

TD – Semantics and Verification
I– Modelling Concurrent Systems
Thursday 14th January 2021

TA: Ralph Sarkis
ralph.sarkis@ens-lyon.fr

In this first set of exercises, we will discuss the modelling of concurrent systems as circuits, transition systems and program graphs. In particular, we will discuss the interleaving of parallel systems.

Preliminaries: Interleaving Operators

In this preliminary section, we provide the definitions of the different interleaving operators from the book.

Definition 1 (Interleaving of Transition Systems). Let $TS_i = (S_i, \text{Act}_i, \rightarrow_i, I_i, \text{AP}_i, L_i)$ be transition systems for $i = 1, 2$. The interleaved transition system is given by

$$TS_1 \parallel TS_2 = (S_1 \times S_2, \text{Act}_1 \cup \text{Act}_2, \rightarrow, I_1 \times I_2, \text{AP}_1 \cup \text{AP}_2, L),$$

where $L\langle s_1, s_2 \rangle = L_1(s_1) \cup L_2(s_2)$ and the transition relation \rightarrow is defined by the following two rules.

$$\frac{s_1 \xrightarrow{\alpha}_1 s'_1}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s_2 \rangle} \quad \frac{s_2 \xrightarrow{\alpha}_2 s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s'_2 \rangle}$$

Definition 2 (Interleaving of Program Graphs). Let $PG_i = (\text{Loc}_i, \text{Act}_i, \text{Effect}_i, \hookrightarrow_i, \text{Loc}_{0,i}, g_{0,i})$ be program graphs for $i = 1, 2$. The interleaved program graph is given by

$$PG_1 \parallel PG_2 = (\text{Loc}_1 \times \text{Loc}_2, \text{Act}_1 \uplus \text{Act}_2, \hookrightarrow, \text{Loc}_{0,1} \times \text{Loc}_{0,2}, g_{0,1} \wedge g_{0,2}),$$

where $\text{Effect}(\alpha, \eta) = \text{Effect}_i(\alpha, \eta)$ for $\alpha \in \text{Act}_i$ and the transition relation \hookrightarrow is defined by the following two rules.

$$\frac{\ell_1 \xrightarrow{g:\alpha}_1 \ell'_1}{\langle \ell_1, \ell_2 \rangle \xrightarrow{g:\alpha} \langle \ell'_1, \ell_2 \rangle} \quad \frac{\ell_2 \xrightarrow{g:\alpha}_2 \ell'_2}{\langle \ell_1, \ell_2 \rangle \xrightarrow{g:\alpha} \langle \ell_1, \ell'_2 \rangle}$$

Definition 3 (Handshaking). Let $TS_i = (S_i, \text{Act}_i, \rightarrow_i, I_i, \text{AP}_i, L_i)$ be transition systems for $i = 1, 2$ and let H be a set of actions with $H \subseteq \text{Act}_1 \cap \text{Act}_2$ and $\tau \notin H$. The synchronised transition system is given by

$$TS_1 \parallel_H TS_2 = (S_1 \times S_2, \text{Act}_1 \cup \text{Act}_2, \rightarrow, I_1 \times I_2, \text{AP}_1 \cup \text{AP}_2, L),$$

where $L\langle s_1, s_2 \rangle = L_1(s_1) \cup L_2(s_2)$ and the transition relation \rightarrow is defined by the following three rules.

$$\frac{s_1 \xrightarrow{\alpha}_1 s'_1}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s_2 \rangle} \alpha \notin H \quad \frac{s_2 \xrightarrow{\alpha}_2 s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s'_2 \rangle} \alpha \notin H \quad \frac{s_1 \xrightarrow{\alpha}_1 s'_1 \quad s_2 \xrightarrow{\alpha}_2 s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s'_2 \rangle} \alpha \in H$$

If $H = \text{Act}_1 \cap \text{Act}_2$, then we abbreviate $TS_1 \parallel_H TS_2$ by $TS_1 \parallel TS_2$.

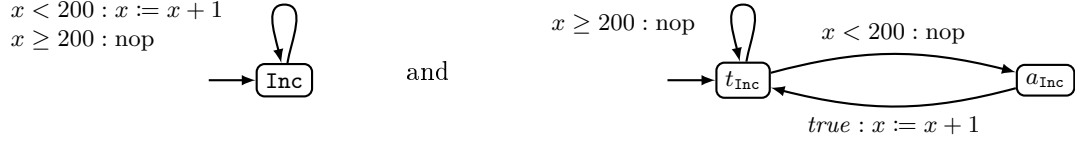
Note: We have that $\parallel = \parallel_{\emptyset}$.

