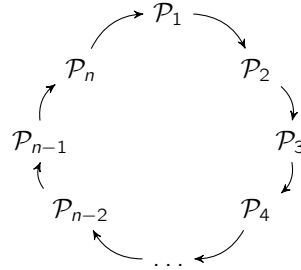


Exercise 1 (Channel Systems):

(3 points)

Consider the following leader election algorithm: For $n \in \mathbb{N}$, n processes $\mathcal{P}_1, \dots, \mathcal{P}_n$ are located in a ring topology where each process is connected by an unidirectional, asynchronous channel to its neighbour as outlined below.



To distinguish the processes, each process i is assigned a unique identifier $id(\mathcal{P}_i) \in \{1, \dots, n\}$ that is written to private variable id_i . The aim of the algorithm is to elect the process with the highest identifier as the (unique) leader within the ring. Therefore each process executes the following algorithm using another private variable m_i (which is initially 0):

```
send(idi); // send own id to next process.
while (true) do {
  receive (mi);
  if (mi == idi) then stop; // process i is the leader
  if (mi > idi) then send(mi); // forward other identifier
}
```

- Model the leader election protocol for n processes as a channel system.
- Give an initial execution fragment of $TS([\mathcal{P}_1 \mid \mathcal{P}_2 \mid \mathcal{P}_3])$ such that at least one process has executed its send-statement within the body of the while-loop. Assume for $1 \leq i \leq 3$, that process $\mathcal{P}_i$ has identifier $id_i = i$.

Solution: _____

- The program graph for process $\mathcal{P}_i$ is given by $\mathcal{P}_i = (\text{Loc}_i, \text{Act}_i, \text{Effect}_i, \xrightarrow{\quad}_i, \text{Loc}_0^i, g_0^i)$ over the set of variables $\text{Var}_i = \{id_i, m_i\}$.

To connect the processes, we define the channels as

$$\text{Chan} := \{c_{ij} \mid i \in \{1, \dots, n\}, j = (i \bmod n) + 1\}$$

where each channel has capacity n :

$$\text{cap}(c) := n \quad \forall c \in \text{Chan}.$$

The domain of the channel is defined by $\text{Dom}(c) := \{1, \dots, n\} \quad \forall c \in \text{Chan}.$

The program graph is given by:

$$\begin{aligned} \text{Loc}_i &:= \{start_i, recv_i, test_i, int_i, stop_i\} \\ \text{Act}_i &:= \{noop_i\} \\ \text{Effect}_i(noop_i, \eta) &:= \eta \\ \text{Loc}_0^i &:= \{start_i\} \\ g_0^i &:= id_i = id(\mathcal{P}_i) \wedge m_i = 0 \end{aligned}$$

The transition relation is given as follows:

$$\begin{aligned}
 start_i &\xrightarrow{c_{i,i+1}!id_i}_i recv_i \\
 recv_i &\xrightarrow{c_{i-1,i}?m_i}_i test_i \\
 test_i &\xrightarrow{m_i=id_i:noop_i}_i stop_i \\
 test_i &\xrightarrow{m_i>id_i}_i int_i \\
 int_i &\xrightarrow{c_{i,i+1}!m_i}_i recv_i \\
 test_i &\xrightarrow{m_i<id_i:noop_i}_i recv_i
 \end{aligned}$$

b) The transition system for $CS = [\mathcal{P}_1 | \mathcal{P}_2 | \dots | \mathcal{P}_n]$ is given as follows:

$$TS(CS) = (S, Act, \rightarrow, I, AP, L) \quad \text{where}$$

- $S := Loc_1 \times \dots \times Loc_n \times Eval(\bigcup_{i=1}^n Var_i) \times Eval(Chan)$
- $Act := \{noop_i \mid i \in \{1, \dots, n\}\} \cup \{\tau\}$
- $\rightarrow \subseteq S \times Act \times S$
- $I := \{(start_1, \dots, start_n, \eta, \xi_\epsilon) \mid \bigwedge_{i=1}^n \eta \models g_0^i\}$ where $\xi_\epsilon : Chan \rightarrow Dom(c)^*$ denotes the initial channel evaluation that assigns an empty content to each channel
- $AP := \{\{id_i = j\} \mid i, j \in \{1, \dots, n\}\} \cup \bigcup_{i=1}^n Loc_i$
- $L : S \rightarrow 2^{AP} : (l_1, \dots, l_n, \eta, \xi) \mapsto \{l_1, \dots, l_n\} \cup \{id_i = j \mid \eta(id_i) = j\}$

