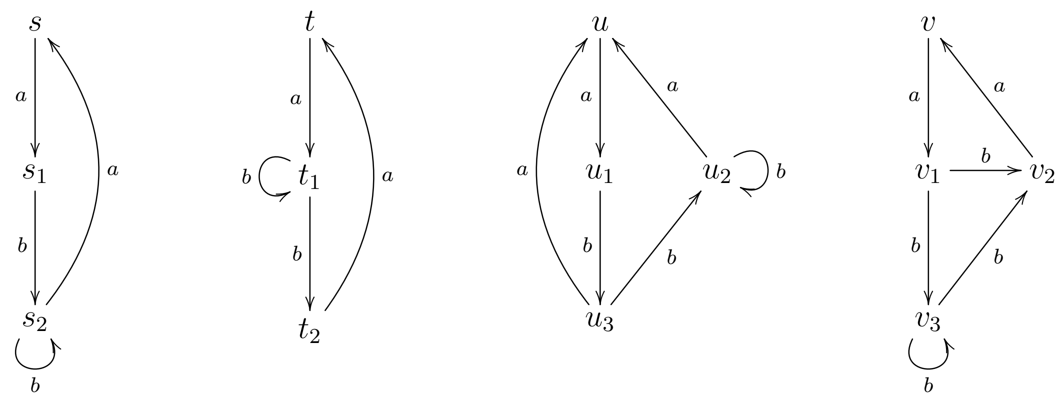
$$P \stackrel{\text{def}}{=} a.P_1$$
$$P_1 \stackrel{\text{def}}{=} b.P + c.P$$

and

$$Q \stackrel{\text{def}}{=} a.Q_1$$
$$Q_1 \stackrel{\text{def}}{=} b.Q_2 + c.Q$$
$$Q_2 \stackrel{\text{def}}{=} a.Q_3$$
$$Q_3 \stackrel{\text{def}}{=} b.Q + c.Q_2 \ .$$

Show that $P \sim Q$ holds by finding an appropriate strong bisimulation.

Exercise 1.7 *Consider the following labelled transition system.*



Decide whether $s \stackrel{?}{\sim} t$, $s \stackrel{?}{\sim} u$, and $s \stackrel{?}{\sim} v$. Support your claims by giving a universal winning strategy either for the attacker (in the negative case) or the defender (in the positive case). In the positive case you can also define a strong bisimulation relating the pair in question.

Exercise 1.8 *Prove that for any CCS processes P and Q the following laws hold:*

- $P \mid Nil \sim P$
- $P + Nil \sim P$

Exercise 1.9 *Argue that any two strongly bisimilar processes have the same sets of traces, i.e., that*

$$s \sim t \text{ implies } Traces(s) = Traces(t).$$

Hint: you can find useful the game characterization of strong bisimilarity.

Exercise 1.10 *Is it true that any relation R that is a strong bisimulation must be reflexive, transitive and symmetric? If yes then prove it, if not then give counter examples, i.e.*

- *define an LTS and a binary relation on states which is not reflexive but it is a strong bisimulation*
- *define an LTS and a binary relation on states which is not symmetric but it is a strong bisimulation*
- *define an LTS and a binary relation on states which is not transitive but it is a strong bisimulation.*

Exercise 1.11 *Find (one) labelled transition system with an initial state* s *such that it satisfies (at the same time) the following properties:*

- $s \models \langle a \rangle (\langle b \rangle \langle c \rangle tt \wedge \langle c \rangle tt)$
- $s \models \langle a \rangle \langle b \rangle ([a] ff \wedge [b] ff \wedge [c] ff)$
- $s \models [a] \langle b \rangle ([c] ff \wedge \langle a \rangle tt)$

Exercise 1.12 *Assume an arbitrary CCS defining equation* $K \stackrel{\text{def}}{=} P$ *where* K *is a process constant and* P *is a CCS expression. Prove that* $K \sim P$. *(Hint: by using SOS rules for CCS, examine the possible transitions from* K *and* P.*)*

Exercise 1.13 *Decide whether the following claims are true or false. Support your claims either by using bisimulation games or directly the definition of strong/weak bisimilarity.*

- $a.\tau.Nil \stackrel{?}{\sim} \tau.a.Nil$
- $\tau.a.A + b.B \stackrel{?}{\sim} \tau.(a.A + b.B)$
- $\tau.Nil + (a.Nil \,|\, \overline{a}.Nil) \smallsetminus \{a, b\} \stackrel{?}{\sim} \tau.Nil$
- $a.(\tau.Nil + b.B) \stackrel{?}{\sim} a.Nil + a.b.B$

The same processes but weak bisimilarity instead of the strong one.

- $a.\tau.Nil \stackrel{?}{\approx} \tau.a.Nil$
- $\tau.a.A + b.B \stackrel{?}{\approx} \tau.(a.A + b.B)$
- $\tau.Nil + (a.Nil \,|\, \overline{a}.Nil) \smallsetminus \{a, b\} \stackrel{?}{\approx} \tau.Nil$
- $a.(\tau.Nil + b.B) \stackrel{?}{\approx} a.Nil + a.b.B$

Hint: draw first the LTS generated by the CCS processes.
Home exercise: try to verify your claims by using the tool CWB.

Exercise 1.14 *Prove that for any CCS process P the following law (called idempotency) holds.*

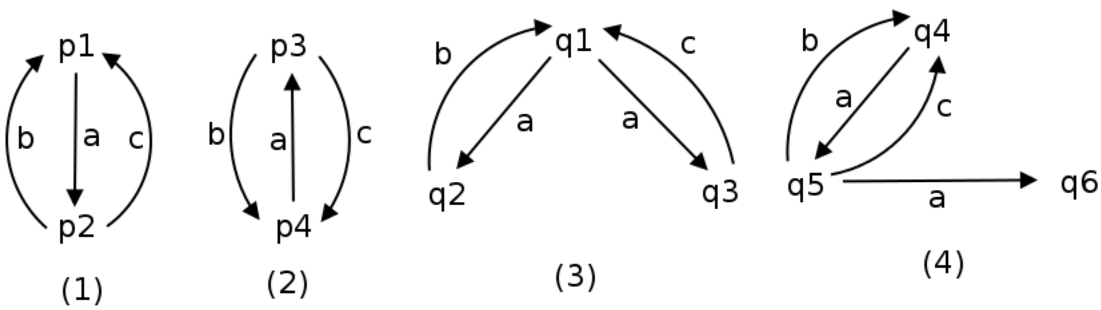
- $P + P \sim P$

By using the fact that $\sim \subseteq \approx$ conclude that also $P + P \approx P$.

Exercise 1.15 *Consider the tiny communication protocol from Lecture 4.*

- *Draw the labelled transition system generated by the processes $Spec$ and $Impl$.*
- *Prove (by hand) that $Spec \approx Impl$. Hint: define a weak bisimulation relation containing $(Spec, Impl)$.*

Exercise 1.16 *Consider the following LTSs:*



Consider also the following HML formulas:

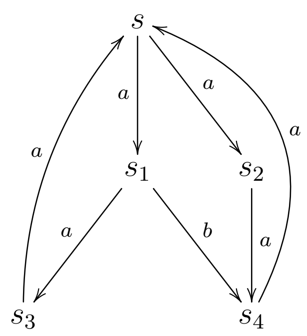
$\phi \stackrel{def}{=} [a](< b > \mathrm{tt} \wedge \ < c > \mathrm{tt})$

$\psi \stackrel{def}{=} [a](< b > \mathrm{tt} \vee \ < c > \mathrm{tt})$

$\varphi \stackrel{def}{=} < a > [b]\mathrm{ff}$

1. *Calculate $[|\phi|]$, $[|\psi|]$ and $[|\varphi|]$ in the LTSs (1), (2), (3) and (4).*
2. *Determine if $p1 \models \phi$, $p1 \models \psi$, $p1 \models \varphi$, $q4 \models \phi$, $q4 \models \psi$, $q4 \models \varphi$.*

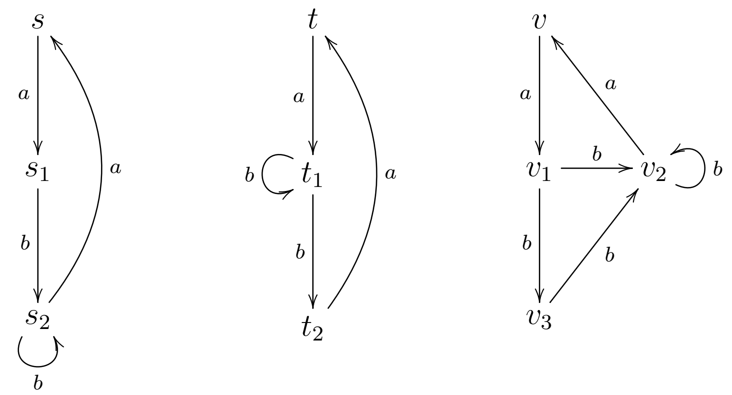
Exercise 1.17 *Consider the following labelled transition system.*



