Model Checking

Ivo Melse s1088677 & Floris Van Kuijen s1155667

January 2025

1

N.B. We assume that the set H is the same for all compositions.

We start by writing out the definitions.

$$(TS_1||TS_2)||TS_3 = ((S_1 \times S_2) \times S_3, (Act_1 \cup Act_2) \cup Act_3, \rightarrow_l, (I_1 \times I_2) \times I_3, (AP_1 \cup AP_2) \cup AP_3, L_l)$$
$$\text{where } L_l = (L_1(s1) \cup L_2(s_2) \cup L_3(s_3),\ \forall((s1, s2), s3) \in (S_1 \times S_2) \times S_3$$
$$\text{and } \rightarrow_l \text{ is defined according to Figure 2.11.}$$

$$TS_1||(TS_2||TS_3) = (S_1 \times (S_2 \times S_3), Act_1 \cup (Act_2 \cup Act_3), \rightarrow_r, I_1 \times (I_2 \times I_3), AP_1 \cup (AP_2 \cup AP_3), L_r)$$
$$\text{where } L_l = L_1(s1) \cup (L_2(s_2) \cup L_3(s_3)),\ \forall(s1, (s2, s3)) \in S_1 \times (S_2 \times S_3)$$
$$\text{and } \rightarrow_r \text{ is defined according to Figure 2.11.}$$

Now it already follows from associativity of $\times$ and $\cup$ that:

- $(S_1 \times S_2) \times S_3 = S_1 \times (S_2 \times S_3)$
- $(Act_1 \cup Act_2) \cup Act_3 = Act_1 \cup (Act_2 \cup Act_3)$
- $(I_1 \times I_2) \times I_3 = I_1 \times (I_2 \times I_3)$
- $(AP_1 \cup AP_2) \cup AP_3 = AP_1 \cup (AP_2 \cup AP_3)$
- $L_l = L_r$

We still need to show that $\rightarrow_l = \rightarrow_r$. We can do this by case distinction. Let $s_1, s_1' \in S_1$, $s_2, s_2' \in S_2$, and $s_3, s_3' \in S_3$. Note that we will refer to the rules of figure 2.11 as `intL`, `intR` and `Hand`.

Because there are so many cases, we will not explicitly enumerate all of them. Instead, we will show cases where {0,1,2,3} states are equal. The rest of the proof can be constructed the same way, but using a different order of rules.

Case $s_1 \neq s_1'$, $s_2 \neq s_2'$, $s_3 \neq s_3'$.

$$\begin{aligned}
<< s_1, s_2 >, s_3 > \rightarrow_l << s_1', s_2' >, s_3' > &\iff \text{(Hand)}\\
< s_1, s_2 > \rightarrow_{1,2} < s_1', s_2' > \wedge\ s_3 \rightarrow_3 s_3' &\iff \text{(Hand)}\\
s_1 \rightarrow_1 s_1' \wedge s_2 \rightarrow_2 s_2' \wedge s_3 \rightarrow_3 s_3' &\iff \text{(Hand)}\\
s_1 \rightarrow_1 s_1' \wedge < s_2, s_3 > \rightarrow_{2,3} < s_2', s_3' > &\iff \text{(Hand)}\\
< s_1, < s_2, s_3 >> \rightarrow_r < s_1', < s_2', s_3' >>
\end{aligned}$$

Case $s_1 = s_1'$, $s_2 \neq s_2'$, $s_3 \neq s_3'$.

$$\begin{aligned}
<< s_1, s_2 >, s_3 > \rightarrow_l << s_1, s_2' >, s_3' > &\iff \text{(Hand)}\\
< s_1, s_2 > \rightarrow_{1,2} < s_1, s_2' > \wedge s_3 \rightarrow_3 s_3' &\iff \text{(intR)}\\
s_2 \rightarrow_2 s_2' \wedge s_3 \rightarrow_3 s_3' &\iff \text{(Hand)}\\
< s_2, s_3 > \rightarrow_{2,3} < s_2', s_3' > &\iff \text{(intR)}\\
< s_1, < s_2, s_3 >> \rightarrow_r < s_1, < s_2', s_3' >> &
\end{aligned}$$