Program Graphs and Atomicity

The first part of the exercise is about different representations of programs as program graphs and the effect of separating tests and assignments. Suppose we are given the following program **Inc**.

Inc: **while** *true* **do** **if** $x < 200$ **then** $x := x + 1$

We may associate two different program graphs, the *atomic* A_{Inc} and the *non-atomic* N_{Inc} , to this program:



The first program graph forces the atomic execution of the test and the assignment, while the second program graph separates these two. Since tests and the body of a while-loop are typically more complex, the second program graph is more realistic. These program graphs show by themselves the same behaviour. However, when combined with other processes that access the same variable, then the separation of test and assignment into the two states t_{Inc} and a_{Inc} matters, as we will see in the following exercise.

Exercise 1.

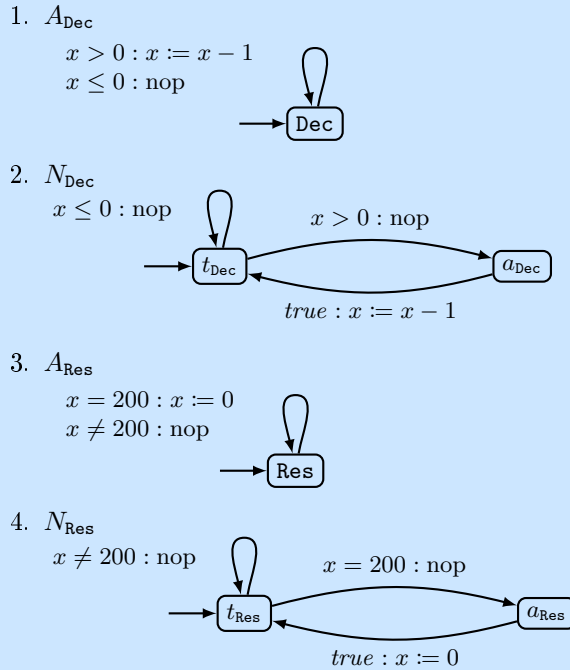
Let the two programs **Dec** and **Res** be given as follows.

Dec: **while** *true* **do** **if** $x > 0$ **then** $x := x - 1$

Res: **while** *true* **do** **if** $x = 200$ **then** $x := 0$

1. Give the atomic and non-atomic program graphs associated to the programs **Dec** and **Res**.

Solution:



2. Compute $TS(A_{\text{Inc}} \parallel A_{\text{Dec}})$ and $TS(A_{\text{Inc}}) \parallel TS(A_{\text{Dec}})$. Which one better modelize shared memory?

Solution:

1. $TS(A_{\text{Inc}} \parallel A_{\text{Dec}}) = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$ where

- $S = \{(\text{Res}, \text{Inc}, \eta) \mid \eta \in \mathbb{N}^{\{x\}}\}$
- $\text{Act} = \{\text{nop}_{\text{Inc}}, \text{nop}_{\text{Res}}, x := 0, x := x + 1\}$
- We have $(\text{Res}, \text{Inc}, \eta) \xrightarrow{\text{nop}_{\text{Inc}}} (\text{Res}, \text{Inc}, \eta)$ if $\eta(x) \geq 200$
 $(\text{Res}, \text{Inc}, \eta) \xrightarrow{\text{nop}_{\text{Inc}}} (\text{Res}, \text{Inc}, \eta)$ if $\eta(x) \neq 200$
 $(\text{Res}, \text{Inc}, \eta) \xrightarrow{x:=0} (\text{Res}, \text{Inc}, \eta[x := 0])$ if $\eta(x) = 200$
 $(\text{Res}, \text{Inc}, \eta) \xrightarrow{x:=x+1} (\text{Res}, \text{Inc}, \eta[x := x + 1])$ if $\eta(x) < 200$
- $I = \{(\text{Res}, \text{Inc}, \eta) \mid \eta \models \top\}$
- $\text{AP} = \{(\text{Res}, \text{Inc})\} \cup \text{Conditions}((x, \mathbb{N}))$
- $L(l, \eta) = \{l\} \cup \{g \mid \eta \models g\}$

2. $TS(A_{\text{Inc}}) \parallel TS(A_{\text{Dec}}) = (S, \text{Act}, \rightarrow, I, \text{AP}, L)$ where

- $S = \{(\text{Inc}, \eta_{\text{Inc}}, \text{Res}, \eta_{\text{Res}}) \mid \eta_{\text{Inc}}, \eta_{\text{Res}} \in \mathbb{N}^{\{x\}}\}$
- $\text{Act} = \{\text{nop}, x := 0, x := x + 1\}$
- We have $(\text{Inc}, \eta_{\text{Inc}}, \text{Res}, \eta_{\text{Res}}) \xrightarrow{\text{nop}} (\text{Inc}, \eta_{\text{Inc}}, \text{Res}, \eta_{\text{Res}})$ if $\eta_{\text{Inc}}(x) \geq 200$ or $\eta_{\text{Res}}(x) \neq 200$
 $(\text{Inc}, \eta_{\text{Inc}}, \text{Res}, \eta_{\text{Res}}) \xrightarrow{x:=0} (\text{Inc}, \eta_{\text{Inc}}, \text{Res}, \eta_{\text{Res}}[x := 0])$ if $\eta_{\text{Res}}(x) = 200$
 $(\text{Inc}, \eta_{\text{Inc}}, \text{Res}, \eta_{\text{Res}}) \xrightarrow{x:=x+1} (\text{Inc}, \eta_{\text{Inc}}[x := x + 1], \text{Res}, \eta_{\text{Res}})$ if $\eta_{\text{Inc}}(x) < 200$
- $I = \{(\text{Inc}, \eta_{\text{Inc}}, \text{Res}, \eta_{\text{Res}}) \mid \eta_{\text{Inc}} \models \top, \eta_{\text{Res}} \models \top\}$
- $\text{AP} = \{\text{Inc}\} \cup \{\text{Res}\} \cup \text{Conditions}((x, \mathbb{N}))$
- $L(\text{Inc}, \eta_{\text{Inc}}, \text{Res}, \eta_{\text{Res}}) = \{\text{Inc}\} \cup \{\text{Res}\} \cup \{g \mid \eta_{\text{Inc}} \models g\} \cup \{g \mid \eta_{\text{Res}} \models g\}$

3. $TS(A_{\text{Inc}}) \parallel TS(A_{\text{Res}})$ “duplicates” x so the memory is not shared (for instance, $\eta_{\text{Inc}}(x)$ is never reset to 0), $TS(A_{\text{Inc}} \parallel A_{\text{Res}})$ better modelize the shared memory.

3. Show that $0 \leq x \leq 200$ is an invariant in the interleaving $A_{\text{Inc}} \parallel A_{\text{Dec}} \parallel A_{\text{Res}}$.

Solution:

We assume that $g_0 \Rightarrow 0 \leq x \leq 200$. We then have to show that if $(\text{Inc}, \text{Dec}, \text{Res}) \xrightarrow{g:\alpha} (\text{Inc}, \text{Dec}, \text{Res})$ is a valid transition and if $\eta \models g$ and $\eta \models 0 \leq x \leq 200$ then $\text{Effect}(\eta, \alpha) \models 0 \leq x \leq 200$. Let's do a case distinction on α :

- If $\alpha = \text{nop}_{\text{Inc}}$, $\alpha = \text{nop}_{\text{Dec}}$ or $\alpha = \text{nop}_{\text{Res}}$, then $\text{Effect}(\eta, \alpha) = \eta$ so $\text{Effect}(\eta, \alpha) \models 0 \leq x \leq 200$.
- If $\alpha = x := x + 1$ then $0 \leq \eta(x) < 200$ and so $0 \leq \text{Effect}(\eta, \alpha)(x) = \eta(x) + 1 \leq 200$.
- If $\alpha = x := x - 1$ then $0 < \eta(x) \leq 200$ and so $0 \leq \text{Effect}(\eta, \alpha)(x) = \eta(x) - 1 \leq 200$.
- If $\alpha = x := 0$ then $0 \leq \text{Effect}(\eta, \alpha)(x) = 0 \leq 200$.

So $0 \leq x \leq 200$ is indeed an invariant of $A_{\text{Inc}} \parallel A_{\text{Dec}} \parallel A_{\text{Res}}$.

4. Show that there is an execution trace in the interleaving $N_{\text{Inc}} \parallel N_{\text{Dec}} \parallel N_{\text{Res}}$ in which x is initially positive but becomes negative.

Solution:

We start with $x = 200$.

$$(t_{\text{Inc}}, t_{\text{Dec}}, t_{\text{Res}}) \xrightarrow{x>0:\text{xnop}} (t_{\text{Inc}}, a_{\text{Dec}}, t_{\text{Res}}) \xrightarrow{x=200:\text{nop}} (t_{\text{Inc}}, a_{\text{Dec}}, a_{\text{Res}}) \xrightarrow{\text{true}:x:=0} (t_{\text{Inc}}, a_{\text{Dec}}, t_{\text{Res}}) \xleftarrow{\text{true}:x:=x-1} (t_{\text{Inc}}, t_{\text{Dec}}, t_{\text{Res}})$$

Mutual Exclusion

Exercise 2.

