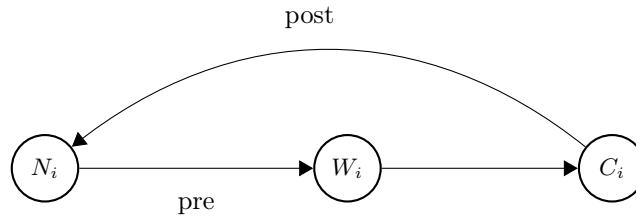


Introduction to Model Checking 2015:

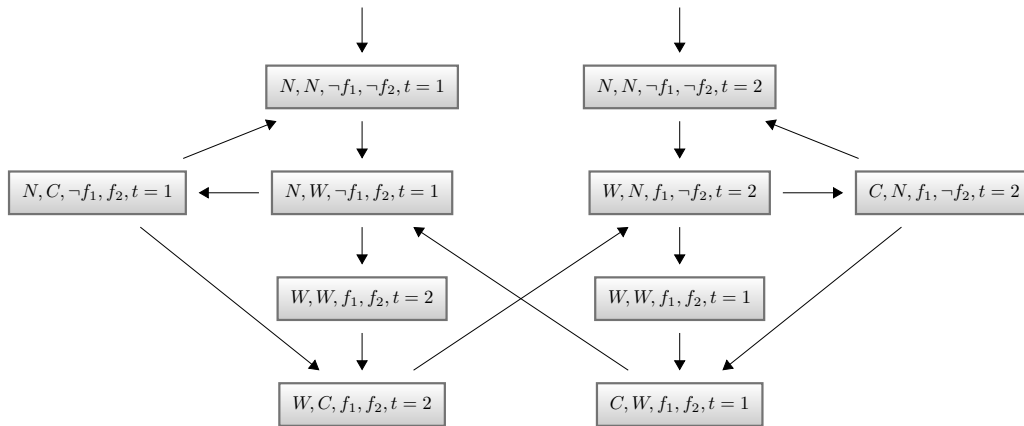
Exercise 2. Solution

Solution 1 Let each process P_i be represented by the following transition system.



1. Peterson's solution is modeled as follows;

(a) We assume initially all flags are false.



(b) **Mutual exclusion:** The state $\langle C, C \rangle$ is not reachable.

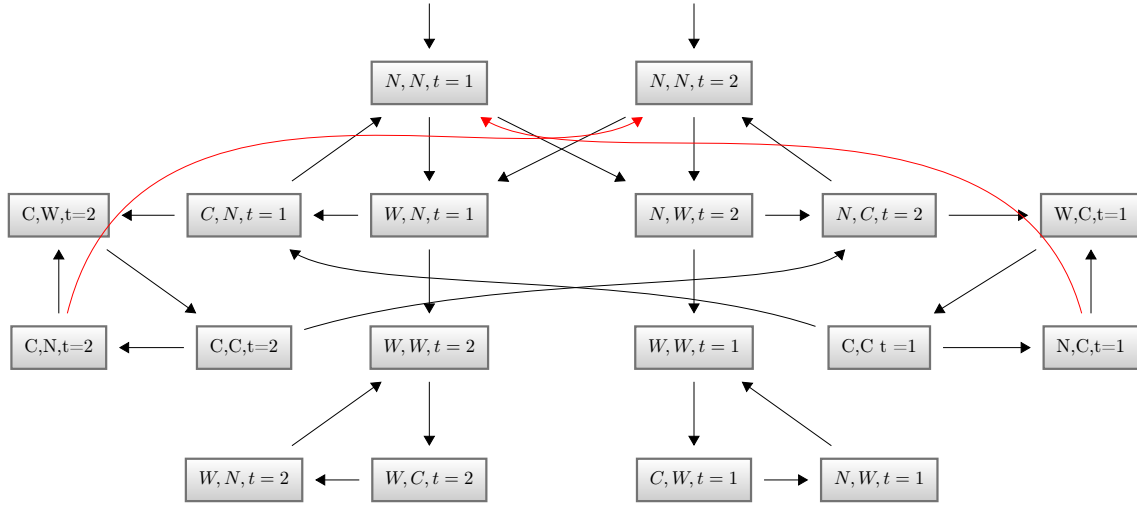
Progress: Consider the states $\langle W, W \rangle$, $\langle N, W \rangle$ and $\langle W, N \rangle$. None of the process are in their critical section and some process wish to enter the critical section. The selection of some process to enter the critical section is done at most by the next two steps.

