Teste final de Verificação de Sistemas (CC4084)

DCC-FCUP, University of Porto
José Proença

15th January 2025 – duration: 2h

CCS e sistemas de transição

Exercise 1. Assuma que $A \stackrel{\text{def}}{=} b.a.B$. Usando as regras da semântica operacional do CCS no Anexo A, prove a existência da seguinte transição.

1.1. $(A \mid b.a.B) + ((b.A)[a \mapsto b]) \xrightarrow{b} (A \mid a.B)$

Exercise 2. Considere os seguintes processos.

$$\begin{aligned} \mathit{Mutex_1} &\stackrel{\text{def}}{=} (\mathit{User} \mid \mathit{Sem}) \mid \mathit{User} \setminus \{p,v\} & \mathit{Mutex_2} &\stackrel{\text{def}}{=} ((\mathit{User} \mid \mathit{Sem}) \mid \mathit{FUser})\setminus\{p,v\} \\ \mathit{User} &\stackrel{\text{def}}{=} \overline{p}.\mathit{enter}.\mathit{exit}.\overline{v}.\mathit{User} & \mathit{FUser} &\stackrel{\text{def}}{=} \overline{p}.\mathit{enter}.(\mathit{exit}.\overline{v}.\mathit{FUser} + \mathit{exit}.\overline{v}.\mathbf{0}) \\ \mathit{Sem} &\stackrel{\text{def}}{=} p.v.\mathit{Sem} \end{aligned}$$

2.1. Desenhe o sistema de transições para o processo $\mathit{Mutex_2}$.

2.2. Recorde a definição de bisimulação no Anexo B. Mostre que os sistemas de transição para os processos $\mathit{Mutex_1}$ e $\mathit{Mutex_2}$ são bisimilares, construindo uma bisimulação que o demonstre.

Exercise 3. Considere os seguintes processos.

$$\begin{aligned} \mathit{CTM} &\stackrel{\text{def}}{=} \mathit{coin}.(\overline{\mathit{coffee}}.\mathit{CTM} + \overline{\mathit{tea}}.\mathit{CTM}) \\ \mathit{CTM'} &\stackrel{\text{def}}{=} \mathit{coin}.\overline{\mathit{coffee}}.\mathit{CTM'} + \mathit{coin}.\overline{\mathit{tea}}.\mathit{CTM'} \\ \mathit{CA} &\stackrel{\text{def}}{=} \overline{\mathit{coin}}.\mathit{coffee}.\mathit{CA} \end{aligned}$$

Verifique se os 2 processos abaixo têm os mesmos traços (*traces*).

$$(\mathit{CA} \mid \mathit{CTM}) \setminus \{\mathit{coin}, \mathit{coffee}, \mathit{tea}\}$$
$$(\mathit{CA} \mid \mathit{CTM'}) \setminus \{\mathit{coin}, \mathit{coffee}, \mathit{tea}\}$$

Lógicas modais

Exercise 4. Considere o seguinte sistema de transições.

$$
\begin{tikzcd}
 & s \arrow[r, "a"] \arrow[d, "a"] & s_2 \arrow[d, "a"] \\
s_3 \arrow[ur, "a"] & s_1 \arrow[l, "a"'] \arrow[r, "b"] & s_4 \arrow[ul, "a"']
\end{tikzcd}
$$

Diga se as seguintes propriedades se verificam.

$$s \models \langle a \rangle tt \tag{1}$$
$$s \models [a]\langle b \rangle tt \tag{2}$$
$$s \models [a]\langle a \rangle [a][b] ff \tag{3}$$

Exercise 5. Recorde o Exercício 3. Encontre uma formula que distinga CTM de CTM'. Segundo to teorema da invariância, o que se pode concluir pela existência desta fórmula?

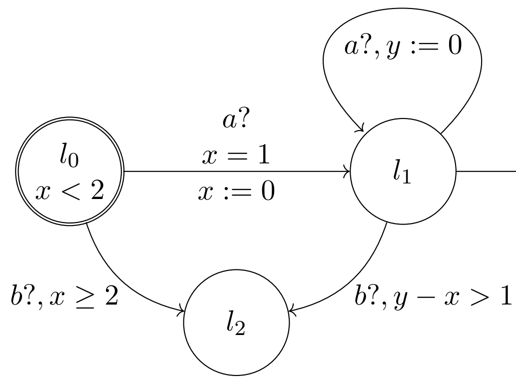
Exercise 6. Recorde a sua propriedade do Exercício 5 acima. Escreva-o usando a notação EARS. Se não conseguiu fazer o Exercício 5 escreva uma propriedade do sistema CTM usando lógica modal e na notação EARS.