Case $s_1 = s_1'$, $s_2 \neq s_2'$, $s_3 = s_3'$.

$$\begin{aligned}
<< s_1, s_2 >, s_3 > \rightarrow_l << s_1, s_2' >, s_3 > &\iff \text{(intL)}\\
< s_1, s_2 > \rightarrow_{1,2} < s_1, s_2' > &\iff \text{(intR)}\\
s_2 \rightarrow_2 s_2' &\iff \text{(IntL)}\\
< s_2, s_3 > \rightarrow_{2,3} < s_2', s_3 > &\iff \text{(IntR)}\\
< s_1, < s_2, s_3 >> \rightarrow_r < s_1, < s_2', s_3 >> &
\end{aligned}$$

Now the rest of the cases where at least one is inequal can be constructed in a similar way.

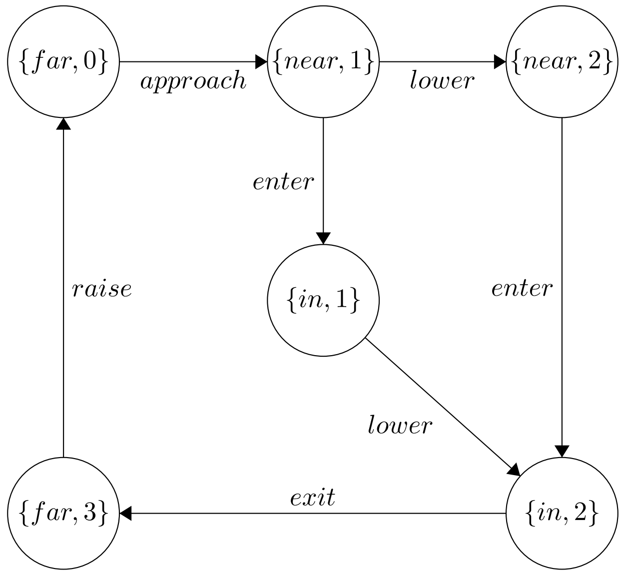
Case $s_1 = s_1'$, $s_2 = s_2'$, $s_3 = s_3'$ Then $\rightarrow_l$ is not defined and $\rightarrow_r$ is not defined, hence it trivially holds that $<< s_1, s_2 >, s_3 > \rightarrow_l << s_1, s_2 >, s_3 >$ $\iff << s_1, s_2 >, s_3 > \rightarrow_r << s_1, s_2 >, s_3 >$

Then we have shown that $(TS_1||TS_2)||TS_3 = TS_1||(TS_2||TS_3)$.

2

a) $H = \{\text{approach}, \text{exit}\}$.

b) (next page)

