LCD (19/03/2024)

* Bisimilarity as a game

Bisimulation: relation $\mathcal{R} \subseteq Proc \times Proc$ such that if $P \mathcal{R} Q$

(i) if $P \xrightarrow{\alpha} P'$ then $Q \xrightarrow{\alpha} Q'$ and $P' \mathcal{R} Q'$

(ii) if $Q \xrightarrow{\alpha} Q'$ then $P \xrightarrow{\alpha} P'$ and $P' \mathcal{R} Q'$

→ P, Q bisimilar ($P \sim Q$) if there exists $\mathcal{R}$ bisimulation s.t. $P \mathcal{R} Q$

i.e.

$$\sim \; = \; \bigcup \{ \mathcal{R} \mid \mathcal{R} \text{ is a bisimulation} \}$$

* how to show $P \not\sim Q$

→ take all possible relations $\mathcal{R} \subseteq Proc \times Proc$ s.t. $P \mathcal{R} Q$

→ check if $\mathcal{R}$ is a bisimulation

suppose P, Q are finite-state, say $n \in \mathbb{N}$ states ($|Proc| = n$)

$\mathcal{R} \subseteq Proc \times Proc$

$|Proc \times Proc| = n^2$

$\#\text{relations} = 2^{n^2}$

if $n = 10$

$\#\text{relations} = 2^{10^2} = 2^{100} \sim 10^{30}$

* Bisimulation Games

on P, Q

2 players

attacker A: aims at proving $P \not\sim Q$ by proposing challenges $P \xrightarrow{\alpha} P'$

defender D: aims at proving $P \sim Q$ by answering to challenges $Q \xrightarrow{\alpha} Q'$

details

→ **rounds** : at each round the game is in a configurations (P', Q')

→ **moves** : **Attacker** – choses a side left P' / right Q'

and a move of the chosen process

$P' \xrightarrow{\alpha} P''$

Defender answers with a move of the other process

$Q' \xrightarrow{\alpha} Q''$

and we continue from (P'', Q'')

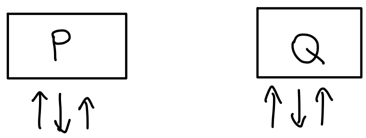
PLAY : sequence of rounds starting from (P, Q)

which is maximal

1. finite with a player who got out of moves
2. infinite

WINNER of a play

1. player who did the last move
2. defender



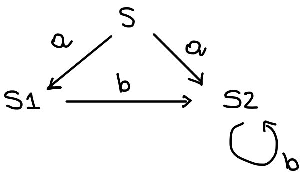
Theorem : Given P, Q processes

- $P \sim Q$ iff the Defender has a winning strategy
- $P \not\sim Q$ iff the Attacker has a winning strategy

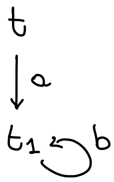
function Attacker (P', Q') ⇝ side left/right & transition

Defender (P', Q') & move of Attacker → move of the other process

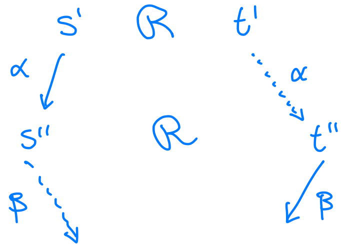
Example



$\sim$



$\mathcal{R} = \{ (s, t) , (s_1, t_1) , (s_2, t_1) \}$



Example

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

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

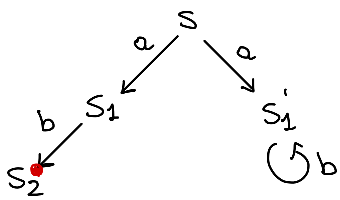
A: $CTM' \xrightarrow{coin} \overline{coffee}.CTM'$

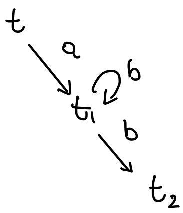
D: $CTM \xrightarrow{coin} \overline{coffee}.CTM + \overline{tea}.CTM$

A: $\overline{coffee}.CTM + \overline{tea}.CTM \xrightarrow{\overline{tea}} CTM$

D: $\overline{coffee}.CTM' \not\xrightarrow{\overline{tea}}$

Example





A: $s \xrightarrow{a} s_1$

D: $t \xrightarrow{a} t_1$

A: $t_1 \xrightarrow{b} t_1$

D: $s_1 \xrightarrow{b} s_2$

A: $t_1 \xrightarrow{b} t_1$

(Defender can win

A: $s \xrightarrow{a} s_1$

D: $t \xrightarrow{a} t_1$

A: $s_1 \xrightarrow{b} s_2$

D: $t_1 \xrightarrow{b} t_2$

* Properties of $\sim$

Bisimulation : relation $R \subseteq Proc \times Proc$ such that if $P \, R \, Q$

(i) if $P \xrightarrow{\alpha} P'$ then $Q \xrightarrow{\alpha} Q'$ and $P' \, R \, Q'$.