Exercise 7. Encontre um sistema de transições com um estado s que obedeça às seguintes propriedades.

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

Modelação de sistemas de tempo real

Exercise 8. Considere o automato de tempo real abaixo.



8.1. O automato tem algum caminho (*trace*) com comportamento Zeno? Explique.

8.2. O automato tem algum caminho (*trace*) com um *timelock*? Explique.

Exercise 9. Considere um sistema com 2 automatos de tempo real em paralelo, *Semáforo* e *Botão*, com estados $\{Verde, Amarelo, Vermelho\}$ e $\{Carregado, Solto\}$, respectivamente. Assuma ainda que o *Semáforo* tem um relógio c que é colocado a zero de cada vez que o sistema chega ao estado $Verde$. Sem modelar os automatos, considere as seguintes propriedades.

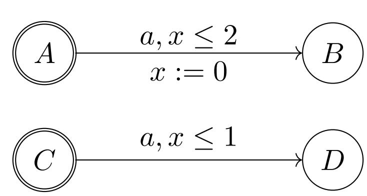
1. O *Botão* não pode estar $Carregado$ enquanto a luz está $Verde$.
2. Demora no máximo 125 unidades de tempo até a luz ficar $Verde$ quando o *Botão* é $Carregado$.

9.1. Escreva as propriedades usando a notação EARS.

9.2. Escreva as propriedades usando lógica temporal (como em UPPAAL).

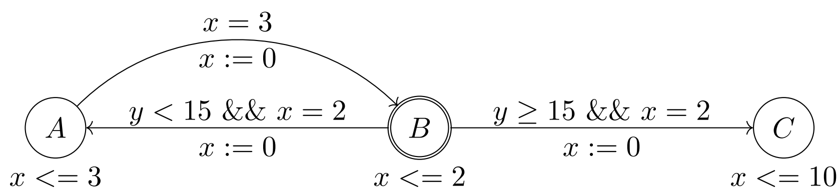
9.3. Escolha uma das propriedades e explique o comportamento de um possível modelo onde a propriedade se verifique e de um outro modelo onde esta não se verifique.

Exercise 10. Considere os 2 automatos de tempo real abaixo, e recorde as definições e bisimulação nos Anexos E e F.



Verifique se os estados A e C são bisimilares, de acordo com a noção de ***untimed*** *bisimulation*. Se sim, mostre uma bisimulação; se não, explique porque é que não podem ser bisimilares.

Exercise 11. Considere o autómato de tempo real abaixo, e recorde a sintaxe do Lince no Anexo G. Observe que este autómato em particular é determinístico e termina. Escreva um programa em Lince que descreva o mesmo comportamento do autómato abaixo, usando duas variáveis x e y que representem o valor dos relógios.



A Anexo: semântica operacional do CCS

$$\frac{}{\alpha.P \xrightarrow{\alpha} P}\text{(act)} \qquad \frac{P \xrightarrow{\alpha} P'}{P+Q \xrightarrow{\alpha} P'}\text{(sum-1)} \qquad \frac{Q \xrightarrow{\alpha} Q'}{P+Q \xrightarrow{\alpha} Q'}\text{(sum-2)} \qquad \frac{P \xrightarrow{\alpha} P'}{P\backslash L \xrightarrow{\alpha} P'\backslash L}\text{(res)}\ \alpha,\overline{\alpha} \notin L$$

$$\frac{P \xrightarrow{\alpha} P'}{P[f] \xrightarrow{f(\alpha)} P'[f]}\text{(rel)} \qquad \frac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q}\text{(com1)} \qquad \frac{Q \xrightarrow{\alpha} Q'}{P|Q \xrightarrow{\alpha} P|Q'}\text{(com2)} \qquad \frac{P \xrightarrow{a} P' \quad Q \xrightarrow{\overline{a}} Q'}{P|Q \xrightarrow{\tau} P'|Q'}\text{(com3)}$$