1. *Decide whether the state* s *satisfies the following formulae of Hennessy-Milner logic:*
   - $s \stackrel{?}{\models} \langle a \rangle tt$
   - $s \stackrel{?}{\models} \langle b \rangle tt$
   - $s \stackrel{?}{\models} [a] ff$
   - $s \stackrel{?}{\models} [b] ff$
   - $s \stackrel{?}{\models} [a]\langle b \rangle tt$
   - $s \stackrel{?}{\models} \langle a \rangle\langle b \rangle tt$
   - $s \stackrel{?}{\models} [a]\langle a \rangle[a][b] ff$
   - $s \stackrel{?}{\models} \langle a \rangle\big(\langle a \rangle tt \wedge \langle b \rangle tt\big)$
   - $s \stackrel{?}{\models} [a]\big(\langle a \rangle tt \vee \langle b \rangle tt\big)$
   - $s \stackrel{?}{\models} \langle a \rangle\big([b][a] ff \wedge \langle b \rangle tt\big)$
   - $s \stackrel{?}{\models} \langle a \rangle\big([a](\langle a \rangle tt \wedge [b] ff) \wedge \langle b \rangle ff\big)$

2. *Compute the following sets according to the denotational semantics for Hennessy-Milner logic.*
   - $[\![[a][b] ff]\!] = ?$
   - $[\![\langle a \rangle\big(\langle a \rangle tt \wedge \langle b \rangle tt\big)]\!] = ?$
   - $[\![[a][a][b] ff]\!] = ?$
   - $[\![[a]\big(\langle a \rangle tt \vee \langle b \rangle tt\big)]\!] = ?$

Exercise 1.18 *Consider the following labelled transition system.*



It it true that $s \not\sim t$, $s \not\sim v$ *and* $t \not\sim v$. *Find a distinguishing formula of Hennessy-Milner logic for the pairs*

- s *and* t
- s *and* v
- t *and* v.

Exercise 1.19 *For each of the following CCS expressions decide whether they are strongly bisimilar and if no, find a distinguishing formula in Hennessy-Milner logic.*

- $b.a.Nil + b.Nil$ *and* $b.(a.Nil + b.Nil)$
- $a.(b.c.Nil + b.d.Nil)$ *and* $a.b.c.Nil + a.b.d.Nil$
- $a.Nil \mid b.Nil$ *and* $a.b.Nil + b.a.Nil$
- $(a.Nil \mid b.Nil) + c.a.Nil$ *and* $a.Nil \mid (b.Nil + c.Nil)$

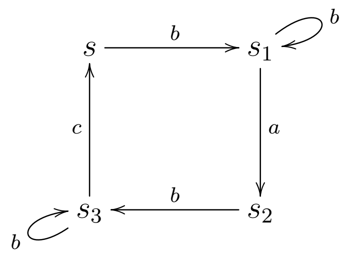
Home exercise: verify your claims in CWB (use the `strongeq` *and* `checkprop` *commands) and check whether you found the shortest distinguishing formula (use the* `dfstrong` *command).*

Exercise 1.20 *Prove that for every Hennessy-Milner formula* F *and every state* $p \in Proc$:

$$p \models F \quad \text{if and only if} \quad p \in [\![F]\!].$$

Hint: use structural induction on the structure of the formula F.

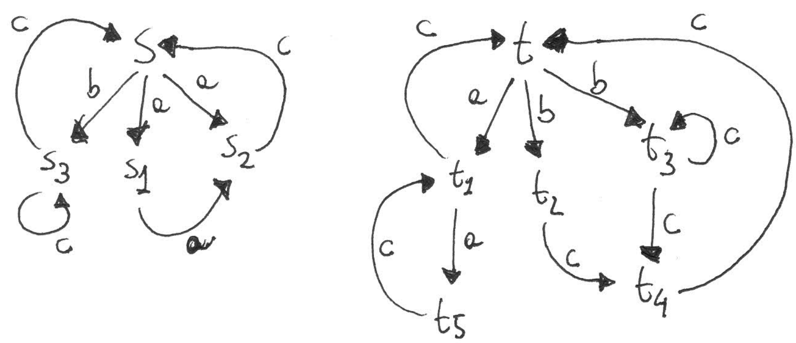
Exercise 1.21 *Consider the following labelled transition system.*



Using the game characterization for recursive Hennessy-Milner formulae decide whether the following claims are true or false and discuss what properties the formulae describe:

- $s \stackrel{?}{\models} X$ *where* $X \stackrel{\min}{=} \langle c \rangle tt \vee \langle Act \rangle X$
- $s \stackrel{?}{\models} X$ *where* $X \stackrel{\min}{=} \langle c \rangle tt \vee [Act] X$
- $s \stackrel{?}{\models} X$ *where* $X \stackrel{\max}{=} \langle b \rangle X$
- $s \stackrel{?}{\models} X$ *where* $X \stackrel{\max}{=} \langle b \rangle tt \wedge [a] X \wedge [b] X$

Exercise 1.22 *Consider the following LTS:*



1. **(2 points)** *Tell whether or not s is strongly bisimilar to t. Justify your answer formally.*
2. **(2 points)** *Tell whether or not t satisfies the formula $\langle b \rangle [c] \langle c \rangle \langle a \rangle tt$. Justify your answer formally.*
3. **(3 points)** *Determine all the states of the LTS that satisfy the following formulas:*
   - $\langle a \rangle [a][c] ff$
   - $[c] ff \wedge [c] tt$

Solutions

Solution of Exercise 1.1

We show that $s_1 \not\sim t_1$ using the game characterization of bisimilarity. In particular we show that the Attacker has the universal winning strategy that follows:

1. The configuration of the game is (s_1, t_1). The Attacker selects s_1 and makes the move: $s_1 \xrightarrow{a} s_4$. The Defender can only reply making the move $t_1 \xrightarrow{a} t_2$.

2. The configuration of the game is (s_4, t_2). The Attacker selects t_2 and makes the move: $t_2 \xrightarrow{b} t_1$. The Defender is stuck: there exists no state s such that $s_4 \xrightarrow{b} s$.

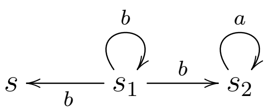
We calculate the semantics of the three formulas in the given LTS.
$[\![[a]\langle b\rangle tt \wedge [a]\langle c\rangle tt]\!] =$
$[\![[a]\langle b\rangle tt]\!] \cap [\![[a]\langle c\rangle tt]\!] =$
$[\cdot a\cdot]([\![\langle b\rangle tt]\!]) \cap [\cdot a\cdot]([\![\langle c\rangle tt]\!]) =$
$[\cdot a\cdot](\{s_2, s_3, t_2\}) \cap [\cdot a\cdot](\{s_2, s_4, t_2, t_3\}) =$
$\{s_2, s_3, s_4, s_5, s_6, t_1, t_2, t_3, t_4\} \cap \{s_2, s_3, s_4, s_5, s_6, t_1, t_2, t_3, t_4\} =$
$\{s_2, s_3, s_4, s_5, s_6, t_1, t_2, t_3, t_4\}$

$[\![\langle a\rangle\langle b\rangle tt \vee \langle c\rangle\langle b\rangle[c] ff]\!] =$
$[\![\langle a\rangle\langle b\rangle tt]\!] \cup [\![\langle c\rangle\langle b\rangle[c] ff]\!] =$
$\langle\cdot a\cdot\rangle([\![\langle b\rangle tt]\!]) \cup \langle\cdot c\cdot\rangle([\![\langle b\rangle[c] ff]\!]) =$
$\langle\cdot a\cdot\rangle(\{s_2, s_3, t_2\}) \cup \langle\cdot c\cdot\rangle(\langle\cdot b\cdot\rangle([\![[c] ff]\!])) =$
$\{s_1, t_1\} \cup \langle\cdot c\cdot\rangle(\langle\cdot b\cdot\rangle(\{s_1, s_3, s_5, s_6, t_1, t_4\}) =$
$\{s_1, t_1\} \cup \langle\cdot c\cdot\rangle(\{s_2, t_2\}) =$
$\{s_1, t_1\} \cup \{\} =$
$\{s_1, t_1\}$

$[\![[a][b]\langle c\rangle tt]\!] =$
$[\cdot a\cdot]([\![[b]\langle c\rangle tt]\!]) =$
$[\cdot a\cdot]([\cdot b\cdot]([\![\langle c\rangle tt]\!])) =$
$[\cdot a\cdot]([\cdot b\cdot](\{s_2, s_4, t_2, t_3\})) =$
$[\cdot a\cdot](\{s_1, s_3, s_4, s_5, s_6, t_1, t_3, t_4\}) =$
$\{s_2, s_3, s_4, s_5, s_6, t_2, t_3, t_4\}$

Solution of Exercise 1.2

Consider the following labelled transition system.

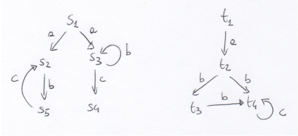


Compute for which sets of states $[\![X]\!] \subseteq \{s, s_1, s_2\}$ the following formulae are true.

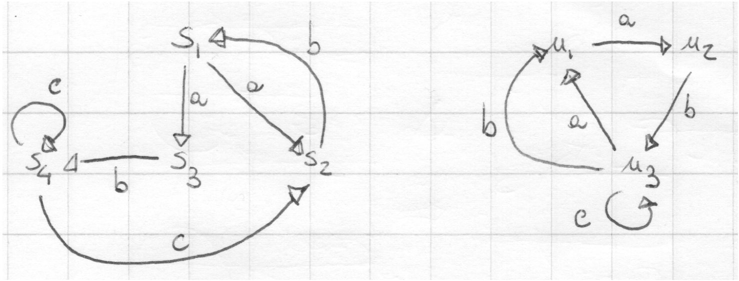
- $X = \langle a\rangle tt \vee [b]X$
  - The equation holds for the following sets of states: $\{s_2, s\}, \{s_2, s_1, s\}$.
- $X = \langle a\rangle tt \vee ([b]X \wedge \langle b\rangle tt)$

– The equation holds only for the set $\{s_2\}$.

