# LCD (15/04/2024)

## * Hennessy - Milner Logic

CCS equivalence $\approx$

simple language approach $\begin{cases} \text{SYS} \\ \text{SPEC} \end{cases}$ correctness

$\text{sys} \approx \text{SPEC}$

Ex. $\text{Office} = (\text{CS} \mid \text{CTM}) \setminus \{\text{coin}, \text{coffee}, \text{tea}\}$

$\approx$

$\text{Spec} = \overline{\text{pub}} . \text{Spec}$

<u>specific properties</u>

→ at any point of the computation the system will out a $\overline{\text{pub}}$

→ no deadlock

⋮

logical language { temporal / modal }

## * Hennessy Milner Logic

for all a-actions the target state satisfies $\varphi$

$$\varphi, \psi \ ::= \ T \ \mid \ F \ \mid \ \varphi \wedge \psi \ \mid \ \varphi \vee \psi \ \mid \ \langle a \rangle \varphi \ \mid \ [a] \varphi$$

can perform a-action and $\varphi$ holds

$$[\![ \ ]\!] : HML \to 2^{Proc}$$

$$[\![ \varphi ]\!] \subseteq Proc$$

processes where $\varphi$ holds

$$P \models \varphi \quad \text{for} \quad P \in [\![ \varphi ]\!]$$

definition

$$[\![ T ]\!] = Proc$$

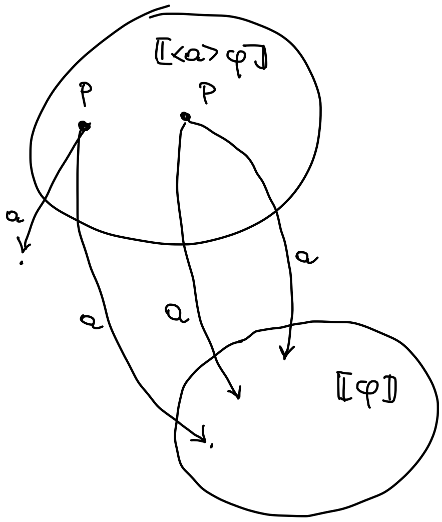
$$[\![ F ]\!] = \emptyset$$

$$[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$$

$$[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$$

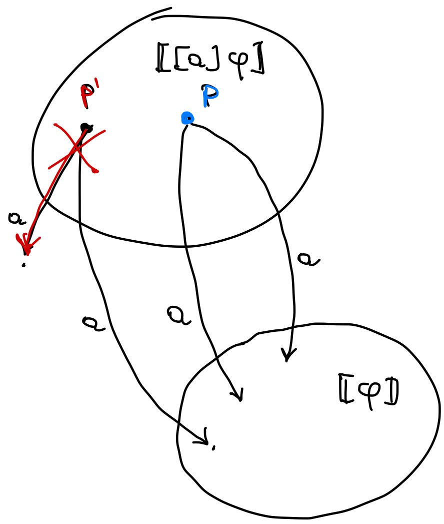
$$[\![\langle a\rangle \varphi]\!] = \langle a\rangle\, [\![\varphi]\!]$$

$$\langle a\rangle X = \{ p \mid \exists p \xrightarrow{a} p' \wedge p' \in X \}$$

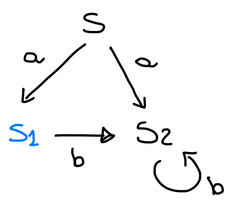


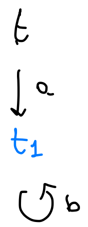

$$[\![[a]\varphi]\!] = [a]\, X$$

$$[a]\, X = \{ p \mid \forall p \xrightarrow{a} p' \;\; p' \in X \}$$




## Example




$X = \{s_1, t_1\}$

$\langle a\rangle X = \{s, t\}$ $\qquad$ $[a]\, X = \{t, s_1, s_2, t_1\}$

$\langle b\rangle X = \{t_1\}$ $\qquad$ $[b]\, X = \{t_1, s, t\}$

* CS can input on coffee

$\langle coffee\rangle \top$

$$[\![\langle cofee\rangle \top]\!] = \langle cofee\rangle [\![\top]\!] = \langle coffee\rangle\, Proc = \{ p \mid \exists p \xrightarrow{coffee} p' \wedge \underbrace{p' \in Proc}_{\text{vacuos}} \}$$