(ii) if $Q \xrightarrow{\alpha} Q'$ then $P \xrightarrow{\alpha} P'$ and $P' \, R \, Q'$

$\rightarrow$ P, Q bisimilar ($P \sim Q$) if there exists R bisimulation s.t $P \, R \, Q$

i.e.

$$\sim \; = \; \bigcup \{ R \mid R \text{ is a bisimulation} \}$$

Is it really an equivalence?

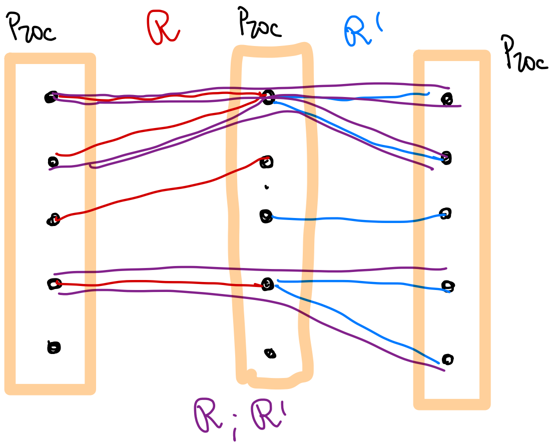
OBSERVATION :

(i) $I = \{ (P, P) \mid P \in Proc \}$ is a bisimulation

(ii) if R is a bisimulation then $R^{-1} = \{ (Q, P) \mid (P, Q) \in R \}$ is a bisimulation

(iii) if R, R' are bisimulation then $R ; R'$ is a bisimulation

" $\{ (P, S) \mid \exists Q \text{ s.t. } P \, R \, Q \text{ and } Q \, R' \, S \}$



(iv) if R_i $i \in I$ are bisimulations then $\bigcup_{i \in I} R_i$ is a bisimulation

proof

(i) let $P \, I \, Q$ then if $P \xrightarrow{\alpha} P'$ then $Q \xrightarrow{\alpha} Q'$ and $P' \, I \, Q'$

$\quad\;\; \overset{\shortparallel}{P}$ $\quad\quad$ $P \xrightarrow{\alpha} P'$ $\quad$ P'

& dual

(ii) obvious

(iii) R, R' bisimulations

let $P\,(R;R')\,S$ and

$\boxed{P \xrightarrow{\alpha} P'}$ we want $S \xrightarrow{\alpha} S'$ and $P'\,(R;R')\,S'$

$\exists Q$ $\boxed{P\,R\,Q}$ & $\boxed{Q\,R'\,S}$

R bisimulation

$\boxed{Q \xrightarrow{\alpha} Q'}$ and $\boxed{P'\,R\,Q'}$ $P'(R;R')S'$

R' bisim.

$\boxed{S \xrightarrow{\alpha} S'}$ and $\boxed{Q'\,R'\,S'}$

$\leadsto$ $R;R'$ is a bisimulation

(iv) R_i $i \in I$ bisimulations

let $P\,(\bigcup_{i\in I} R_i)\,Q$ i.e. $\exists i \in I$ s.t. $P\,R_i\,Q$

and $P \xrightarrow{\alpha} P'$

$Q \xrightarrow{\alpha} Q'$ and $P'\,R_i\,Q'$ $\leadsto$ $P'\,(\bigcup_{i\in I} R_i)\,Q'$

<u>OBSERVATION</u>: Bisimilarity $\sim$ is the largest bisimulation

i.e.