Bounded waiting: We do not have a cycle where some process is always waiting.

(c) The bound is 1.

2. Simple solution to critical section problem:

(a) The transition system describing the program graph:



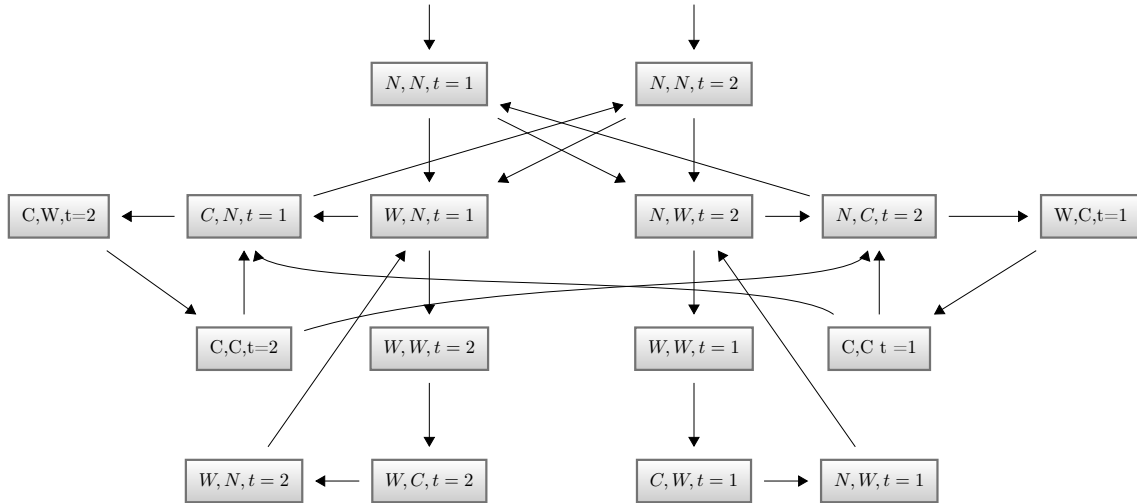
(b) **Mutual exclusion:** The state $\langle C, C \rangle$ is reachable.

Progress: Consider the state $\langle W, N, t=2 \rangle$. None of the process are in their critical section and some process wish to enter the critical section. We can get stuck at this state if process 2 does not want to enter the critical section. Thus Progress is not guaranteed.

Bounded waiting: There are cycles where some process is always waiting. Thus bounded waiting is not guaranteed.

3. Little less simple solution to critical section problem:

(a) The transition system describing the program graph:

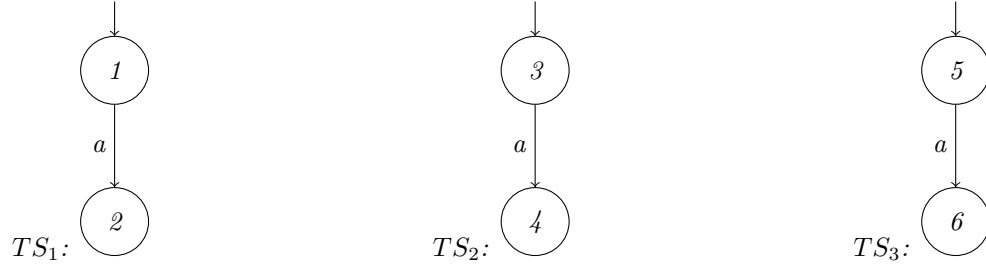


(b) **Mutual exclusion:** The state $\langle C, C \rangle$ is reachable.