* CS cannot input on coffee

$\neg \cancel{\langle coffee \rangle} T$

$\langle coffee \rangle F$ ⇝ logically equivalent to false

$[\![ \langle coffee \rangle F ]\!] = \langle coffee \rangle [\![ F ]\!] = \langle coffee \rangle \emptyset = \{ p \mid \exists p \xrightarrow{coffee} p' \wedge p' \in \emptyset \}$

$= \emptyset$

$[coffee]\, F$

$[\![ [coffee] F ]\!] = [coffee]\, \emptyset = \{ p \mid \forall p \xrightarrow{coffee} p' \quad p' \in \emptyset \}$

$= \{ p \mid p \not\xrightarrow{coffee} \}$

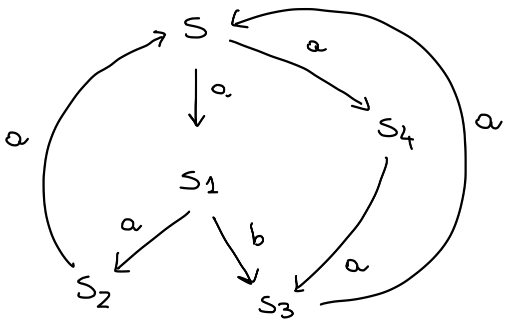
* CS can input both on coffee and tea

$\langle coffee \rangle T \wedge \langle tea \rangle T$

what if each input disable the other?

$\langle coffee \rangle [tea] F \wedge \langle tea \rangle [coffee] F$

Example :




$s \overset{?}{\models} \varphi$

$s \models \langle a \rangle T$ ok

$[b] F$ ok

$[a] \langle a \rangle T$ ok

$s \not\models [a] \langle b \rangle T$ NO

$\langle a \rangle \langle b \rangle T$ ok

$[a][a] \langle a \rangle T$ ok

$[b] \langle a \rangle T$ ok

$\langle a \rangle ( [b][a] F \wedge \langle b \rangle T )$ NO

**Example** :

$$Clock = tick . Clock$$

$$Clock \models \langle tick \rangle T$$

$$Clock \models [tick] \langle tick \rangle T$$

$$Clock \models [tick][tick] \langle tick \rangle T$$

$\vdots$

$$Clock \models \underbrace{[tick] \ldots [tick]}_{n} \langle tick \rangle T \qquad \forall n \in \mathbb{N}$$

**Example** :

$$CTM = coin ( \overline{coffee} . CTM + \overline{tea} \; CTM)$$

$$CTM' = coin . \overline{coffee} . CTM' + coin . \overline{tea} . CTM'$$

$$CTM \not\sim CTM'$$

$$CTM \models [coin] \langle \overline{coffee} \rangle T \quad = \varphi \qquad \not\dashv \; CTM'$$

$$\not\models \langle coin \rangle [\overline{coffee}] F \qquad \dashv$$

* Negation is encodable

Given $\varphi \in HML$ there is $\varphi^c \in HML$ s.t.

for all $P$ $\qquad P \models \varphi$ iff $P \not\models \varphi^c$

$$( [\![ \varphi^c ]\!] = Proc \setminus [\![ \varphi ]\!] ) \qquad (*)$$

$T^c = F$

$F^c = T$ $\qquad$ (EXERCISE)

$(\varphi \wedge \psi)^c = \varphi^c \vee \psi^c$

$(\varphi \vee \psi)^c = \varphi^c \wedge \psi^c$

$(\langle a \rangle \varphi)^c = [a] \varphi^c$

$([a] \varphi)^c = \langle a \rangle \varphi^c$

Example :

$A = a.0 + a.A$ $\qquad A \models \langle a \rangle \langle a \rangle [a] F \not\models B$

$B = a.0 + a.a.B$ $\qquad \not\models [a][a]\langle a \rangle T \;=\!|$

$A \not\sim B$

Hennessy - Milner's Theorem

it holds for image finite processes

P image finite : $\quad$ if $\quad \{ P' \mid P \xrightarrow{a} P' \}$ finite

for all $a \in Act$

Ex.

