Aula 7: Hennessy-Milner Logic (cont.)

Interaction & Concurrency Course Unit: Reactive Systems Module

April 28, 2023

Recommended reading

Chapter 5 of Aceto et al. 2007.

Concepts introduced and discussed:

- verification of properties of a process by exploring its state space,
- examples of formulas satisfied in a state of a LTS,
- examples of LTS that satisfy simultaneously a set of formulas, in a state,
- distinguishing formulas,
- denotational semantics of HTML,

Some relevant definitions, examples, theorems (from Aceto et al. 2007):

- def. 5.2 (denotational semantics of HML);
- example 5.1;

Exercises suggested (from Aceto et al. 2007):

- Exercise 5.1;
- Exercise 5.2;
- Exercise 5.3;
- Exercise 5.5;
- Exercise 5.7; pg 108
- ~~Exercise 5.6;~~
- Exercise 5.10; pg 113
- Exercise 5.11. pg 113

Other exercises suggested

For each of the following CCS expressions decide whether they are strongly bisimilar and if no, find a distinguishing formula in Hennessy-Milner Logic:

1 - $b.a.Nil + b.Nil$ and $b.(a.Nil + b.Nil)$
2 - $a.(b.c.Nil + b.d.Nil)$ and $a.b.c.Nil + a.b.d.Nil$
3 - $a.Nil \mid b.Nil$ and $a.b.Nil \mid b.a.Nil$
4 - $(a.Nil \mid b.Nil) + c.a.Nil$ and $a.Nil \mid (b.Nil + c.Nil)$

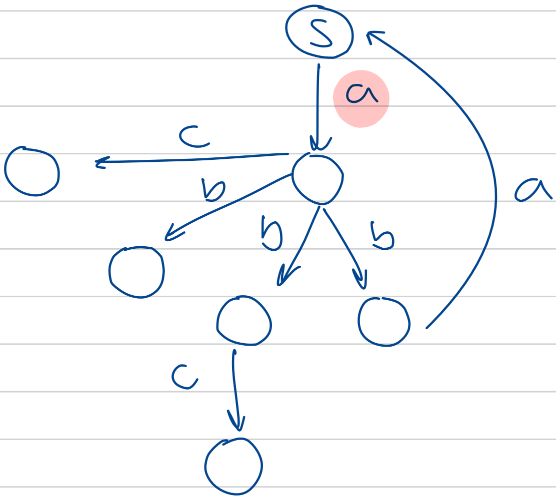
References

Aceto, Luca et al. (2007). *Reactive Systems - Modelling, Specification and Verification*. Cambridge University Press.

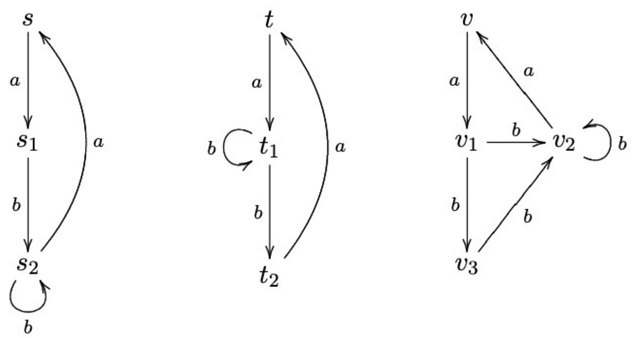
se são bissimilares não há
uma fórmula que os distinga.

Exercise 5.7 *Find one labelled transition system with initial state s that satisfies all of the following properties:*

- $\langle a \rangle(\langle b \rangle \langle c \rangle tt \wedge \langle c \rangle tt)$,
- $\langle a \rangle \langle b \rangle([a]ff \wedge [b]ff \wedge [c]ff)$, *and*
- $[a]\langle b \rangle([c]ff \wedge \langle a \rangle tt)$.