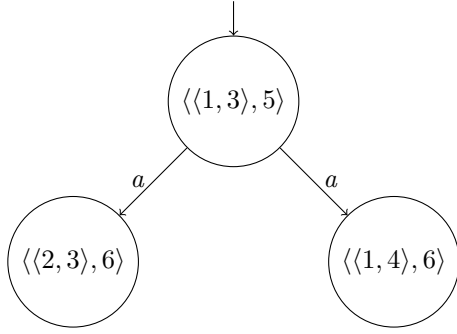
Progress: Consider the state $\langle W, N, t=2 \rangle$. None of the process are in their critical section and some process wish to enter the critical section. Unlike the previous case, we can't get stuck at this state even if process 2 does not want to enter the critical section. Thus Progress is guaranteed.

Bounded waiting: There are cycles where some process is always waiting. Thus bounded waiting is not guaranteed.

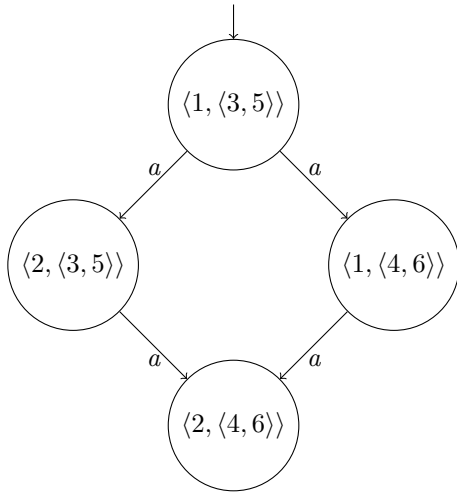
Solution 2 1. Consider the following three transition systems:



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



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



2. Let us define $L = (\mathsf{T}_1 \parallel \mathsf{T}_2) \parallel \mathsf{T}_3$ and $R = \mathsf{T}_1 \parallel (\mathsf{T}_2 \parallel \mathsf{T}_3)$. We want to show that L is isomorphic to R . The state space of both systems is $S_1 \times S_2 \times S_3$. We define a mapping that relates the states of the two systems in the following way:

$$\langle \langle l_1, l_2 \rangle, l_3 \rangle \approx \langle r_1, \langle r_2, r_3 \rangle \rangle$$

if

$$l_1 = r_1$$

$$l_2 = r_2$$

$$l_3 = r_3$$

We now need to show that our mapping is a bijection and preserves the transition relation.

Bijection is obvious!

Now we show that the transition relation is preserved. Fix any action α . For the remaining argument it is relevant in which of the original transition systems $\mathsf{T}_1, \mathsf{T}_2, \mathsf{T}_3$ the action α exists. We distinguish the following cases:

1.) $\alpha \in \text{Act}_1 \setminus (\text{Act}_2 \cup \text{Act}_3)$

2.) $\alpha \in (\text{Act}_1 \cap \text{Act}_2) \setminus \text{Act}_3$

3.) $\alpha \in \text{Act}_1 \cap \text{Act}_2 \cap \text{Act}_3$

The case where α does not belong to any action set is irrelevant and all other cases are symmetric.

1.) Fix any triple of states from T_1, T_2 and T_3 , say s_1, s_2, s_3 . 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 . T_1 and T_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 T_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 $T_2 \parallel T_3$ 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 (in case 1) from two states l and r (from L and R) with $l \approx r$ a transition leads to l' and r' with $l' \approx r'$.

2.) Fix any triple of states from T_1, T_2 and T_3 , say s_1, s_2, s_3 . There is no α -transition from l_3 . If there is no α -transition from s_1 or s_2 again there will not be any α -transition in L and R and there is nothing to show.

Now assume there is (at least) one α -transition from s_1 and s_2 each. Pick α -successors, say s'_1 and s'_2 . In $T_1 \parallel T_2$ 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 T_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 T_2 and T_3 interleave on α : $\langle s_2, s_3 \rangle \xrightarrow{\alpha} \langle s'_2, s_3 \rangle$. This subsystem synchronises with T_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 (in case 2) from two states l and r (from L and R) with $l \approx r$ a transition leads to l' and r' with $l' \approx r'$.