$A = c.0 \mid A$

$A \xrightarrow{c} A \mid 0 \mid \underbrace{c.0 \mid \ldots \mid c.0}_{n}$ $\qquad$ for all $n \in \mathbb{N}$

not image finite

Theorem : Let $P, Q$ image finite processes

$P \sim Q$ $\quad$ iff $\quad (\forall \varphi \in HML \quad P \models \varphi \Leftrightarrow Q \models \varphi)$

i.e.

1 $\quad$ if $P \sim Q$ then $\forall \varphi \in HML \quad P \models \varphi \Leftrightarrow Q \models \varphi$ (adequacy)

2 $\quad$ if $P \not\sim Q$ then $\exists \varphi \in HML \quad P \models \varphi$ and $Q \not\models \varphi$

proof

$(\Rightarrow)$ if $P \sim Q$ $\quad \forall \varphi$ $\quad$ if $P \models \varphi$ then $Q \models \varphi$

$\Longrightarrow$

$\Longleftarrow$

$(\varphi = T)$ $\quad$ if $P \models T$ then $Q \models T$

$(\varphi = F)$ $\quad$ if $P \models F$ then $Q \models F$

$(\varphi = \psi_1 \wedge \psi_2)$ if $P \models \varphi = \psi_1 \wedge \psi_2$ then $P \models \psi_1$ and $P \models \psi_2$

by ind. hyp $Q \models \psi_1$ and $Q \models \psi_2$

hence $Q \models \psi_1 \wedge \psi_2 = \varphi$

$(\quad \vee \quad)$ same

$(\varphi = \langle a \rangle \psi)$ let $P \models \langle a \rangle \psi$

i.e. $\underline{P \xrightarrow{a} P'}$ and $\underline{P' \models \psi}$

but $\underline{P \sim Q}$ $\boxed{Q \xrightarrow{a} Q'}$ with $\underline{P' \sim Q'}$

ind. hyp.

$\boxed{Q' \models \psi}$

$Q \models \langle a \rangle \psi = \varphi$

$(\varphi = [a] \psi)$ dual

$(\Leftarrow)$

if $\forall \varphi \; (P \models \varphi$ iff $Q \models \varphi)$ then $P \sim Q$

$\mathcal{R} = \{ (P', Q') \mid \forall \varphi \; (P' \models \varphi \Leftrightarrow Q' \models \varphi) \}$

is a bisimulation

i.e.

if $P' \mathcal{R} Q'$ then

- if $P' \xrightarrow{a} P''$ then $Q' \xrightarrow{a} Q''$ and $P'' \mathcal{R} Q''$
- dual

by contradiction: assume $\mathcal{R}$ not a bisimulation i.e. there are $P' \mathcal{R} Q'$ and $P' \xrightarrow{a} P''$ s.t.

$\forall Q' \xrightarrow{a} Q'' \quad P'' \not\mathcal{R} Q''$ i.e. $\exists \varphi \quad P'' \models \varphi$

$Q'' \not\models \varphi$

by image finiteness there are finitely many $Q''$

$$\text{all the a-transitions}\left\{\begin{array}{ll} Q' \xrightarrow{a} Q_1'' & \exists \varphi_1 \text{ s.t. } P'' \models \varphi_1 \,,\; Q_1'' \not\models \varphi_1 \\ \vdots & \vdots \\ Q' \xrightarrow{a} Q_m'' & \exists \varphi_m \text{ s.t. } P'' \models \varphi_m \quad Q_m'' \not\models \varphi_m \end{array}\right.$$

define $\varphi = \langle a \rangle (\varphi_1 \wedge \dots \wedge \varphi_m)$

then $P' \models \varphi \qquad Q' \not\models \varphi$

but this contradicts $P' \mathcal{R} Q'$.

$\square$

<u>EXERCISE</u> : Counterexample to the theorem when processes are not image-finite $(\Leftarrow\!\!\!\!/\;)$