① $\sim$ is a bisimulation ($\sim = \bigcup\{R \mid R \text{ bisimulation}\}$ and use (IV))

② for all R if R is a bisimulation then $R \subseteq \sim$

<u>OBSERVATION</u>: $\sim$ is an equivalence

<u>proof</u>

- reflexive: for all P $P\,I\,P$ thus by (i) $P \sim P$
- symmetric: if $P \sim Q$ then there is R bisimulation s.t. $P\,R\,Q$

  Thus $Q\,R^{-1}\,P$ & by (ii) R^{-1} bisimulation $\Rightarrow$ $Q \sim P$

· transitivity:

if $P \sim Q$ and $Q \sim S$ then $P \mathcal{R} Q$ & $Q \mathcal{R}' S$

with $\mathcal{R}, \mathcal{R}'$ bisimulations

then $P (\mathcal{R};\mathcal{R}') S$ and by (iii) $\mathcal{R};\mathcal{R}'$ is a bisimulation

$\rightsquigarrow$ $P \sim S$ $\square$

EXERCISE: find a bisimulation which is not

- reflexive
- symmetric
- transitive

EXERCISE: show

$P \sim Q$ iff (i) if $P \xrightarrow{\alpha} P'$ then $Q \xrightarrow{\alpha} Q'$ and $P' \sim Q'$

(ii) if $Q \xrightarrow{\alpha} Q'$ then $P \xrightarrow{\alpha} P'$ and $P' \sim Q'$

$\Longrightarrow$

$\sim$ is a bisimulation

$\Longleftarrow$

?

EXERCISE (E) : FINITE CCS (exam)

CCS with no constants

$$P, Q ::= \alpha.P \mid \underbrace{\sum_{i \in I} P_i}_{I \text{ finite}} \mid P|Q \mid P \setminus L \mid P[f]$$

two properties

1. programs always terminate
2. " are finite-state

1. every computation

$$P \xrightarrow{\alpha_1} P_1 \xrightarrow{\alpha_2} P_2 \cdots \longrightarrow \quad \text{is finite}$$

proof idea:

show that if $P_1 \xrightarrow{\alpha_1} P_2 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_{n-1}} P_n$

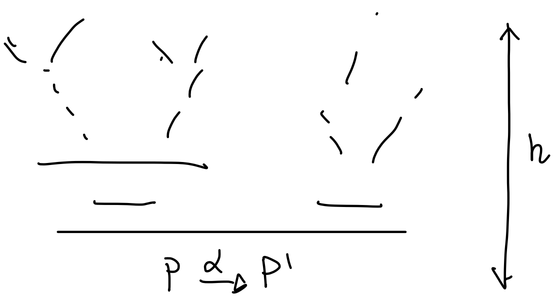
then $n \leq |P_1|$ ← for a reasonable notion of size $|P|$

which in turn follows from

$$P \xrightarrow{\alpha} P' \quad \text{then} \quad |P'| < |P|$$

↑

proof by induction on h



2. every P has a finite number of states

$$\text{states}(P) = \{ P' \mid P \xrightarrow{\alpha_1} P_1 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_n} P' \} \quad \text{is finite}$$

define $\#(P)$ = bound to the number of states of P

$$\#0 = 1$$

$$\#(\alpha.P) = 1 + \#P$$

$$\#\left(\sum_{i\in I} P_i\right) = \sum_{i \in I} \#P_i$$

$$\#(P \mid Q) = (\#P) * (\#Q)$$

$$\#(P \setminus L) = \#P$$

$$\#(P[f]) = \#P$$

prove $\quad |\text{States}(P)| \leq \#P$

$*$ What if sums are not finite?

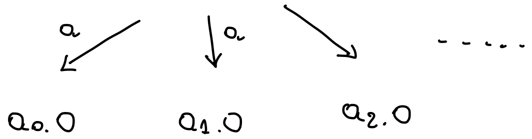
$$P, Q ::= \alpha.P \mid \sum_{i\in I} P_i \mid P \mid Q \mid P\setminus L \mid P[f]$$

possibly infinite

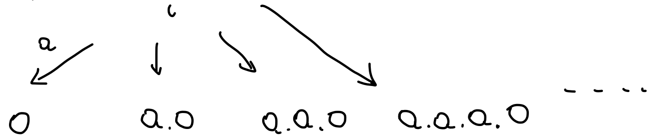
② fails

→ states can be infinite

$$\sum_{i\in\mathbb{N}} a.a_i.0 \qquad\qquad \mathcal{A} = \{a\} \cup \{a_i \mid i \in \mathbb{N}\}$$



$$\sum_{i\in\mathbb{N}} \underbrace{a.\ldots.a}_{i}.0$$



① ? Is termination ensured? YES