An initial execution fragment:

$$\begin{aligned}
 &\langle st, st, st, \overbrace{[id_1/1, id_2/2, id_3/3, m_1/0, m_2/0, m_3/0]}^\eta, c_{1,2} = c_{2,3} = c_{3,1} = \epsilon \rangle \\
 &\xrightarrow{\tau} \langle rc, st, st, \eta, c_{1,2} = 1, c_{2,3} = c_{3,1} = \epsilon \rangle \\
 &\xrightarrow{\tau} \langle rc, st, rc, \eta, c_{1,2} = 1, c_{2,3} = \epsilon, c_{3,1} = 3 \rangle \\
 &\xrightarrow{\tau} \langle test, st, rc, \eta[m_1/3], c_{1,2} = 1, c_{2,3} = c_{3,1} = \epsilon \rangle \\
 &\xrightarrow{\tau} \langle int, st, rc, \eta[m_1/3], c_{1,2} = 1, c_{2,3} = c_{3,1} = \epsilon \rangle \\
 &\xrightarrow{\tau} \langle rc, st, rc, \eta[m_1/3], c_{1,2} = 13, c_{2,3} = c_{3,1} = \epsilon \rangle \\
 &\dots
 \end{aligned}$$

Exercise 2 (Extending Channel Systems):

(2 points)

According to the lecture, the transition relation $\hookrightarrow$ of a program graph $\mathcal{P} = (Loc, Act, Effect, \hookrightarrow, Loc_0, g_0)$ in a channel system over the set of variables Var and set of channels $Chan$ consists of transitions of the form

- $\ell \xrightarrow{g:\alpha} \ell'$ with $\ell, \ell' \in Loc$, $g \in Cond(Var)$, $\alpha \in Act$, or
- $\ell \xrightarrow{c!v} \ell'$ with $\ell, \ell' \in Loc$, $c \in Chan$, $v \in Dom(c)$, or
- $\ell \xrightarrow{c?x} \ell'$ with $\ell, \ell' \in Loc$, $c \in Chan$, $x \in Var$.

For both subtasks, consider a channel system consisting of the program graphs $\mathcal{P}_1, \dots, \mathcal{P}_n$ that are extended or modified as described in the subtasks.

- a) Let $env \notin \text{Chan}$ be a distinguished channel. Reading from this channel is supposed to model reading a value from an (unknown) environment. Give SOS rules for the transition system semantics for transitions of the form $\ell \xrightarrow{env?x} \ell'$.
- b) For channels c with $cap(c) = 0$, we change the semantics of a transition $\ell \xrightarrow{c!v} \ell'$ to that of a broadcasting mechanism: if a value is sent via such a channel, any number of processes (including none) can decide to participate in the handshaking and receive the value. Give SOS rules that formalize the transition system semantics of this operation.

Solution: _____

- a) Since the environment is unknown, we model reading a value as nondeterministically reading any possible value. We formalize this as follows:

$$\frac{\ell_i \xrightarrow{env?x}_i \ell'_i \wedge v \in \text{Dom}(x)}{\langle \ell_1, \dots, \ell_i, \dots, \ell_n, \eta, \xi \rangle \xrightarrow{\tau} \langle \ell_1, \dots, \ell'_i, \dots, \ell_n, \eta[x := v], \xi \rangle}$$

- b) For all partitions $A \uplus \{i\} \uplus B = \{1, \dots, n\}$ of the index set we allow all of the processes with an index in A to receive the message sent by process i while processes in B remain unchanged.

$$\frac{\ell_i \xrightarrow{c!v}_i \ell'_i \wedge cap(c) = 0 \wedge \bigwedge_{j \in A} \ell_j \xrightarrow{c?x_j}_j \ell'_j}{\langle \ell_1, \dots, \ell_n, \eta, \xi \rangle \xrightarrow{\tau} \langle \pi_A(\ell_1), \dots, \pi_A(\ell_n), \eta[x_i := v \text{ for all } i \in A], \xi \rangle}$$

$$\text{where } \pi_A(\ell_j) = \begin{cases} \ell'_j & j \in A \cup \{i\} \\ \ell_j & \text{otherwise} \end{cases}.$$

Exercise 3 (Parallel Composition):

(3 points)

In the following, whenever transition systems are compared via $=$ or $\neq$, this means (in)equality **up to renaming of states** (i.e. isomorphism).

- a) Show that, the handshaking $\parallel_H$ operator **is not** associative, i.e. that in general

$$(TS_1 \parallel_H TS_2) \parallel_{H'} TS_3 \neq TS_1 \parallel_H (TS_2 \parallel_{H'} TS_3)$$

- b) The handshaking operator $\parallel$ that forces transition systems to synchronize over their common actions **is** associative. Show that

$$\underbrace{(TS_1 \parallel TS_2) \parallel TS_3}_L = \underbrace{TS_1 \parallel (TS_2 \parallel TS_3)}_R$$

where TS_1, TS_2, TS_3 are arbitrary (finite) transition systems. To this end, show that the bijective function $f_{\approx}: (S_1 \times S_2) \times S_3 \rightarrow S_1 \times (S_2 \times S_3)$ given by $f_{\approx}(\langle \langle s_1, s_2 \rangle, s_3 \rangle) = \langle s_1, \langle s_2, s_3 \rangle \rangle$ preserves the transition relation in the sense that

$$I \xrightarrow{\alpha}_L I' \iff f_{\approx}(I) \xrightarrow{\alpha}_R f_{\approx}(I') \quad (1)$$

where $I, I' \in S_L$, S_L is the state space of transition system L and $\xrightarrow{\alpha}_L, \xrightarrow{\alpha}_R$ are the transition relations of L and R , respectively.

Hint: When considering an action α , you need only distinguish the cases

- (i) $\alpha \in \text{Act}_1 \setminus (\text{Act}_2 \cup \text{Act}_3)$

(ii) $\alpha \in (Act_1 \cap Act_2) \setminus Act_3$

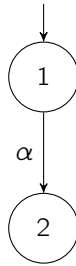
(iii) $\alpha \in Act_1 \cap Act_2 \cap Act_3$

(Act_i is the action set of TS_i) as all other cases are symmetric. Also, for simplicity, it suffices to show the direction " $\implies$ " of condition (1). However, keep in mind that L and R are not necessarily action-deterministic (see exercise sheet 1).

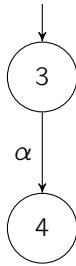
Solution: _____

a) Consider the following three transition systems:

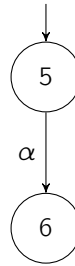
TS_1 :



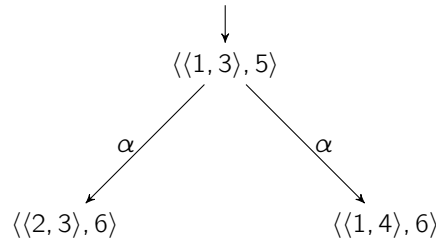
TS_2 :



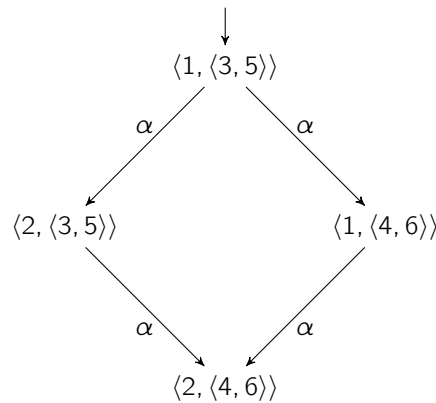
TS_3 :



The result of the composition $(TS_1 \parallel_{\emptyset} TS_2) \parallel_{\{\alpha\}} TS_3$ is:



whereas the result of the composition $TS_1 \parallel_{\emptyset} (TS_2 \parallel_{\{\alpha\}} TS_3)$ is:



b) It remains to show the $\implies$ of condition (1), i.e.