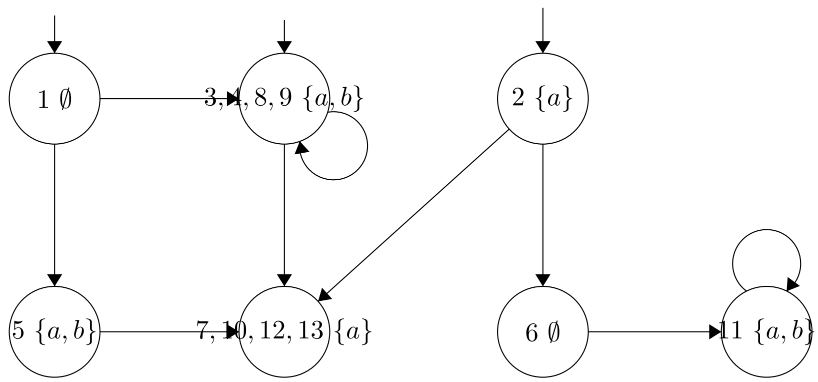


3

- $TS_1 \sim TS_2$. $R = \{(s_1, t_1), (s_2, t_2), (s_3, t_3), (s_4, t_3), (s_5, t_4), (s_6, t_4)\}$
- $TS_1 \nsim TS_3$. $\varphi = \exists \circ \forall \Box (a \wedge b)$. Then $TS_1 \Vdash \varphi$ but $TS_3 \nVdash \varphi$.
- $TS_1 \nsim TS_4$. $\varphi = \exists \circ \exists \circ (a \wedge \neg b)$. Then $TS_1 \nVdash \varphi$, but $TS_4 \Vdash \varphi$.
- Then it also follows that $TS_2 \nsim TS_3$ and $TS_2 \nsim TS_4$.
- $TS_3 \nsim TS_4$. $\varphi = \exists \circ \exists \circ (a \wedge \neg b)$. Then $TS_3 \nVdash \varphi$, but $TS_4 \Vdash \varphi$.

4

Let's execute the algorithm. Start by Paritioning the sets based on labels:
$\{\{s_1, s_6\}, \{s_3, s_4, s_5, s_8, s_9, s_{11}\}, \{s_{10}, s_2, s_7, s_{12}, s_{13}\}\}$
Split on s_3
$\{\{s_1, s_6\}, \{s_3, s_4, s_8, s_9, \}, \{s_5, s_{11}\}, \{s_{10}, s_2, s_7, s_{12}, s_{13}\}\}$
Split on s_5.
$\{\{s_1, s_6\}, \{s_3, s_4, s_8, s_9, \}, \{s_5\}, \{s_{11}\}, \{s_{10}, s_2, s_7, s_{12}, s_{13}\}\}$
Split on s_{10}. $\{\{s_1, s_6\}, \{s_3, s_4, s_8, s_9, \}, \{s_5\}, \{s_{11}\}, \{s_7, s_{10}, s_{12}, s_{13}\}, \{s_2\}\}$
Split on s_1. $\{\{s_1\}, \{s_6\}, \{s_3, s_4, s_8, s_9, \}, \{s_5\}, \{s_{11}\}, \{s_7, s_{10}, s_{12}, s_{13}\}, \{s_2\}\}$
Now we can no longer split.



5

(next page)

5. $\Pi_0 = \Pi_{AP} = \{\{s_0, s_4, s_5, s_7, s_8\}, \{s_1, s_2, s_3, s_6\}\}$

Π_1: $B_1 = \{s_0, s_4, s_5, s_7, s_8\}$, $s_0 \nsim s_4$ so split.

$B_2 = \{s_1, s_2, s_3, s_6\}$, $s_1 \nsim s_2$ so split.

$\Pi_1 = \{\{s_0\}, \{s_4, s_5, s_7, s_8\}, \{s_2\}, \{s_1, s_3, s_6\}\}$

Π_2: $B_2 = \{s_4, s_5, s_7, s_8\}$, $s_4 \sim s_5 \sim s_7 \sim s_8$, next.

$B_4 = \{s_1, s_3, s_6\}$, $s_1 \nsim s_3$ so split.

$\Pi_2 = \{\{s_0\}, \{s_4, s_5, s_7, s_8\}, \{s_2\}, \{s_3\}, \{s_1, s_6\}\}$

Π_3: $B_2 = \{s_4, s_5, s_7, s_8\}$, $s_4 \sim s_5 \sim s_7 \sim s_8$, next.

$B_5 = \{s_1, s_6\}$, $s_1 \sim s_6$. No block can further be refined.

$\sim_{TS} = R_{\Pi_3} = \{(s_i, s_i), (s_4, s_5), (s_4, s_7), (s_4, s_8), (s_5, s_7), (s_7, s_8), (s_1, s_6)\}$

$TS/\sim$: