LCD (31/03)

* Hennessy - Milner's Logic

CCS equivalence $\approx$

single language approach { SYS, SPEC } correctness

SYS $\approx$ SPEC

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

$\approx\!\!\approx$

Spec = $\overline{pub}$. Spec

specific properties

→ at any point of the computation in the sequel there will be a $\overline{pub}$

→ there is no deadlock

logical (temporal/modal) language

* Hennessy Milner Logic

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

$\langle a \rangle \varphi$: can execute a and then φ holds

$[a] \varphi$: for all actions a after the step φ holds

Semantics

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

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

often we use $P \models \varphi$ instead of $P \in [\![\varphi]\!]$

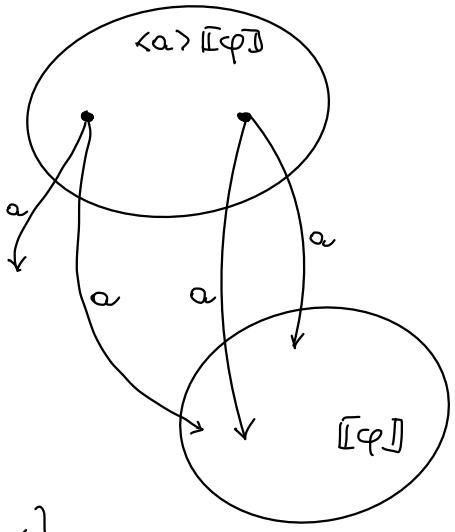
$[\![T]\!] = Proc$

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

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

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

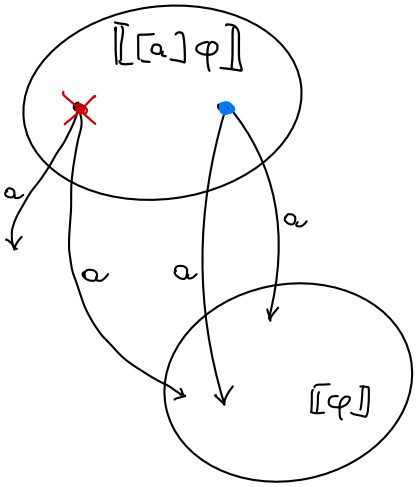
$[\![\langle a \rangle \varphi]\!] = \langle a \rangle \underbrace{[\![\varphi]\!]}_{\text{set of processes}}$



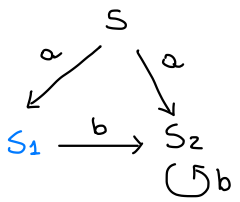
where $\langle a \rangle X = \{ P \mid \exists P \xrightarrow{a} P' \wedge P' \in X \}$

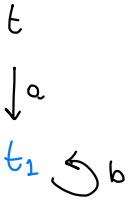
$[\![[a] \varphi]\!] = [a] [\![\varphi]\!]$

where $[a] X = \{ P \mid \forall P \xrightarrow{a} P' \quad P' \in X \}$



Example :





$X = \{s_1, t_1\}$

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

$\langle b \rangle X = \{ t_1 \}$

* CS can input "coffee"

$\langle coffee \rangle T$

$[\![\langle coffee \rangle T]\!] = \langle coffee \rangle [\![T]\!] = \langle coffee \rangle Proc = \{ P \mid P \xrightarrow{coffee} P' \wedge P' \in Proc \}$

* CS cannot input "coffee"

$\neg \langle coffee \rangle T$

$[coffee]\ F$

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

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

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

$\langle coffee \rangle F$ equivalent to F

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

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

$= \emptyset$

* CS can input both coffee and tea

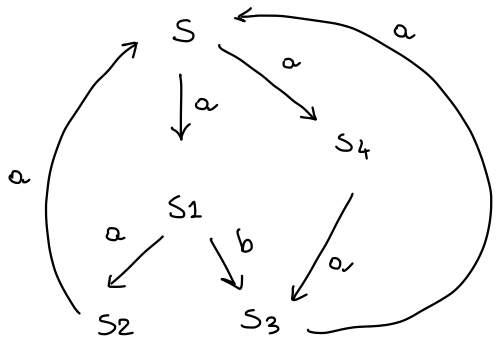
$\langle coffee \rangle T \wedge \langle tea \rangle T$

what if I want that only one possibility holds ?

$(\langle coffee \rangle T \wedge [tea]\ F) \vee (\langle tea \rangle T \wedge [coffee]\ F)$

Example

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



$s \models \langle a \rangle T$

$s \models [b]\ F$

$s \not\models \langle b \rangle T$

$s \models [a] \langle a \rangle T$

$s \not\models [a] \langle b \rangle T$

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

$s \models [a][a] \langle a \rangle T$

$s \not\models \langle a \rangle ([b][a]F \wedge \langle b \rangle T)$

Example : $Clock = tick.\ Clock$

$Clock \models \langle tick \rangle T$

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

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

$\vdots$

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

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

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

$CTM \not\sim CTM'$

$CTM \models [coin]\langle \overline{coffee} \rangle T \qquad \not\models CTM'$

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

* Negation is encodable

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

$\forall P \in Proc \quad P \models \varphi$ iff $P \not\models \varphi^c$

(i.e. $[\![\varphi^c]\!] = Proc \setminus [\![\varphi]\!]$)

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

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

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

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

EXAMPLE: $Clock = tick.0 + tick.Clock$

$Clock' = tick.0 + tick.tick.Clock'$

$Clock \overset{?}{\approx} Clock'$

NO

$Clock \models \langle tick\rangle\langle tick\rangle [tick] F \quad \not\equiv \quad Clock' \models \langle tick\rangle\langle tick\rangle [tick] F$

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

* Hennessy - Milner's Theorem

it holds under image finiteness assumption

P is image finite if $\{ P' \mid P \xrightarrow{a} P' \}$ is finite $\forall a \in Act$

Ex. $A = c.0 \mid A$ (reasonable variation $A = b.(c.0 \mid A)$

$A \xrightarrow{c} \underbrace{c.0 \mid \cdots \mid c.0 \mid c.0}_{\text{any length}} \mid A \mid 0$

Theorem: Let P, Q be image-finite process. Then

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

i.e.

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

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

proof

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

induction on φ

($\varphi \equiv T$) if $P \models T$ then $Q \models T$

($\varphi \equiv F$) if $P \models F$ then $Q \models F$

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

by inductive hyp. $Q \vDash \psi_1$ & $Q \vDash \psi_2$

thus $Q \vDash \psi_1 \wedge \psi_2 = \varphi$

$(\varphi = \psi_1 \vee \psi_2)$ same

$(\varphi = \langle a \rangle \psi)$ if $P \vDash \langle a \rangle \psi$

then $P \xrightarrow{a} P'$ $\quad P' \vDash \psi$

since

$P \sim Q$ $\quad Q \xrightarrow{a} Q'$ and $P' \sim Q'$

ind. hyp.

$Q' \vDash \psi$

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

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

(up to here, image finiteness not needed)

($\Leftarrow$) if $\forall \varphi \in HML \quad (P \vDash \varphi \leftrightarrow Q \vDash \varphi)$ then $P \sim Q$

$R = \{ (P', Q') \mid \forall \varphi . \ (P' \vDash \varphi \leftrightarrow Q' \vDash \varphi) \}$

is bisimulation, i.e. when $P' \, R \, Q'$

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

let's assume by contradiction that R is not a bisimulation

there are P', Q' s.t. $P' \, R \, Q'$ and

$P' \xrightarrow{a} P''$ s.t. $\forall \, Q' \xrightarrow{a} Q'' \quad P'' \not R \, Q''$ ← i.e. $\exists \varphi$ s.t. $P'' \vDash \varphi$ and $Q'' \nvDash \varphi$

finitely many by image finiteness

we can list Q'' a-transitions

$$Q' \xrightarrow{a} Q''_1 \qquad \text{there is } \varphi_1 \text{ s.t. } P'' \models \varphi_1 \text{ and } Q''_1 \not\models \varphi_1$$
$$\vdots \qquad\qquad \vdots$$
$$Q' \xrightarrow{a} Q''_k \qquad \varphi_k \text{ s.t. } P'' \models \varphi_k \text{ and } Q''_k \not\models \varphi_k$$

define

$$\varphi = \langle a \rangle (\varphi_1 \wedge \cdots \wedge \varphi_k)$$

then

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

and this contradicts $P' \, R \, Q'$ (by definition of R).

Hence R is a bisimulation. □

EXERCISE: Counterexample to the theorem when image finiteness fails. ($\Leftarrow$)