Atenção
[a] → todas as transições



Argue that $s \not\sim t$, $s \not\sim v$ and $t \not\sim v$. Next, find a distinguishing formula of Hennessy-Milner logic for the pairs

- *s and t,*
- *s and v, and*
- *t and v.*

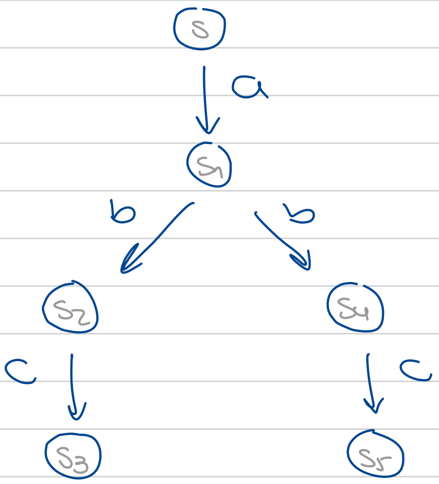
$s \models [a][b]\langle a \rangle$ true $\not\models t$
$\not\models v$

$v \models [a][b]\langle b \rangle$ true $\not\models s$
$\not\models t$

$t \models [a]\langle b \rangle [b]$ false → Não queremos transições por b em t_2

$s \not\models$ ← falha

② $a \cdot (b \cdot c \cdot Nil + b \cdot d \cdot Nil)$



LTS

Não são bissimilares
(contraexemplo)

$t \xrightarrow{a} t_4 \quad s \xrightarrow{a} s_1$

(s_1, t_1) ...

(s_1, t_4)

$s_1 \xrightarrow{b} s_2$

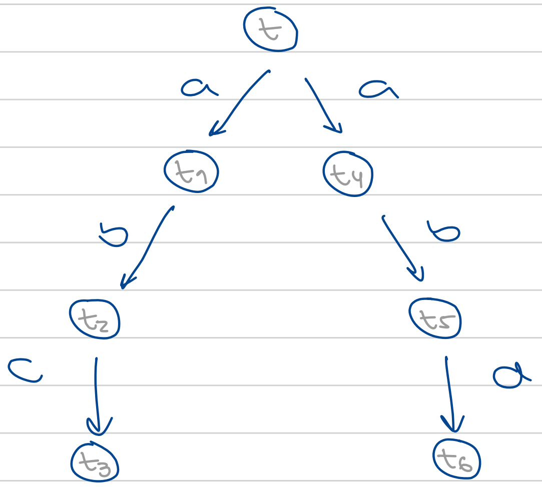
$t_4 \xrightarrow{b} t_5$

(s_2, t_5) falha

$\Downarrow$

encontrar caminho que falha

$a \cdot b \cdot c \cdot Nil + a \cdot b \cdot d \cdot Nil$



A partir de um programa CCS conseguimos chegar a um LTS pelas regras estruturais.

$$\begin{tikzcd} & a \cdot B + c \cdot C \arrow[dl, "a"'] \arrow[dr, "c"] & \\ B & & C \end{tikzcd}$$

→ CCS

→ conseguimos gerar um LTS

ou

$$\begin{tikzcd} & a \cdot B \mid c \cdot C \arrow[dl, "a"'] \arrow[dr, "c"] & \\ B \mid c \cdot C & & a \cdot B \mid C \end{tikzcd}$$

Fórmulas

$s \models [a]\langle b\rangle\langle c\rangle\, true$

$t \not\models$

$t \models [a](\langle b\rangle\langle c\rangle\, true \vee \langle b\rangle\langle a\rangle\, true)$

$s \not\models$

Nil está sempre implícito

Caso tivessemos:

$a \cdot (b \cdot c \cdot Nil \mid b \cdot a \cdot Nil)$

$\xrightarrow{a}$

$b \cdot c \cdot Nil \mid b \cdot a \cdot Nil$

$\xrightarrow{b} \quad c \cdot Nil \mid b \cdot a \cdot Nil$

$\xrightarrow{b} \quad b \cdot c \cdot Nil \mid a \cdot Nil$

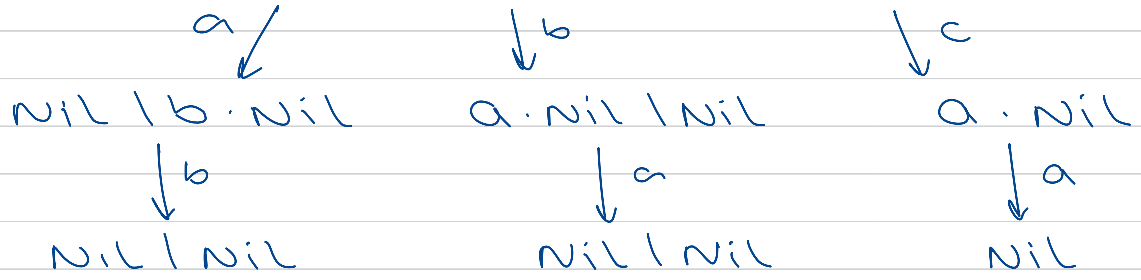
até chegar a Nil

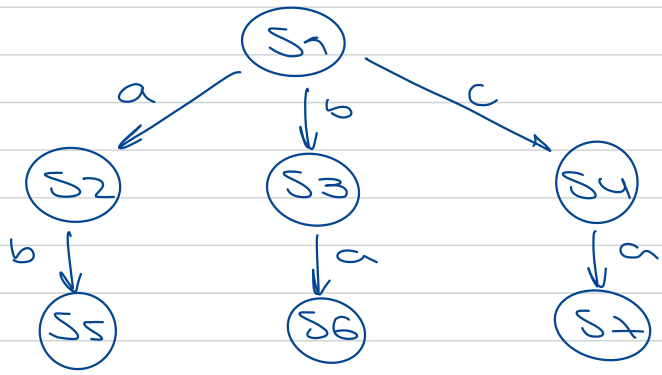
③ $a \cdot Nil \mid b \cdot Nil$ e $a \cdot b \cdot Nil \mid b \cdot a \cdot Nil$

$$
\begin{tikzcd}
 & a \cdot Nil \mid b \cdot Nil \arrow[dl, "a"'] \arrow[dr, "b"] & \\
Nil \mid b \cdot Nil \arrow[d, "b"'] & & a \cdot Nil \mid Nil \arrow[d, "a"] \\
Nil \mid Nil & & Nil \mid Nil
\end{tikzcd}
\qquad
\begin{tikzcd}
 & S \arrow[dl, "a"'] \arrow[dr, "b"] & \\
S_1 \arrow[d, "b"'] & & S_2 \arrow[d, "a"] \\
S_3 & & S_4
\end{tikzcd}
$$

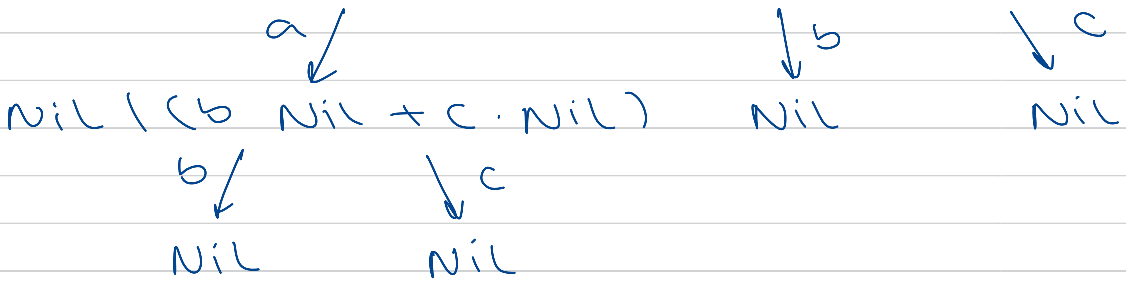
$$
\begin{tikzcd}[column sep=small]
 & & a \cdot b \cdot Nil \mid b \cdot a \cdot Nil \arrow[dl, "a"'] \arrow[dr, "b"] & \\
 & b \cdot Nil \mid b \cdot a \cdot Nil \arrow[dl, "b"'] \arrow[d, "b"] & & a \cdot b \cdot Nil \mid a \cdot Nil \arrow[d] \\
Nil \mid b \cdot a \cdot Nil \arrow[d, "b"'] & b \cdot Nil \mid a \cdot Nil \arrow[d, "b"'] \arrow[dr, "a"] & & \text{(mesma coisa)} \\
Nil \mid a \cdot Nil \arrow[d, "a"'] & Nil \mid a \cdot Nil \arrow[d, "a"'] & b \cdot Nil \mid Nil \arrow[d, "b"] & \\
Nil \mid Nil & Nil \mid Nil & Nil \mid Nil &
\end{tikzcd}
$$

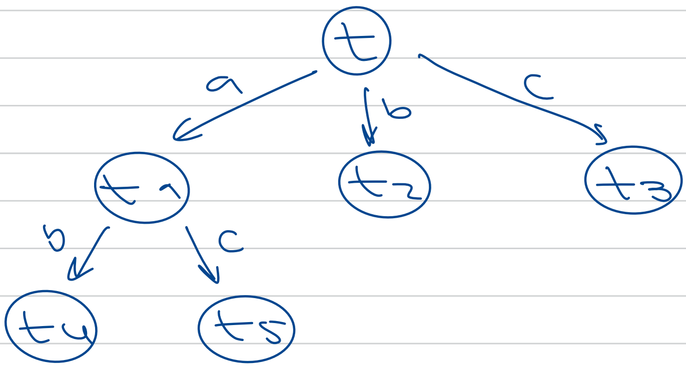
4 $(a \cdot Nil \mid b \cdot Nil) + c \cdot a \cdot Nil$





$a \cdot Nil \mid (b \cdot Nil + c \cdot Nil)$ $\nsim$





Não são fortemente bissimilares por p.ex

(s_3, t_2) $\quad s_3 \xrightarrow{a} s_6 \quad t_2 \not\xrightarrow{a}$

Exemplo em CCS.

Descobrir uma fórmula que os distinga:

① $b \cdot a\ Nil + b\ Nil$

② $b \cdot (a \cdot Nil + b \cdot Nil)$

$$
\begin{tikzcd}
 & b \cdot a \cdot Nil + b \cdot Nil \arrow[dl, "b"'] \arrow[dr, "b"] & \\
a \cdot Nil \arrow[d, "a"] & & Nil \\
Nil & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & b \cdot (a \cdot Nil + b \cdot Nil) \arrow[d, "b"] & \\
 & a \cdot Nil + b \cdot Nil \arrow[dl, "a"'] \arrow[dr, "b"] & \\
Nil & & Nil
\end{tikzcd}
$$

$F = \langle b \rangle [a]\, false$

① $\models F$

② $\not\models F$

$F = \langle b \rangle (\langle a \rangle true \wedge \langle b \rangle true)$

① $\not\models F$

② $\models F$

ou

$[b]\langle a \rangle tt$

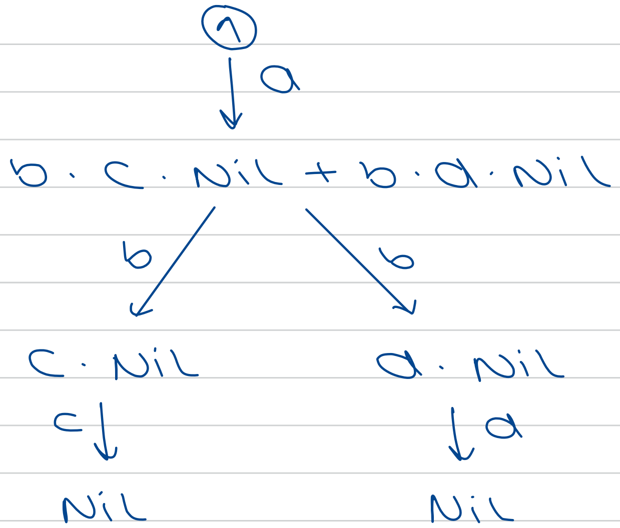
Possibilidade $\langle a \rangle$

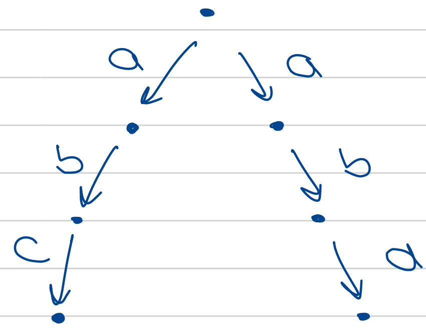
Necessidade $[a]$

Exemplo 2:

① $a \cdot (b \cdot c \cdot Nil + b \cdot d \cdot Nil)$

② $a \cdot b \cdot c \cdot Nil + a \cdot b \cdot d \cdot Nil$





$F = [a] \langle b \rangle \langle c \rangle true \wedge \langle b \rangle \langle d \rangle true$

① $\models F$

② $\not\models F$

$F_2 = [a] (\langle b \rangle [c] false \wedge \langle b \rangle \langle d \rangle false)$

① $\models F$

② $\not\models F$