Consider the following mutual exclusion algorithm that was proposed 1966 as a simplification of Dijkstra's mutual exclusion algorithm in case there are just two processes:

```

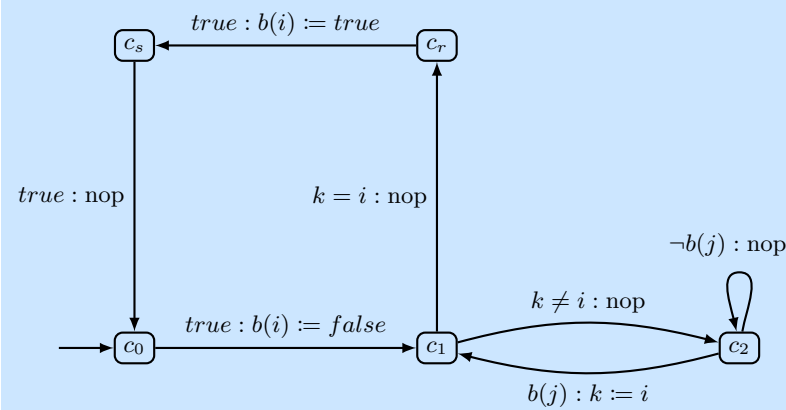
boolean array  $b = [0; 1]$ ;
integer  $k = 1, i, j$ ;
/* This is the program  $P_i$  for computer  $i$ , which may be either 0 or 1, computer
    $j \neq i$  is the other one, 1 or 0 */
C0:  $b(i) := \text{false}$ ;
C1: if  $k \neq i$  then
C2:   if  $\neg b(j)$  then goto C2;
     else  $k := i$ ; goto C1;
    else critical section;
     $b(i) := \text{true}$ ;
    remainder of program;
    goto C0;

```

Here **C0**, **C1**, and **C2** are program labels, and the word “computer” should be interpreted as process.

1. Give the program graph representations for a single process. (A pictorial representation suffices.)

Solution:



2. Give the reachable part of the transition system of $P_0 \parallel P_1$.

Solution:

	$c_{0,0}$	$c_{1,0}$	$c_{2,0}$	$c_{r,0}$	$c_{s,0}$
$c_{0,1}$	✓	✓	✓	✓	✓
$c_{1,1}$	✓	✓	✓	✓	✓
$c_{2,1}$	✓	✓	×	✓	✓
$c_{r,1}$	✓	✓	✓	×	✓
$c_{s,1}$	✓	✓	✓	✓	✓

For all reachable state, we can give an execution reaching this state.

To show that $(c_{2,0}, c_{2,1})$ and $(c_{r,0}, c_{r,1})$ are not reachable, notice that if the process i is in the state $c_{2,i}$ then $k \neq i$ (and so the process i can not be in the state $(c_{2,0}, c_{2,1})$ since it would implied $k \neq 0$ and $k \neq 1$ which is not possible). Also, if the process i is in the state $c_{r,i}$ then necessary $b(i) = \text{false}$ and $k = i$ (and again the state $(c_{r,0}, c_{r,1})$ is unreachable as otherwise there would be state where $k = 0$ and $k = 1$).

3. Check whether the algorithm indeed ensures mutual exclusion, that is, check whether that there is no reachable state in which both processes are in their critical section.

Solution:

The state $(c_{r,0}, c_{r,1})$ is not reachable so the algorithm does ensure mutual exclusion.

Properties of Interleaving

Exercise 3.

Give an example of program graphs PG_1 and PG_2 , such that $TS(PG_1) \parallel TS(PG_2)$ has evaluations as states that are impossible in $TS(PG_1 \parallel PG_2)$ *Hint: In the interleaving $TS(PG_1) \parallel TS(PG_2)$ the variables of PG_1 and PG_2 are renamed and thus not shared.*

Solution:

See exercise 1 question 2.

Exercise 4.

Show that the handshaking operator \parallel is associative. That is, show for arbitrary transition systems TS_1, TS_2, TS_3 that $(TS_1 \parallel TS_2) \parallel TS_3$ and $TS_1 \parallel (TS_2 \parallel TS_3)$ are essentially the same transition system.

Solution:

See the proof of Proposition 15 in Ralph's notes.