B Anexo: NFA Bisimulation

Given NFA A_1 and A_2 over N with states S_1 and S_2 respectively, relation $R \subseteq S_1 \times S_2$ is a bisimulation iff both R and its converse R° are simulations. I.e., whenever $\langle p, q\rangle \in R$ and $a \in N$,

(1) $p \xrightarrow{a}_1 p' \;\Rightarrow$ there is a transition $q \xrightarrow{a}_2 q'$ and $\langle p', q'\rangle \in R$

(2) $q \xrightarrow{a}_2 q' \;\Rightarrow$ there is a transition $p \xrightarrow{a}_1 p'$ and $\langle p', q'\rangle \in R$

C Anexo: Semantica da lógica modal

$\mathcal{M}, w \models tt$	always	
$\mathcal{M}, w \not\models ff$	always	
$\mathcal{M}, w \models p$	iff	$w \in V(p)$
$\mathcal{M}, w \models \neg\phi$	iff	$\mathcal{M}, w \not\models \phi$
$\mathcal{M}, w \models \phi_1 \wedge \phi_2$	iff	$\mathcal{M}, w \models \phi_1$ and $\mathcal{M}, w \models \phi_2$
$\mathcal{M}, w \models \phi_1 \rightarrow \phi_2$	iff	$\mathcal{M}, w \not\models \phi_1$ or $\mathcal{M}, w \models \phi_2$
$\mathcal{M}, w \models \langle m\rangle\phi$	iff	there exists $v \in W$ st $wR_m v$ and $\mathcal{M}, v \models \phi$
$\mathcal{M}, w \models [m]\phi$	iff	for all $v \in W$ st $wR_m v$ and $\mathcal{M}, v \models \phi$
$\mathcal{M}, w \models i$	iff	$w = V(i)$
$\mathcal{M}, w \models @_i\phi$	iff	$\mathcal{M}, V(i) \models \phi$

D Anexo: Timed traces and their equivalence

A timed trace over a timed LTS is a (finite or infinite) sequence $\langle t_1, a_1\rangle, \langle t_2, a_2\rangle, \cdots$ in $\mathbb{R}_0^+ \times Act$ such that there exists a path

$$\langle l_0, \eta_0\rangle \xrightarrow{d_1} \langle l_0, \eta_1\rangle \xrightarrow{a_1} \langle l_1, \eta_2\rangle \xrightarrow{d_2} \langle l_1, \eta_3\rangle \xrightarrow{a_2} \cdots$$

such that

$$t_i = t_{i-1} + d_i$$

with $t_0 = 0$ and, for all clock x, $\eta_0\, x = 0$.

Two states s_1 and s_2 of a timed LTS are timed-language equivalent if the set of finite timed traces of s_1 and s_2 coincide;

E Anexo: Timed bisimulation

A relation R is an timed simulation iff whenever $s_1 R s_2$, for any action a and delay $d \in \mathbb{R}_0^+$,

$$s_1 \xrightarrow{a} s_1' \ \Rightarrow \text{ there is a transition } \ s_2 \xrightarrow{a} s_2' \ \& \ s_1' R s_2'$$
$$s_1 \xrightarrow{d} s_1' \ \Rightarrow \text{ there is a transition } \ s_2 \xrightarrow{d} s_2' \ \& \ s_1' R s_2'$$

And it is an timed bisimulation if its converse is also an untimed simulation.

F Anexo: Untimed bisimulation

A relation R is an untimed simulation iff whenever $s_1 R s_2$, for any action a and delays $d, d' \in \mathbb{R}_0^+$,

$$s_1 \xrightarrow{a} s_1' \ \Rightarrow \text{ there is a transition } \ s_2 \xrightarrow{a} s_2' \ \& \ s_1' R s_2'$$
$$s_1 \xrightarrow{d} s_1' \ \Rightarrow \text{ there is a transition } \ s_2 \xrightarrow{d'} s_2' \ \& \ s_1' R s_2'$$

And it is an untimed bisimulation if its converse is also an untimed simulation.

G Anexo: Syntax of Lince

A program in Lince `p` is given by the grammar below, where $n \in \mathbb{R}$ ranges over real numbers and f ranges over functions over real numbers.

```
p ::= x1' = e ,..., xn' = e for e | x := e
    | p ; p | if b then p else p | while b p
e ::= x | n | f(e,...,e)
b ::= e <= e | b && b | ‘' b || b | tt | ff
```