Solution of Exercise 1.3



Solution of Exercise 1.4



Solution of Exercise 1.5

If we can show that $R = \{(s,t),(s_1,t_1),(s_3,t_2),(s_4,t_2),(s_2,t_3),(s_4,t_4)\}$ is a strong bisimulation, then $s \sim t$. Indeed R is a strong bisimulation since:

- Consider $(s,t) \in R$. Transitions from s:
  - If $s \xrightarrow{a} s_1$, match by doing $t \xrightarrow{a} t_1$, and $(s_1,t_1) \in R$.
  - If $s \xrightarrow{a} s_2$, match by doing $t \xrightarrow{a} t_3$, and $(s_2,t_3) \in R$.
  - These are all transitions from s.

  Transitions from t:
  - If $t \xrightarrow{a} t_1$, match by doing $s \xrightarrow{a} s_1$, and $(s_1,t_1) \in R$.
  - If $t \xrightarrow{a} t_3$, match by doing $s \xrightarrow{a} s_2$, and $(s_2,t_3) \in R$.
  - These are all transitions from t.
- Consider $(s_1,t_1) \in R$. Transitions from s_1:
  - If $s_1 \xrightarrow{a} s_3$, match by doing $t_1 \xrightarrow{a} t_2$ and $(s_3,t_2) \in R$.
  - If $s_1 \xrightarrow{b} s_4$, match by doing $t_1 \xrightarrow{b} t_2$ and $(s_4,t_2) \in R$.

  Transitions from t_1:
  - If $t_1 \xrightarrow{a} t_2$, match by doing $s_1 \xrightarrow{a} s_3$ and $(s_3,t_2) \in R$.
  - If $t_1 \xrightarrow{b} t_2$, match by doing $s_1 \xrightarrow{b} s_4$ and $(s_4,t_2) \in R$.
- Consider $(s_3,t_2) \in R$. Transitions from s_3:
  - If $s_3 \xrightarrow{a} s$, match by doing $t_2 \xrightarrow{a} t$ and $(s,t) \in R$.

  Transitions from t_2:
  - If $t_2 \xrightarrow{a} t$, match by doing $s_3 \xrightarrow{a} s$ and $(s,t) \in R$.
- Consider $(s_4,t_2) \in R$. Transitions from s_4:
  - If $s_4 \xrightarrow{a} s$, match by doing $t_2 \xrightarrow{a} t$ and $(s,t) \in R$.

  Transitions from t_2:
  - If $t_2 \xrightarrow{a} t$, match by doing $s_4 \xrightarrow{a} s$ and $(s,t) \in R$.
- Consider $(s_2,t_3) \in R$. Transitions from s_2:
  - If $s_2 \xrightarrow{a} s_4$, match by doing $t_3 \xrightarrow{a} t_4$ and $(s_4,t_4) \in R$.

  Transitions from t_3:
  - If $t_3 \xrightarrow{a} t_4$, match by doing $s_2 \xrightarrow{a} s_4$ and $(s_4,t_4) \in R$.
- Consider $(s_4,t_4) \in R$. Transitions from s_4:
  - If $s_4 \xrightarrow{a} s$, match by $t_4 \xrightarrow{a} t$ and $(s,t) \in R$.

  Transitions from t_4:
  - If $t_4 \xrightarrow{a} t$, match by $s_4 \xrightarrow{a} s$ and $(s,t) \in R$.

Solution of Exercise 1.6

Let $R = \{(P,Q),(P_1,Q_1),(P,Q_2),(P_1,Q_3)\}$. We only outline the proof; it follows along the lines as the proof in Exercise **??**. You should complete the details.

- From $(P,Q) \in R$ either P or Q can do an a transition.
  - In either case the response is to match by making an a transition from the remaining state, so we end up in $(P_1,Q_1) \in R$.
- From $(P_1,Q_1) \in R$ we end up in either $(P,Q) \in R$ or $(P,Q_2) \in R$.
- From $(P,Q_2) \in R$ we can only end up in $(P_1,Q_3) \in R$.
- From $(P_1,Q_3) \in R$ we end up in either $(P,Q) \in R$ or $(P,Q_2) \in R$.

Solution of Exercise 1.7

In this exercise you are asked to train yourself in the use of the game characterization for strong bisimulation. We therefore give universal winning strategy for the attacker or the defender in order to prove strong nonbisimilarity or bisimilarity. Let A denote the attacker and D the defender.

- Claim: $s \not\sim t$. The universal winning strategy for A is as follows.
  - In configuration (s,t), A chooses s and makes the move $s \xrightarrow{a} s_1$.
    - D's only possible response is to choose t and make the move $t \xrightarrow{a} t_1$. The current configuration is now (s_1,t_1)
  - In configuration (s_1,t_1), A chooses s_1 and makes the move $s_1 \xrightarrow{b} s_2$.

  Now the winning strategy depends on D's next move and is as follows. D can only choose the state t_1, but has two possible moves. Suppose D chooses $t_1 \xrightarrow{b} t_1$. Then the current configuration becomes (s_2,t_1). Now A choose s_2 and makes the move $s_2 \xrightarrow{a} s$. Then D looses since there are no a-transitions from t_1. If D uses the other possible move, namely $t_1 \xrightarrow{b} t_2$, the current configuration becomes (s_2,t_2). But then A chooses s_2 and makes the move $s_2 \xrightarrow{b} s_2$. Again D looses since there are no b-transitions from t_2.

  Remark: there is another winning strategy for the attacker which is easier to describe; try to find it.

- Claim: $s \sim u$: The universal winning strategy for D is as follows.
  - Starting in (s,u), A has two possible moves. Either (a) $s \xrightarrow{a} s_1$ or (b) $u \xrightarrow{a} u_1$.
    - If A chooses (a), then D takes the move $u \xrightarrow{a} u_1$, and the current configuration becomes (s_1,u_1).
    - If A chooses (b), then D takes the move $s \xrightarrow{a} s_1$, and the current configuration again becomes (s_1,u_1).
  - In configuration (s_1,u_1), A can choose either (a) $s_1 \xrightarrow{b} s_2$, or (b) $u_1 \xrightarrow{b} u_3$.
    - If A chooses (a), then D takes the move $u_1 \xrightarrow{b} u_3$, and the current configuration becomes (s_2,u_3).
    - If A chooses (b), then D takes the move $s_1 \xrightarrow{b} s_2$, and the current configuration again becomes (s_2,u_3).

- In configuration (s_2, u_3), A can choose either (a) $s_2 \xrightarrow{b} s_2$ or (b) $s_2 \xrightarrow{a} s$ or (c) $u_3 \xrightarrow{a} u$ or (d) $u_3 \xrightarrow{b} u_2$.
  * If A chooses (a), then D takes the move $u_3 \xrightarrow{b} u_2$ and the current configuration becomes (s_2, u_2).
  * If A chooses (b), then D takes the move $u_3 \xrightarrow{a} u$ and the current configuration becomes (s, u) which is exactly the start configuration.
  * If A chooses (c), then D takes the move $s_2 \xrightarrow{a} s$ and the current configuration becomes (s, u) which is the start configuration.
  * If A chooses (d), then D takes the move $s_2 \xrightarrow{b} s_2$ and the current configuration becomes (s_2, u_2) as when the attacker played (a). Hence from now we only need to consider games form the state (s_2, u_2).

  Now we can argue that D has a winning strategy. From (s_2, u_2), D's response to any move from A will be to take the same transition. This means that the next configuration is either (s_2, u_2) or (s, u). The game will be infinite, and hence D is the winner.

- Claim: $s \not\sim v$: The universal winning strategy for A is as follows.
  - In configuration (s, v), A makes the move $s \xrightarrow{a} s_1$.
    * Now D must make the move $v \xrightarrow{a} v_1$ and the current configuration becomes (s_1, v_1).
  - In configuration (s_1, v_1), A chooses $v_1 \xrightarrow{b} v_2$.
    * D must make the move $s_1 \xrightarrow{b} s_2$. The current configuration is (s_2, v_2).

  Now A wins since from (s_2, v_2) as he can choose to make the move $s_2 \xrightarrow{b} s_2$. Since there are no b-transitions from v_2, D looses.

Solution of Exercise 1.8

The general idea in this exercise is that in order to prove that $P \sim Q$ you define some binary relation R such that $(P, Q) \in R$, and then proceed to prove that R is indeed a strong bisimulation.

- Define $R = \{(P|Nil, P) \quad | \quad \text{P is a CCS process}\}$. We show that R is a strong bisimulation.
  - Suppose for some $\alpha \in Act$ that $P|Nil \xrightarrow{\alpha} P'|Nil$. We now have to find some process $\tilde{P}$ such that $P \xrightarrow{\alpha} \tilde{P}$ and $(P'|Nil, \tilde{P}) \in R$. Now use the transition relation. The only rule that could have been used is the COM1-rule.

  $$\frac{P \xrightarrow{\alpha} P'}{P|Nil \xrightarrow{\alpha} P'|Nil}.$$

  Now set $\tilde{P} = P'$. Then we are finished since we now know that $P \xrightarrow{\alpha} P'$ and by the definition of R, $(P'|Nil, \tilde{P}) = (P'|Nil, P') \in R$.
  - Symmetrically we must prove that when $P \xrightarrow{\alpha} P'$, then some $\tilde{P}$ exists so that $P|Nil \xrightarrow{\alpha} \tilde{P}$ and $(\tilde{P}, P') \in R$. But this is easy. By using the COM1-rule we have

  $$\frac{P \xrightarrow{\alpha} P'}{P|Nil \xrightarrow{\alpha} P'|Nil}.$$

  So we simply let $\tilde{P} = P'|Nil$. And again by definition of R, we have that $(\tilde{P}, P') = (P'|Nil, P') \in R$. This proves that R, is a bisimulation. And since $(P|Nil, P) \in R$, this means that $P|Nil \sim P$.

- This time we show that $P + Nil \sim P$ by giving a universal winning strategy for the defender. Remember that the game is played on the LTS, so we will just denote the states of the LTS by the CCS-expression. If the attacker chooses $P+Nil$, then the only possible moves are those of P since Nil has no transitions. So if $P \xrightarrow{a} P'$, the attacker can make the move $P + Nil \xrightarrow{a} P'$. But then the defender can make the move $P \xrightarrow{a} P'$. The current configuration is now (P', P'). From now on the defenders strategy is do to the same as the attacker. Either the game is infinite, in which case the defender wins. Or the game is finite. But then the defender wins, since the attacker cannot make any move because both processes are stuck. Similarly if the attacker plays $P \xrightarrow{a} P'$. Then the defender moves $P + Nil \xrightarrow{a} P'$, and the configuration again becomes (P', P').

- We show now that $R = \{(P|Q, Q|P) \quad | \quad P, QareCCS - expressions\}$ is a strong bisimulation. We only give an outline of the proof, the method is the same as in the first bullet. Suppose $P|Q \xrightarrow{a} P'|Q'$.

  – If COM3-rule was applied, we can argue as follows:

  $$\frac{P \xrightarrow{a} P' \qquad Q \xrightarrow{\overline{a}} Q'}{P|Q \xrightarrow{\tau} P'|Q'}$$

  But then since $\overline{\overline{a}} = a$ we can use the same rule to derive:

  $$\frac{Q \xrightarrow{\overline{a}} Q' \qquad P \xrightarrow{a} P'}{Q|P \xrightarrow{\tau} Q'|P'}.$$

  And by the definition of R, we know that $(P'|Q', Q'|P') \in R$.

  – If COM1 or COM2 rule was used, we do the following analysis. Suppose the COM1-rule was the one used. Then we know that

  $$\frac{P \xrightarrow{a} P'}{P|Q \xrightarrow{a} P'|Q}.$$

  Again one can now apply the COM2-rule and derive

  $$\frac{P \xrightarrow{a} P'}{Q|P \xrightarrow{a} Q|P'},$$

  and $(P'|Q, Q|P') \in R$. In order to finish the proof we need to argue for the symmmetric case (i.e. when the rule COM2 was used from $P|Q$). The argument for this case is similar as before.

  The case when $Q|P \xrightarrow{a} Q'|P'$ is completely symmetric.

Solution of Exercise 1.9

Assume that $s \sim t$. We will show both trace inclusions as follows.

- $\mathit{Traces}(s) \subseteq \mathit{Traces}(t)$: Let $w = a_1 a_2 \ldots a_n$ be a trace from $\mathit{Traces}(s)$. The attacker will play the sequence w in n-rounds of the strong bisimulation game, always from the left processes s. As $s \sim t$, the defender has to be able to answer to such an attack and hence he has to be able to do the same sequence w from the right process t. This means that $w \in \mathit{Traces}(t)$.

- $\mathit{Traces}(t) \subseteq \mathit{Traces}(s)$: The argument is completely symmetric, the attacker plays the whole sequence from the right process t and the defender has to be able to match it in the left process.

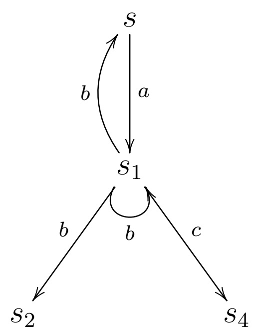
This implies that $Traces(s) = Traces(t)$.

Solution of Exercise 1.10

The answer is no for all the cases and the relation R of strong bisimulation from Exercise **??** can serve as a counter example for reflexivity and symmetry.

Solution of Exercise 1.11

One possible solution is as follows.



Solution of Exercise 1.12

Let $K \stackrel{\text{def}}{=} P$. We define

$$R = \{(K, P)\} \cup \{(P', P') \mid \text{P' is a CCS process}\}.$$

We will argue that R is a strong bisimulation. We analyze only the pair (K, P) from R as any pair of the form (P', P') can be safely added to R (why?).

Let $K \stackrel{a}{\longrightarrow} P'$. We must find $\tilde{P}$ such that $P \stackrel{a}{\longrightarrow} \tilde{P}$ and $(P', \tilde{P}) \in R$. The transition $K \stackrel{a}{\longrightarrow} P'$ must have been derived using the CON-rule with the premise $P \stackrel{a}{\longrightarrow} P'$. Then we can just let $\tilde{P} = P'$ as we know that $P \stackrel{a}{\longrightarrow} P'$, and $(P', P') \in R$.

Let $P \stackrel{a}{\longrightarrow} P'$. Then using the SOS rule CON we know that also $K \stackrel{a}{\longrightarrow} P'$ and again $(P', P') \in R$.

Solution of Exercise 1.13

Decide whether the following claims are true or false. Support your claims either by using bisimulation games or directly the definition of strong/weak bisimilarity.

- $a.\tau.Nil \not\sim \tau.a.Nil$
  - The attacker plays the action a in the left process and the defender does not have any a-move available in the right process and looses.
- $\tau.a.A + b.B \not\sim \tau.(a.A + b.B)$
  - The attacker plays the action b from the left process, there is no action b available in the right process in the first round. The attacker clearly wins.
- $\tau.Nil + (a.Nil \,|\, \overline{a}.Nil) \smallsetminus \{a, b\} \sim \tau.Nil$

- $R = \{(\tau.Nil + (a.Nil \,|\, \overline{a}.Nil) \smallsetminus \{a,b\}, \tau.Nil), (Nil, Nil), ((Nil \,|\, Nil) \smallsetminus \{a,b\}, Nil)\}$ is a strong bisimulation.

- $a.(\tau.Nil + b.B) \not\sim a.Nil + a.b.B$
  - In the first round the attacker plays from the left the action a and in the second round he plays again from left the action τ. The defender looses as he can never play the same sequence of a followed by τ from the right process.

The same processes but weak bisimilarity instead of the strong one.

- $a.\tau.Nil \approx \tau.a.Nil$
  - $R = \{(a.\tau.Nil, \tau.a.Nil), (\tau.Nil, Nil), (Nil, Nil), (a.\tau.Nil, a.Nil)\}$ is a weak bisimulation.
- $\tau.a.A + b.B \not\approx \tau.(a.A + b.B)$
  - The attacker plays the action τ from the left and reaches the process $a.A$. The defender can either answer by (i) doing nothing on the right and staying in the process $\tau.(a.A+b.B)$ or (ii) by playing the action τ and reaching $a.A + b.B$. In case (i) the attacker will play in second round on the right the action τ, the defender can only stay in $a.A$ and in the next round the attacker wins by making the b-move on the right. In case (ii) the attacker wins already in the second round by playing b from the right process.
- $\tau.Nil + (a.Nil \,|\, \overline{a}.Nil) \smallsetminus \{a,b\} \approx \tau.Nil$
  - These two processes are even strongly bisimilar so they must be also weakly bisimilar.
- $a.(\tau.Nil + b.B) \not\approx a.Nil + a.b.B$
  - The attacker plays $a.Nil + a.b.B \stackrel{a}{\longrightarrow} b.B$ on the right, the defender can answer either by $a.(\tau.Nil + b.B) \stackrel{a}{\Longrightarrow} \tau.Nil + b.B$ or by $a.(\tau.Nil + b.B) \stackrel{a}{\Longrightarrow} Nil$. In the first case the attacker plays $\tau.Nil + b.B \stackrel{\tau}{\longrightarrow} Nil$ and the defender can only do nothing and will loose in the next round. In the second case, the attacker plays the action b from the left and the defender looses.

Home exercise: try to verify your claims by using the tool CWB.

Solution of Exercise 1.14

We now argue that $P + P \sim P$ using the game characterization. We start from the configuration $(P+P, P)$. Suppose the attacker chooses $P + P \stackrel{a}{\longrightarrow} P'$. Then we know (from the SOS transition rules) that this transition can only have been derived if $P \stackrel{a}{\longrightarrow} P'$. So, of course, the defender replies by doing $P \stackrel{a}{\longrightarrow} P'$. The current configuration becomes (P', P') from which the defender always has a winning strategy by simply doing exactly the same as the attacker. Conversely, if the attacker from $(P + P, P)$ chooses $P \stackrel{a}{\longrightarrow} P'$ then the defender responds by playing $P + P \stackrel{a}{\longrightarrow} P'$ and the current configuration becomes again (P', P').

Solution of Exercise 1.15

$$\begin{aligned}
\mathsf{Send} &\stackrel{\text{def}}{=} \mathsf{acc.Sending} \\
\mathsf{Sending} &\stackrel{\text{def}}{=} \overline{\mathsf{send}}.\mathsf{Wait} \\
\mathsf{Wait} &\stackrel{\text{def}}{=} \mathsf{ack.Send} + \mathsf{error.Sending}
\end{aligned}
\qquad
\begin{aligned}
\mathsf{Rec} &\stackrel{\text{def}}{=} \mathsf{trans.Del} \\
\mathsf{Del} &\stackrel{\text{def}}{=} \overline{\mathsf{del}}.\mathsf{Ack} \\
\mathsf{Ack} &\stackrel{\text{def}}{=} \overline{\mathsf{ack}}.\mathsf{Rec}
\end{aligned}$$

$$\begin{aligned}
\mathsf{Med} &\stackrel{\text{def}}{=} \mathsf{send.Med}' \\
\mathsf{Med}' &\stackrel{\text{def}}{=} \tau.\mathsf{Err} + \overline{\mathsf{trans}}.\mathsf{Med} \\
\mathsf{Err} &\stackrel{\text{def}}{=} \overline{\mathsf{error}}.\mathsf{Med}
\end{aligned}$$

$$\mathsf{Impl} \stackrel{\text{def}}{=} (\mathsf{Send} \mid \mathsf{Med} \mid \mathsf{Rec}) \smallsetminus \{\mathsf{send}, \mathsf{trans}, \mathsf{ack}, \mathsf{error}\}$$

$$\mathsf{Spec} \stackrel{\text{def}}{=} \mathsf{acc}.\overline{\mathsf{del}}.\mathsf{Spec}$$

Solution of Exercise 1.16

First question

First LTS

In according to the definition of LTS (Label Transition System), in this case we have:

$$\begin{aligned}
Proc &= \{p_1, p_2\} \\
Act &= \{a, b, c\} \\
\xrightarrow{a} &= \{(p_1, p_2)\} \\
\xrightarrow{b} &= \{(p_2, p_1)\} \\
\xrightarrow{c} &= \{(p_2, p_1)\}
\end{aligned}$$

$$\begin{aligned}
\phi &= \llbracket [a](\langle b\rangle tt \wedge \langle c\rangle tt)]\!] = [\cdot a\cdot][\![\langle b\rangle tt \wedge \langle c\rangle tt]\!] \\
&= [\cdot a\cdot]([\![\langle b\rangle tt]\!] \cap [\![\langle c\rangle tt]\!]) \\
&= [\cdot a\cdot](\langle \cdot b\cdot\rangle Proc \cap \langle \cdot c\cdot\rangle Proc) \\
&= [\cdot a\cdot](\{p_2\} \cap \{p_2\}) \\
&= [\cdot a\cdot](\{p_2\}) \\
&= \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \{p_2\}\} \\
&= \{p_1, p_2\} = Proc
\end{aligned}$$

$$\begin{aligned}
\psi &= \llbracket [a](\langle b\rangle tt \vee \langle c\rangle tt)]\!] = [\cdot a\cdot][\![\langle b\rangle tt \vee \langle c\rangle tt]\!] \\
&= [\cdot a\cdot]([\![\langle b\rangle tt]\!] \cup [\![\langle c\rangle tt]\!]) \\
&= [\cdot a\cdot](\langle \cdot b\cdot\rangle Proc \cup \langle \cdot c\cdot\rangle Proc) \\
&= [\cdot a\cdot](\{p_2\} \cup \{p_2\}) \\
&= [\cdot a\cdot](\{p_2\}) \\
&= \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \{p_2\}\} \\
&= \{p_1, p_2\} = Proc
\end{aligned}$$

$$\begin{aligned}
\varphi &= [\![\langle a\rangle [b] ff]\!] = \langle \cdot a\cdot\rangle [\![[b] ff]\!] = \langle \cdot a\cdot\rangle [\cdot b\cdot][\![ff]\!] \\
&= \langle \cdot a\cdot\rangle [\cdot b\cdot]\emptyset \\
&= \langle \cdot a\cdot\rangle \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \emptyset\} \\
&= \langle \cdot a\cdot\rangle (\{p_1\}) \\
&= \emptyset
\end{aligned}$$

Second LTS

In according to the definition of LTS (Label Transition System), in this case we have:

$$\begin{aligned} Proc &= \{p_3, p_4\} \\ Act &= \{a, b, c\} \\ \xrightarrow{a} &= \{(p_4, p_3)\} \\ \xrightarrow{b} &= \{(p_3, p_4)\} \\ \xrightarrow{c} &= \{(p_3, p_4)\} \end{aligned}$$

$$\begin{aligned} \phi &= [\![[a](\langle b\rangle tt \wedge \langle c\rangle tt)]\!] = [\cdot a\cdot][\![\langle b\rangle tt \wedge \langle c\rangle tt]\!] \\ &= [\cdot a\cdot]([\![\langle b\rangle tt]\!] \cap [\![\langle c\rangle tt]\!]) \\ &= [\cdot a\cdot](\langle\cdot b\cdot\rangle Proc \cap \langle\cdot c\cdot\rangle Proc) \\ &= [\cdot a\cdot](\{p_3\} \cap \{p_3\}) \\ &= [\cdot a\cdot](\{p_3\}) \\ &= \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \{p_3\}\} \\ &= \{p_3, p_4\} = Proc \end{aligned}$$

$$\begin{aligned} \psi &= [\![[a](\langle b\rangle tt \vee \langle c\rangle tt)]\!] = [\cdot a\cdot][\![\langle b\rangle tt \vee \langle c\rangle tt]\!] \\ &= [\cdot a\cdot]([\![\langle b\rangle tt]\!] \cup [\![\langle c\rangle tt]\!]) \\ &= [\cdot a\cdot](\langle\cdot b\cdot\rangle Proc \cup \langle\cdot c\cdot\rangle Proc) \\ &= [\cdot a\cdot](\{p_3\} \cup \{p_3\}) \\ &= [\cdot a\cdot](\{p_3\}) \\ &= \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \{p_3\}\} \\ &= \{p_3, p_4\} = Proc \end{aligned}$$

$$\begin{aligned} \varphi &= [\![\langle a\rangle [b] ff]\!] = \langle\cdot a\cdot\rangle [\![[b] ff]\!] = \langle\cdot a\cdot\rangle [\cdot b\cdot] [\![ff]\!] \\ &= \langle\cdot a\cdot\rangle [\cdot b\cdot] \emptyset \\ &= \langle\cdot a\cdot\rangle \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \emptyset\} \\ &= \langle\cdot a\cdot\rangle (\{p_4\}) \\ &= \emptyset \end{aligned}$$

Third LTS

In according to the definition of LTS (Label Transition System), in this case we have:

$$\begin{aligned} Proc &= \{q_1, q_2, q_3\} \\ Act &= \{a, b, c\} \\ \xrightarrow{a} &= \{(q_1, q_2), (q_1, q_3)\} \\ \xrightarrow{b} &= \{(q_2, q_1)\} \\ \xrightarrow{c} &= \{(q_3, q_1)\} \end{aligned}$$

$$
\begin{aligned}
\phi &= [\![[a](\langle b\rangle tt \wedge \langle c\rangle tt)]\!] = [\cdot a\cdot][\![\langle b\rangle tt \wedge \langle c\rangle tt]\!] \\
&= [\cdot a\cdot]([\![\langle b\rangle tt]\!] \cap [\![\langle c\rangle tt]\!]) \\
&= [\cdot a\cdot](\langle b\rangle Proc \cap \langle c\rangle Proc) \\
&= [\cdot a\cdot](\{q_2\} \cap \{q_3\}) \\
&= [\cdot a\cdot](\emptyset) \\
&= \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \emptyset\} \\
&= \{q_2, q_3\}
\end{aligned}
$$

$$
\begin{aligned}
\psi &= [\![[a](\langle b\rangle tt \vee \langle c\rangle tt)]\!] = [\cdot a\cdot][\![\langle b\rangle tt \vee \langle c\rangle tt]\!] \\
&= [\cdot a\cdot]([\![\langle b\rangle tt]\!] \cup [\![\langle c\rangle tt]\!]) \\
&= [\cdot a\cdot](\langle b\rangle Proc \cup \langle c\rangle Proc) \\
&= [\cdot a\cdot](\{q_2\} \cup \{q_3\}) \\
&= [\cdot a\cdot](\{q_2, q_3\}) \\
&= \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \{q_2, q_3\}\} \\
&= \{q_1, q_2, q_3\} = Proc
\end{aligned}
$$

$$
\begin{aligned}
\varphi &= [\![\langle a\rangle [b] \mathrm{ff}]\!] = \langle \cdot a\cdot\rangle [\![[b]\mathrm{ff}]\!] = \langle \cdot a\cdot\rangle [\cdot b\cdot][\![\mathrm{ff}]\!] \\
&= \langle \cdot a\cdot\rangle [\cdot b\cdot]\emptyset \\
&= \langle \cdot a\cdot\rangle \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \emptyset\} \\
&= \langle \cdot a\cdot\rangle (\{q_1, q_3\}) \\
&= \{q_1\}
\end{aligned}
$$

Fourth LTS

In according to the definition of LTS (Label Transition System), in this case we have:

$$
\begin{aligned}
Proc &= \{q_4, q_5, q_6\} \\
Act &= \{a, b, c\} \\
\xrightarrow{a} &= \{(q_4, q_5), (q_5, q_6)\} \\
\xrightarrow{b} &= \{(q_5, q_4)\} \\
\xrightarrow{c} &= \{(q_5, q_4)\}
\end{aligned}
$$

$$
\begin{aligned}
\phi &= [\![[a](\langle b\rangle tt \wedge \langle c\rangle tt)]\!] = [\cdot a\cdot][\![\langle b\rangle tt \wedge \langle c\rangle tt]\!] \\
&= [\cdot a\cdot]([\![\langle b\rangle tt]\!] \cap [\![\langle c\rangle tt]\!]) \\
&= [\cdot a\cdot](\langle b\rangle Proc \cap \langle c\rangle Proc) \\
&= [\cdot a\cdot](\{q_5\} \cap \{q_5\}) \\
&= [\cdot a\cdot](\{q_5\}) \\
&= \{P | \forall P', P \xrightarrow{a} P' \Rightarrow P' \in \{q_5\}\} \\
&= \{q_4, q_6\}
\end{aligned}
$$

$$
\begin{aligned}
\psi &= [\![[a](\langle b\rangle tt \vee \langle c\rangle tt)]\!] = [\cdot a\cdot][\![\langle b\rangle tt \vee \langle c\rangle tt]\!] \\
&= [\cdot a\cdot]([\![\langle b\rangle tt]\!] \cup [\![\langle c\rangle tt]\!]) \\
&= [\cdot a\cdot](\langle b\rangle Proc \cup \langle c\rangle Proc) \\
&= [\cdot a\cdot](\{q_5\} \cup \{q_5\}) \\
&= [\cdot a\cdot](\{q_5\}) \\
&= \{P|\forall P', P \xrightarrow{a} P' \Rightarrow P' \in \{q_5\}\} \\
&= \{q_4, q_6\}
\end{aligned}
$$

$$
\begin{aligned}
\varphi &= [\![\langle a\rangle [b]\mathrm{ff}]\!] = \langle\cdot a\cdot\rangle[\![[b]\mathrm{ff}]\!] = \langle\cdot a\cdot\rangle[\cdot b\cdot][\![\mathrm{ff}]\!] \\
&= \langle\cdot a\cdot\rangle[\cdot b\cdot]\emptyset \\
&= \langle\cdot a\cdot\rangle\{P|\forall P', P \xrightarrow{a} P' \Rightarrow P' \in \emptyset\} \\
&= \langle\cdot a\cdot\rangle(\{q_4, q_6\}) \\
&= \{q_5\}
\end{aligned}
$$

Second question

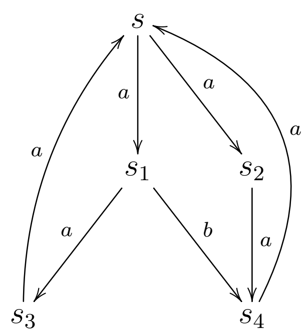
LTS	ϕ	ψ	φ
(1)	$\{p_1, p_2\}$	$\{p_1, p_2\}$	$\emptyset$
(2)	$\{p_3, p_4\}$	$\{p_3, p_4\}$	$\emptyset$
(3)	$\{q_2, q_3\}$	$\{q_1, q_2, q_3\}$	$\{q_1\}$
(4)	$\{q_4, q_6\}$	$\{q_4, q_6\}$	$\{q_5\}$

Based on the table above and with the last definition that we have given, we can answer the second question:.

- $p_1 \models \phi \Leftrightarrow p_1 \in [\![\phi]\!]$ becomes $p_1 \models \phi \Leftrightarrow p_1 \in \{p_1, p_2\}$ so the answer is: $\boldsymbol{p_1 \models \phi}$,
- $p_1 \models \psi \Leftrightarrow p_1 \in [\![\psi]\!]$ becomes $p_1 \models \psi \Leftrightarrow p_1 \in \{p_1, p_2\}$ so the answer is: $\boldsymbol{p_1 \models \psi}$,
- $p_1 \models \varphi \Leftrightarrow p_1 \in [\![\varphi]\!]$ becomes $p_1 \models \varphi \Leftrightarrow p_1 \in \emptyset$. As we can see, $p_1 \notin \emptyset$ so the answer is: $\boldsymbol{p_1 \not\models \varphi}$,
- $q_4 \models \phi \Leftrightarrow q_4 \in [\![\phi]\!]$ becomes $q_4 \models \phi \Leftrightarrow q_4 \in \{q_4, q_6\}$ so the answer is: $\boldsymbol{q_4 \models \phi}$,
- $q_4 \models \psi \Leftrightarrow q_4 \in [\![\psi]\!]$ becomes $q_4 \models \psi \Leftrightarrow q_4 \in \{q_4, q_6\}$ so the answer is: $\boldsymbol{q_4 \models \psi}$,
- $q_4 \models \varphi \Leftrightarrow q_4 \in [\![\varphi]\!]$ becomes $q_4 \models \varphi \Leftrightarrow q_4 \in \{q_5\}$. As we can see, $q_4 \notin q_5$ so the answer is: $\boldsymbol{q_4 \not\models \varphi}$.

Solution of Exercise 1.17

Consider the following labelled transition system.



1. Decide whether the state s satisfies the following formulae of Hennessy-Milner logic:
   - $s \models \langle a \rangle tt$
   - $s \not\models \langle b \rangle tt$
   - $s \not\models [a] ff$
   - $s \models [b] ff$
   - $s \not\models [a]\langle b \rangle tt$
   - $s \models \langle a \rangle\langle b \rangle tt$
   - $s \models [a]\langle a \rangle[a][b] ff$
   - $s \models \langle a \rangle\big(\langle a \rangle tt \wedge \langle b \rangle tt\big)$
   - $s \models [a]\big(\langle a \rangle tt \vee \langle b \rangle tt\big)$
   - $s \not\models \langle a \rangle\big([b][a] ff \wedge \langle b \rangle tt\big)$
   - $s \not\models \langle a \rangle\big([a](\langle a \rangle tt \wedge [b] ff) \wedge \langle b \rangle ff\big)$

2. Compute the following sets according to the denotational semantics for Hennessy-Milner logic.
   - $$\begin{aligned} [\![[a][b] ff]\!] &= [\cdot a \cdot][\![[b] ff]\!] \\ &= [\cdot a \cdot][\cdot b \cdot][\![ff]\!] \\ &= [\cdot a \cdot][\cdot b \cdot]\emptyset \\ &= [\cdot a \cdot]\{P \mid \forall P'.P \xrightarrow{b} P' \Rightarrow P' \in \emptyset\} \\ &= [\cdot a \cdot]\{s, s_3, s_2, s_4\} \\ &= \big\{P \mid \forall P'.P \xrightarrow{a} P' \Rightarrow P' \in \{s, s_3, s_2, s_4\}\big\} \\ &= \{s_1, s_2, s_3, s_4\} \end{aligned}$$
   - $$\begin{aligned} [\![\langle a \rangle\big(\langle a \rangle tt \wedge \langle b \rangle tt\big)]\!] &= \langle \cdot a \cdot \rangle [\![\langle a \rangle tt \wedge \langle b \rangle tt]\!] \\ &= \langle \cdot a \cdot \rangle\big([\![\langle a \rangle tt]\!] \cap [\![\langle b \rangle tt]\!]\big) \\ &= \langle \cdot a \cdot \rangle\big(\langle \cdot a \cdot \rangle Proc \cap \langle \cdot b \cdot \rangle Proc\big) \\ &= \langle \cdot a \cdot \rangle\big(\{s, s_1, s_2, s_3, s_4\} \cap \{s_1\}\big) \\ &= \langle \cdot a \cdot \rangle\{s_1\} \\ &= \{s\} \end{aligned}$$

- $$\begin{aligned}[\![[a][a][b]ff]\!] &= [\cdot a\cdot][\cdot a\cdot][\cdot b\cdot]\emptyset \\ &= [\cdot a\cdot][\cdot a\cdot]\{s, s_2, s_3, s_4\} \\ &= [\cdot a\cdot]\{s_1, s_2, s_3, s_4\} \\ &= \{s, s_1, s_2\}\end{aligned}$$

- $$\begin{aligned}[\![[a]\big(\langle a\rangle tt \vee \langle b\rangle tt\big)]\!] &= [\cdot a\cdot][\![\langle a\rangle tt \vee \langle b\rangle tt]\!] \\ &= [\cdot a\cdot]\big(\langle\cdot a\cdot\rangle Proc \cup \langle\cdot b\cdot\rangle Proc\big) \\ &= [\cdot a\cdot]\{s, s_1, s_2, s_3, s_4\} \\ &= \{s, s_1, s_2, s_3, s_4\}\end{aligned}$$

Solution of Exercise 1.18

Distingushing HML-formulae are as follows.

- Let $F_1 = \langle a\rangle[b]\langle b\rangle tt$. Then $s \models F_1$, but $t \not\models F_1$.
- Let $F_2 = \langle a\rangle[b]\langle a\rangle tt$. Then $s \models F_2$ but $v \not\models F_3$.
- Let $F_3 = \langle a\rangle\langle b\rangle\big(\langle a\rangle tt \wedge \langle b\rangle tt\big)$. Then $t \not\models F_3$ but $v \models F_3$.

Solution of Exercise 1.19

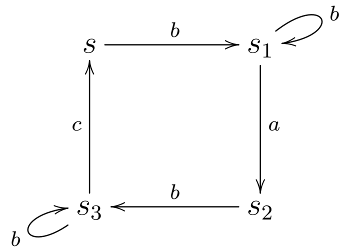
For each of the following CCS expressions decide whether they are strongly bisimilar and if not, find a distinguishing formula in Hennessy-Milner logic.

- $b.a.Nil + b.Nil$ and $b.(a.Nil + b.Nil)$
  - They are not bisimilar. Let $F_1 = [b]\langle b\rangle tt$. Then $b.a.Nil+b.Nil \not\models F_1$ but $b.(a.Nil+b.Nil) \models F_1$.
- $a.(b.c.Nil + b.d.Nil)$ and $a.b.c.Nil + a.b.d.Nil$
  - They are not bisimilar. Let $F_2 = [a]\big(\langle b\rangle\langle c\rangle tt \wedge \langle b\rangle\langle d\rangle tt\big)$. Then $a.(b.c.Nil + b.d.Nil) \models F_2$ but $a.b.c.Nil + a.b.d.Nil \not\models F_2$.
- $a.Nil \,|\, b.Nil$ and $a.b.Nil + b.a.Nil$
  - They are bisimilar.
- $(a.Nil \,|\, b.Nil) + c.a.Nil$ and $a.Nil \,|\, (b.Nil + c.Nil)$
  - They are not bisimilar. Let $F_3 = [a]\langle c\rangle tt$. Then $(a.Nil \,|\, b.Nil)+c.a.Nil \not\models F_3$ but $a.Nil \,|\, (b.Nil+c.Nil) \models F_3$.

Home exercise: verify your claims in CWB (use the `strongeq` and `checkprop` commands) and check whether you found the shortest distinguishing formula (use the `dfstrong` command).

Solution of Exercise 1.21

Consider the following labelled transition system.



Using the game characterization for recursive Hennessy-Milner formulae decide whether the following claims are true or false and discuss what properties the formulae describe:

- $s \models X$ where $X \stackrel{\min}{=} \langle c \rangle tt \vee \langle Act \rangle X$
  - A universal winning strategy for the defender starting from (s, X) is as follows:

$$\begin{aligned}(s, X) \quad &\to (s, \langle c \rangle tt \vee \langle Act \rangle X) \xrightarrow{D} (s, \langle Act \rangle X) \xrightarrow{D} (s_1, X) \\ &\to (s_1, \langle c \rangle tt \vee \langle Act \rangle X) \xrightarrow{D} (s_1, \langle Act \rangle X) \xrightarrow{D} (s_2, X) \\ &\to (s_2, \langle c \rangle tt \vee \langle Act \rangle X) \xrightarrow{D} (s_2, \langle Act \rangle X) \xrightarrow{D} (s_3, X) \\ &\to (s_3, \langle c \rangle tt \vee \langle Act \rangle X) \xrightarrow{D} (s_3, \langle c \rangle tt) \xrightarrow{D} (s, tt),\end{aligned}$$

    where (s, tt) by definition is a winning configuration for the defender.

- $s \not\models X$ where $X \stackrel{\min}{=} \langle c \rangle tt \vee [Act] X$
  - A universal winning strategy for the attacker is as follows: $(s, X) \to (s, \langle c \rangle tt \vee [Act] X)$ Then if the defender plays $\langle c \rangle tt$, he loses since there are no c-transitions from s, thus the defender must play $(s, \langle c \rangle tt \vee [Act] X) \xrightarrow{D} (s, [Act] X)$. Then the attacker plays $(s, [Act] X) \xrightarrow{A} (s_1, X)$. And we have $(s_1, X) \to (s_1, \langle c \rangle tt \vee [Act] X)$. Now for similar reasons as above the defender must choose to play $(s_1, \langle c \rangle tt \vee [Act] X) \xrightarrow{D} (s_1, [Act] X)$. The attacker plays $(s_1, [Act] X) \xrightarrow{A} (s_1, X)$ which is a configuration we have seen earlier. Thus either the play is infinite, in which case the attacker wins since X is defined as the least fixed-point. Or the play is finite, in which case the attacker also wins.

- $s \models X$ where $X \stackrel{\max}{=} \langle b \rangle X$
  - A universal winning strategy for the defender is:

$$(s, X) \to (s, \langle b \rangle X) \xrightarrow{D} (s_1, X) \to (s_1, \langle b \rangle X) \xrightarrow{D} (s_1, X).$$

    Thus the play is infinite, and since X is defined as the greatest fixed-point, the defender wins.

- $s \models X$ where $X \stackrel{\max}{=} \langle b \rangle tt \wedge [a] X \wedge [b] X$
  - Universal winning strategy for the defender: We have $(s, X) \to (s, \langle b \rangle tt \wedge [a] X \wedge [b] X)$. Now if the attacker plays $(s, \langle b \rangle tt \wedge [a] X \wedge [b] X) \xrightarrow{A} (s, \langle b \rangle tt)$ he loses since the defender can then play $(s, \langle b \rangle tt) \xrightarrow{D} (s_1, tt)$. Furthermore if the attacker plays $(s, \langle b \rangle tt \wedge [a] X \wedge [b] X) \xrightarrow{A} (s, [a] X)$, then he also loses since he is stuck in the configuration $(s, [a] X)$. The third option for the attacker is to choose $(s, \langle b \rangle tt \wedge [a] X \wedge [b] X) \xrightarrow{A} (s, [b] X) \xrightarrow{A} (s_1, X)$.
    Expanding X we get $(s_1, X) \to (s_1, \langle b \rangle tt \wedge [a] X \wedge [b] X)$. From here if the attacker plays $(s_1, \langle b \rangle tt \wedge [a] X \wedge [b] X) \xrightarrow{A} (s_1, \langle b \rangle tt)$ he loses since the defender can play $(s_1, \langle b \rangle tt) \xrightarrow{D} (s_1, tt)$.

If the attacker plays $(s_1, \langle b \rangle tt \wedge [a]X \wedge [b]X) \xrightarrow{A} (s_1, [b]X)$, then the only possible next move is $(s_1, [b]X) \xrightarrow{A} (s_1, X)$ which is a previously encountered configuration. The last option for the attacker is to play $(s_1, \langle b \rangle tt \wedge [a]X \wedge [b]X) \xrightarrow{A} (s_1, [a]X) \xrightarrow{A} (s_2, X)$.
Expanding the encoding we get $(s_2, X) \rightarrow (s_2, \langle b \rangle tt \wedge [a]X \wedge [b]X)$. Again if the attacker plays $(s_2, \langle b \rangle tt \wedge [a]X \wedge [b]X) \xrightarrow{A} (s_2, \langle b \rangle tt)$ he loses by the defenders move $(s_2, \langle b \rangle tt) \xrightarrow{D} (s_3, tt)$. If the attacker plays $(s_2, \langle b \rangle tt \wedge [a]X \wedge [b]X) \xrightarrow{A} (s_2, [a]X)$ he loses since he is stuck. Finally he can play $(s_2, \langle b \rangle tt \wedge [a]X \wedge [b]X) \xrightarrow{A} (s_2, [b]X) \xrightarrow{A} (s_3, X)$.
Expanding X we obtain $(s_3, X) \rightarrow (s_3, \langle b \rangle tt \wedge [a]X \wedge [b]X)$. Now playing $(s_3, \langle b \rangle tt \wedge [a]X \wedge [b]X) \xrightarrow{A} (s_3, \langle b \rangle tt)$ he loses by the defenders move $(s_3, \langle b \rangle tt) \xrightarrow{D} (s_3, tt)$. If the attacker plays $(s_3, \langle b \rangle tt \wedge [a]X \wedge [b]X) \xrightarrow{A} (s_3, [a]X)$ he is stuck. Finally the attacker can play $(s_3, \langle b \rangle tt \wedge [a]X \wedge [b]X) \xrightarrow{A} (s_3, [b]X) \xrightarrow{A} (s_3, X)$ which is a previously encountered configuration.
Thus either the attacker loses in a finite play, or the play is infinite in which case the defender wins since X is defined as the greatest fixed-point.

Solution of Exercise 1.22

MV 14/15 18/12/14 Appello ES 2

1) $s \not\sim t$ because in the game characterization of bisimilarity the attacker has a universal winning strategy, as follows:

(s,t) A: $s \xrightarrow{a} s_1$
D: $t \xrightarrow{a} t_1$

(s_1,t_1) A: $t_1 \xrightarrow{c} t$
D: $s_1 \not\xrightarrow{c}$

2) To decide if the formula is true or not in t let us check if $t \in [\![\langle b \rangle [c] \langle c \rangle \langle a \rangle tt]\!]$

$[\![\langle b \rangle [c] \langle c \rangle \langle a \rangle tt]\!] =$
$\langle \cdot b \cdot \rangle ([\cdot c \cdot] (\langle \cdot c \cdot \rangle (\langle \cdot a \cdot \rangle (Proc))))=$
$= \langle \cdot b \cdot \rangle ([\cdot c \cdot] (\langle \cdot c \cdot \rangle (\{ s, s_1, t, t_1 \}) =$
$= \langle \cdot b \cdot \rangle ([\cdot c \cdot] (\{ s_2, s_3, t_4, t_5, t_1 \})$
$= \langle \cdot b \cdot \rangle (\{ s, s_1, t, t_2, t_5 \})$
$= \{ t \}$

Since $t \in \{t\}$ then we derive that t satisfies the given formula.

3) $[\![\langle a \rangle [a][c] ff]\!] =$

$= \langle \cdot a \cdot \rangle ([\cdot a \cdot] ([\cdot c \cdot] (\emptyset))) =$

$= \langle \cdot a \cdot \rangle ([\cdot a \cdot] (\{ s, s_2, t \})) =$

$= \langle \cdot a \cdot \rangle (\{ s_2, s_3, t_2, t_3, t_4, t_5 \}) =$

$= \{ s, s_1, t_1 \}$

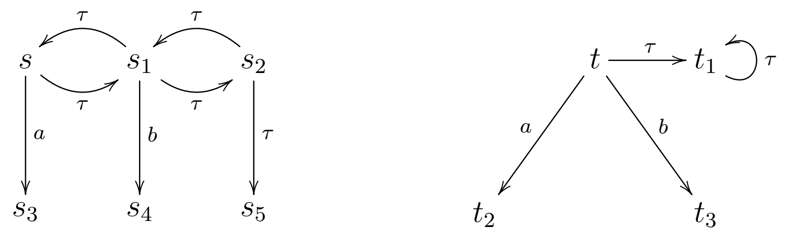
Note that $[c] ff \wedge [c] tt \equiv [c] ff \wedge tt \equiv [c] ff$

So let us calculate the semantics of $[c] ff$

$[\![[c] ff]\!] = [\cdot c \cdot](\emptyset) = \{ s, s_2, t \}$

2 Weak Bisimulation

Exercise 2.1 *Consider the following labelled transition system.*



Show that $s \approx t$ *by finding a weak bisimulation* R *containing the pair* (s, t)*.*

Exercise 2.2 *In the weak bisimulation game the attacker is allowed to use* $\stackrel{a}{\longrightarrow}$ *moves for the attacks and the defender can use* $\stackrel{a}{\Longrightarrow}$ *in response. Argue that if we modify the game rules so that the attacker can also use the long moves* $\stackrel{a}{\Longrightarrow}$ *then this does not provide any additional power for the attacker. Conclude that both versions of the game provide the same answer about bisimilarity/nonbisimilarity of two processes.*

Solutions

Solution of Exercise 2.1

Let $R = \{(s,t),(s_1,t),(s_2,t),(s_3,t_2),(s_4,t_3),(s_5,t_1)\}$. Now one can argue that R is a weak bisimulation as follows.

- Transitions from the pair (s,t): if $s \xrightarrow{a} s_3$ then $t \overset{a}{\Longrightarrow} t_2$ and $(s_3,t_2) \in R$. If $s \xrightarrow{\tau} s_1$ then $t \overset{\tau}{\Longrightarrow} t$ and $(s_1,t) \in R$. If $t \xrightarrow{a} t_2$ then $s \overset{a}{\Longrightarrow} s_3$ and $(s_3,t_2) \in R$. If $t \xrightarrow{b} t_3$ then $s \overset{b}{\Longrightarrow} s_4$ and $(s_4,t_3) \in R$. If $t \xrightarrow{\tau} t_1$ then $s \overset{\tau}{\Longrightarrow} s_5$ and $(s_5,t_1) \in R$.
- The transitions from the remaining pairs can be checked in a similar way.

Solution of Exercise 2.2

Observe that each long attack can be simulated (in more rounds) by doing in series all single steps that are contained in the long move, so the defender in fact has an answer even to the long move by combining the answers to the series

3 Complete Lattices and Fix Points

Exercise 3.1 *Draw a graphical representation of the complete lattice* $(2^{\{a,b,c\}}, \subseteq)$ *and compute supremum and infimum of the following sets:*

- $\sqcap\{\{a\}, \{b\}\} = ?$
- $\sqcup\{\{a\}, \{b\}\} = ?$
- $\sqcap\{\{a\}, \{a, b\}, \{a, c\}\} = ?$
- $\sqcup\{\{a\}, \{a, b\}, \{a, c\}\} = ?$
- $\sqcap\{\{a\}, \{b\}, \{c\}\} = ?$
- $\sqcup\{\{a\}, \{b\}, \{c\}\} = ?$
- $\sqcap\{\{a\}, \{a, b\}, \{b\}, \emptyset\} = ?$
- $\sqcup\{\{a\}, \{a, b\}, \{b\}, \emptyset\} = ?$

Exercise 3.2 *Prove that for any partially ordered set* $(D, \sqsubseteq)$ *and any* $X \subseteq D$*, if supremum of* X *(*$\sqcup X$*) and infimum of* X *(*$\sqcap X$*) exist then they are uniquely defined. (Hint: use the definition of supremum and infimum and antisymmetry of* $\sqsubseteq$*.)*

Exercise 3.3 *Let* $(D, \sqsubseteq)$ *be a complete lattice. What are* $\sqcup\emptyset$ *and* $\sqcap\emptyset$ *equal to?*

Exercise 3.4 *Consider the complete lattice* $(2^{\{a,b,c\}}, \subseteq)$*. Define a function* $f : 2^{\{a,b,c\}} \to 2^{\{a,b,c\}}$ *such that* f *is monotonic.*

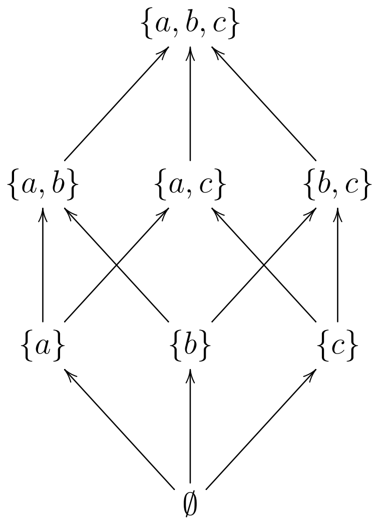
- *Compute the greatest fixed point by using directly the Tarski's fixed point theorem.*
- *Compute the least fixed point by using the Tarski's fixed point theorem for finite lattices (i.e. by starting from* $\perp$ *and by applying repeatedly the function* f *until the fixed point is reached).*

Solutions

Solution of Exercise 3.1

Draw a graphical representation of the complete lattice $(2^{\{a,b,c\}}, \subseteq)$ and compute supremum and infimum of the sets below.

The complete lattice:



- $\sqcap\{\{a\}, \{b\}\} = \emptyset$
- $\sqcup\{\{a\}, \{b\}\} = \{a, b\}$
- $\sqcap\{\{a\}, \{a, b\}, \{a, c\}\} = \{a\}$
- $\sqcup\{\{a\}, \{a, b\}, \{a, c\}\} = \{a, b, c\}$
- $\sqcap\{\{a\}, \{b\}, \{c\}\} = \emptyset$
- $\sqcup\{\{a\}, \{b\}, \{c\}\} = \{a, b, c\}$
- $\sqcap\{\{a\}, \{a, b\}, \{b\}, \emptyset\} = \emptyset$
- $\sqcup\{\{a\}, \{a, b\}, \{b\}, \emptyset\} = \{a, b\}$

Solution of Exercise 3.2

Prove that for any partially ordered set $(D, \sqsubseteq)$ and any $X \subseteq D$, if supremum of X ($\sqcup X$) and infimum of X ($\sqcap X$) exist then they are uniquely defined. (Hint: use the definition of supremum and infimum and antisymmetry of $\sqsubseteq$.)

We prove the claim for the supremum (least upper bound) of X. The arguments for the infimum are symmetric. Let $d_1, d_2 \in D$ be two supremums of a given set X. This means that $X \sqsubseteq d_1$ and $X \sqsubseteq d_2$ as both d_1 and d_2 are upper bounds of X. Now because d_1 is the least upper bound and d_2 is an upper bound we get $d_1 \sqsubseteq d_2$. Similarly, d_2 is the least upper bound and d_1 is an upper bound so $d_2 \sqsubseteq d_1$. However, from antisymmetry and $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1$ we get that $d_1 = d_2$.

S	$f(S)$
$\emptyset$	$\{a\}$
$\{a\}$	$\{a\}$
$\{b\}$	$\{a\}$
$\{c\}$	$\{a\}$
$\{a,b,c\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$
$\{a,c\}$	$\{a,b\}$
$\{b,c\}$	$\{a,b\}$

Table 1: Definition of a monotonic function f in Exercise **??**.

Solution of Exercise 3.3

Let $(D, \sqsubseteq)$ be a complete lattice. What are $\sqcup\emptyset$ and $\sqcap\emptyset$ equal to?

- $\sqcup\emptyset = \bot = \sqcap D$.
- $\sqcap\emptyset = \top = \sqcup D$.

Solution of Exercise 3.4

Consider the complete lattice $(2^{\{a,b,c\}}, \subseteq)$. Define a function $f : 2^{\{a,b,c\}} \to 2^{\{a,b,c\}}$ such that f is monotonic.

For example we define f as in Table 1 (note that there are many possibilites).

The function f is monotonic which we can verify by a case inspection.

- Compute the greatest fixed point by using directly the Tarski's fixed point theorem.
  - According to Tarski's fixed point theorem the largest fixed point z_{max} is given by $z_{max} = \sqcup A$, where
$$A = \{x \in 2^{\{a,b,c\}} \,|\, x \sqsubseteq f(x)\}.$$
    In our case, by the definition of f we get $A = \{\emptyset, \{a\}, \{a,b\}\}$. The supremum of A in $2^{\{a,b,c\}}$ is $\{a,b\}$ so by Tarski's fixed point theorem, the largest fixed point of f is $\{a,b\}$.
- Compute the least fixed point by using the Tarski's fixed point theorem for finite lattices (i.e. by starting from $\bot$ and by applying repeatedly the function f until the fixed point is reached).
  - First note that $\bot = \sqcap 2^{\{a,b,c\}} = \emptyset$. We now repeatedly apply f until it stabilizes
$$\begin{aligned} f(\emptyset) &= \{a\} \\ f(f(\emptyset)) = f(\{a\}) &= \{a\} \end{aligned}$$
    and hence the least fixed point of f is $\{a\}$.