$$I \xrightarrow{\alpha}_L I' \implies f_{\approx}(I) \xrightarrow{\alpha}_R f_{\approx}(I')$$

Fix any action $\alpha \in Act_L$. We distinguish the following cases:

- (i) $\alpha \in \text{Act}_1 \setminus (\text{Act}_2 \cup \text{Act}_3)$
- (ii) $\alpha \in (\text{Act}_1 \cap \text{Act}_2) \setminus \text{Act}_3$
- (iii) $\alpha \in \text{Act}_1 \cap \text{Act}_2 \cap \text{Act}_3$

The case where α does not belong to any action set is irrelevant and all other cases are symmetric. Fix any triple of states from TS_1 , TS_2 and TS_3 , say s_1, s_2, s_3 . Let $l = \langle \langle s_1, s_2 \rangle, s_3 \rangle$ and $r = f_{\approx}(l) = \langle s_1, \langle s_2, s_3 \rangle \rangle$

- (i) There is no α -transition from s_2 or s_3 . If there is no α -transition from s_1 then there is also no α -transition in the composed systems from $\langle \langle s_1, s_2 \rangle, s_3 \rangle$ or $\langle s_1, \langle s_2, s_3 \rangle \rangle$ respectively. So there is nothing to show.

Now assume there is (at least) one α -transition from s_1 . Pick one α -successor, say s'_1 . TS_1 and TS_2 interleave on α : $\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s_2 \rangle$. This subsystem again interleaves on α with TS_3 so in L we get a transition $\langle \langle s_1, s_2 \rangle, s_3 \rangle \xrightarrow{\alpha} \langle \langle s'_1, s_2 \rangle, s_3 \rangle$. On the other hand in $\text{TS}_2 \parallel \text{TS}_3$ there is no α -transition from $\langle s_2, s_3 \rangle$. In R we get the transition $\langle s_1, \langle s_2, s_3 \rangle \rangle \xrightarrow{\alpha} \langle s'_1, \langle s_2, s_3 \rangle \rangle$. We have shown that for the transition $l = \langle \langle s_1, s_2 \rangle, s_3 \rangle \xrightarrow{\alpha} \langle \langle s'_1, s_2 \rangle, s_3 \rangle = l'$ there exists a transition $f_{\approx}(l) = \langle s_1, \langle s_2, s_3 \rangle \rangle \xrightarrow{\alpha} \langle s'_1, \langle s_2, s_3 \rangle \rangle = f_{\approx}(l')$.

- (ii) There is no α -transition from s_3 . If there is no α -transition from s_1 or no α transition in s_2 , again there is no α -transition in l and there is nothing to show.

Now assume there is (at least) one α -transition from s_1 and one α transition in s_2 . Pick α -successors, say s'_1 and s'_2 . In $\text{TS}_1 \parallel \text{TS}_2$ the systems synchronise on α and we have the transition $\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s'_2 \rangle$. This subsystem interleaves with TS_3 on α and so in L we get a transition $\langle \langle s_1, s_2 \rangle, s_3 \rangle \xrightarrow{\alpha} \langle \langle s'_1, s'_2 \rangle, s_3 \rangle$. On the other hand TS_2 and TS_3 interleave on α : $\langle s_2, s_3 \rangle \xrightarrow{\alpha} \langle s'_2, s_3 \rangle$. This subsystem synchronizes with TS_1 on α and so in R we get the transition $\langle s_1, \langle s_2, s_3 \rangle \rangle \xrightarrow{\alpha} \langle s'_1, \langle s'_2, s_3 \rangle \rangle$. We have shown that for the transition $l = \langle \langle s_1, s_2 \rangle, s_3 \rangle \xrightarrow{\alpha} \langle \langle s'_1, s'_2 \rangle, s_3 \rangle = l'$ there exists a transition $f_{\approx}(l) = \langle s_1, \langle s_2, s_3 \rangle \rangle \xrightarrow{\alpha} \langle s'_1, \langle s'_2, s_3 \rangle \rangle = f_{\approx}(l')$.

- (iii) If there is no α transition in any one of the states s_1, s_2, s_3 , then in both the composed systems L and R there is no α -transition from both $\langle \langle s_1, s_2 \rangle, s_3 \rangle$ and $\langle s_1, \langle s_2, s_3 \rangle \rangle$ and there is nothing to show.