3.) Fix any triple of states from T_1, T_2 and T_3 , say s_1, s_2, s_3 . If any of these states does not have an α -successor then in both the composed systems L and R there is no α -transition from $\langle\langle s_1, s_2 \rangle, s_3 \rangle$ or $\langle s_1, \langle s_2, s_3 \rangle \rangle$ respectively.

Assume there is (at least) one α -transition from s_1, s_2 and s_3 each. Pick α -successors, say s'_1, s'_2 and s'_3 . In $T_1 \parallel T_2$ 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 synchronises with T_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 T_2 and T_3 also synchronise on α : $\langle s_2, s_3 \rangle \xrightarrow{\alpha} \langle s'_2, s'_3 \rangle$. This subsystem synchronises with T_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 (in case 3) from two states l and r (from L and R) with $l \approx r$ a transition leads to l' and r' with $l' \approx r'$.

A isomorphism has to work both ways. However the direction from R to L is absolutely symmetric and needs no further argument.

Hence we have shown that the order in which you compose the systems does not matter.

Solution 3 We define $\text{TS}(CS) = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$ where $S, \text{Act}, I, \text{AP}, L$ are exactly as in Def. 2.33. And $\rightarrow$ is the smallest relation satisfying the axioms and rules:

- “interleaving”:

$$\frac{l_i \xrightarrow{g_i:\alpha} l'_i \wedge \eta \models g}{\langle l_1, \dots, l_i, \dots, l_n, \eta, \xi \rangle \xrightarrow{\tau} \langle l_1, \dots, l'_i, \dots, l_n, \eta', \xi \rangle}$$

where $\eta' = \text{Effect}(\alpha, \eta)$.

- asynchronous message passing

– receive value and assign it to a variable as:

$$\frac{l_i \xrightarrow{g_i:c?x} l'_i \wedge \eta \models g_i \wedge \text{len}(\xi(c)) = k > 0 \wedge \xi(c) = v_1, \dots, v_n}{\langle l_1, \dots, l_i, \dots, l_n, \eta, \xi \rangle \xrightarrow{\tau} \langle l_1, \dots, l'_i, \dots, l_n, \eta', \xi' \rangle}$$

where $\eta' = \eta[x := v_1]$ and $\xi' = \xi[c := v_2 \dots v_k]$.

– transmit value over a channel which is not full as:

$$\frac{l_i \xrightarrow{g_i:c!v} l'_i \wedge \eta \models g_i \wedge \text{len}(\xi(c)) = k < \text{cap}(c) \wedge \xi(c) = v_1, \dots, v_n}{\langle l_1, \dots, l_i, \dots, l_n, \eta, \xi \rangle \xrightarrow{\tau} \langle l_1, \dots, l'_i, \dots, l_n, \eta, \xi' \rangle}$$

where $\xi' = \xi[c := v_2, \dots, v_n, v]$.

- transmit value $v \in \text{dom}(c)$ over full channel c with capacity $\text{cap}(c)$.

$$\frac{l_i \xrightarrow{g_i:clv} l'_i \wedge \eta \models g_i \wedge \text{len}(\xi(c)) = \text{cap}(c) \wedge \xi(c) = v_1, \dots, v_n}{\langle l_1, \dots, l_i, \dots, l_n, \eta, \xi \rangle \xrightarrow{\tau} \langle l_1, \dots, l'_i, \dots, l_n, \eta, \xi' \rangle} \quad (1)$$

where $\xi' = \xi[c := v_2, \dots, v_n, v]$.

- *synchronous message passing*

- 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.

$$\frac{l_i \xrightarrow{g_i:clv} l'_i \wedge \eta \models g_i \wedge \bigwedge_{a \in A} \left(l_a \xrightarrow{g_a:c?x_a} l'_a \wedge \eta \models g_a \right)}{\langle l_{A_1}, \dots, l_{A_k}, l_i, l_{B_1}, \dots, l_{B_m}, \eta, \xi \rangle \xrightarrow{\tau} \langle l'_{A_1}, \dots, l'_{A_k}, l'_i, l_{B_1}, \dots, l_{B_m}, \eta', \xi \rangle} \quad (2)$$

where $k = |A|$ and $m = |B|$ and $\eta' = \eta[x_a := v]$ for all $a \in A$.