Assume there is (at least) one α -transition from s_1 , one from s_2 and one from s_3 . Pick α -successors, say s'_1, s'_2 and s'_3 . In $\text{TS}_1 \parallel \text{TS}_2$ the systems synchronize on α and we have the transition $\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s'_2 \rangle$. This subsystem synchronizes with TS_3 on α and so in L we get a transition $\langle \langle s_1, s_2 \rangle, s_3 \rangle \xrightarrow{\alpha} \langle \langle s'_1, s'_2 \rangle, s'_3 \rangle$. On the other hand in TS_2 and TS_3 also synchronize on α : $\langle s_2, s_3 \rangle \xrightarrow{\alpha} \langle s'_2, s'_3 \rangle$. This subsystem synchronizes with TS_1 on α and so in R we get the transition $\langle s_1, \langle s_2, s_3 \rangle \rangle \xrightarrow{\alpha} \langle s'_1, \langle s'_2, s'_3 \rangle \rangle$. We have shown that for the transition $l = \langle \langle s_1, s_2 \rangle, s_3 \rangle \xrightarrow{\alpha} \langle \langle s'_1, s'_2 \rangle, s'_3 \rangle = l'$ there exists a transition $f_{\approx}(l) = \langle s_1, \langle s_2, s_3 \rangle \rangle \xrightarrow{\alpha} \langle s'_1, \langle s'_2, s'_3 \rangle \rangle = f_{\approx}(l')$.

Exercise 4 (LT properties):

(2 points)

Let's do some rocket science. Imagine a rocket whose possible (observable) behaviors are infinite traces over the atomic propositions

$$\text{AP} = \{\text{parachute}, \text{ground}, \text{space}\}$$

All signals are issued by two detectors on board the rocket: a parachute detector and a ground/space detector. Assume that the detectors are working perfectly unless otherwise specified, meaning that *ground* and *space* are never detected in a contradictory way. Note that a rocket can only go from the ground to space and back (and repeat this). It is not possible to go from space into the atmosphere and back to space again without coming back to the ground. I mean c'mon, seriously, what kind of rocket could do that?!

Express the following informally stated properties as LT-properties over the given atomic propositions AP and indicate which of them are invariants. Give (very) brief explanations for your answers.

- (i) Initially, the rocket is on the ground.
- (ii) Assuming that the detector actually *can* break:

The ground/space detector is never broken, meaning that it never yields contradictory results.

- (iii) Whenever the rocket leaves the ground, it eventually returns to the ground.
- (iv) Whenever the rocket descends back to earth, the parachute is open at most two time steps after space has been left.
- (v) The rocket is only finitely many time steps in space.

Solution: _____

The task is to create linear time properties over the set of atomic propositions AP. That is, we have to give languages over infinite words over the alphabet 2^{AP} .

(i)

$$P = \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \text{ground} \in A_0\}$$

This property **is not** an invariant.

Explanation: The atomic proposition *ground* needs to hold in the first time step.

(ii)

$$P = \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \forall i. (\text{ground} \notin A_i \vee \text{space} \notin A_i)\}$$

This property **is** an invariant.

Explanation: For every time point, either *ground* or *space* is not detected.

(iii)

$$P = \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \forall i. (\text{ground} \notin A_i \implies \exists j > i. \text{ground} \in A_j)\}$$

This property **is not** an invariant.

Explanation: For every time point that the rocket is on the *ground*, there exists some point in the future where the ship is again on the *ground*.

(iv)

$$P = \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \forall i. (\text{space} \in A_i \wedge \text{space} \notin A_{i+1}) \implies (\text{parachute} \in A_{i+1} \vee \text{parachute} \in A_{i+2})\}$$

This property **is not** an invariant.

Explanation: As soon as the rocket has left space, *parachute* must hold in the next time step or in the one after that.

(v)

$$P = \{A_0 A_1 \dots \in (2^{AP})^\omega \mid \exists i. \forall j > i. \text{space} \notin A_j\}$$

This property **is not** an invariant.

Explanation: From some point on, the rocket is never in space again.