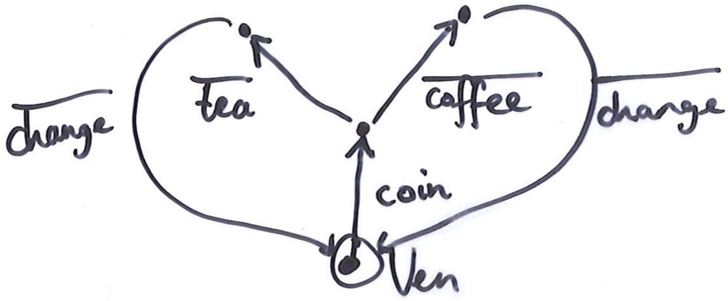
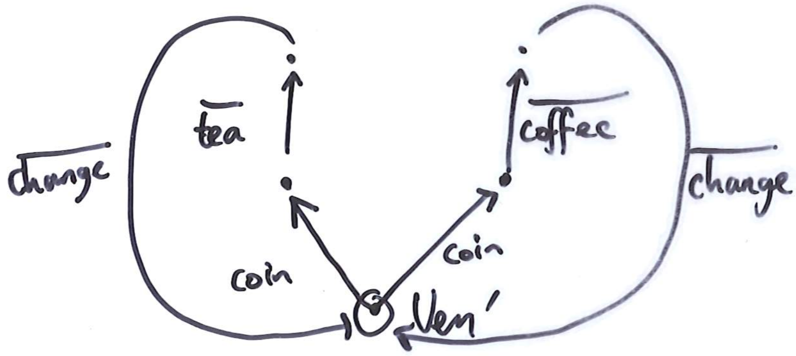
An example (pure) CCS process: The Vending Machine

Ven $\stackrel{def}{=}$



Ven' $\stackrel{def}{=}$



User $\stackrel{def}{=}$ $\overline{coin}$. coffee . change . $\overline{work}$

Specification & correctness → Assertions + logic

e.g. (User || Ven)\{coin, change, coffee} never deadlocks / always outputs 'work'

Specification & correctness → Equivalence

Language equivalences.

* An ∞-trace of a process p is a (possibly infinite) sequence of actions

$$v = (a_1, a_2, a_3, \dots, a_i, a_{i+1}, \dots)$$ (possibly empty)

s.t.

$$p \xrightarrow{a_1} p_1 \xrightarrow{a_2} p_2 \xrightarrow{a_3} \dots \; p_{i-1} \xrightarrow{a_i} p_i \xrightarrow{a_{i+1}} p_{i+1} \longrightarrow \dots$$

* Two processes p_1 and p_2 are ∞-trace-equivalent iff they have the same sets of traces

[v is an ∞-trace of p_1 iff v is an ∞-trace of p_2]

* Are Ven and Ven' ∞-trace-equivalent?

* Are $(Ven \| User) \setminus \{coin, coffee, tea, change\}$ and $(Ven' \| User) \setminus \{coin, coffee, tea, change\}$ ∞-trace-equivalent?

* An ω-trace v of p is maximal if either it is infinite or, if not, the process reached by v is deadlocked

$$v = (a_1, \ldots a_n)$$

$$p \xrightarrow{a_1} p_1 \longrightarrow \cdots p_{n-1} \xrightarrow{a_n} p_n \not\longrightarrow$$

$$(\nexists q, a: p_n \xrightarrow{a} q)$$

* Two processes p_1 and p_2 are completed trace-equivalent iff they have the same sets of maximal traces.

   * Are Ven and Ven' completed trace-equivalent?
   * Are (Ven || User) \ {coin, coffee, tea, change} and (Ven' || User) \ {coin, coffee, tea, change} completed trace-equivalent?

But ...

Bisimulation
– a process equivalence

To

- support equational reasoning
- simplify the verification of
  $p \models A$ (A modal μ-calc, CTL, CTL* ...)

A strong bisimulation is a relation R between states for which

If $p \, R \, q$, then

(i) $\forall \alpha, p'. \quad p \xrightarrow{\alpha} p' \Rightarrow$

$\exists q'. \quad q \xrightarrow{\alpha} q' \;\&\; p' R q'$

(ii) $\forall \alpha, q'. \quad q \xrightarrow{\alpha} q' \Rightarrow$

$\exists p'. \quad p \xrightarrow{\alpha} p' \;\&\; p' R q'$.

Strong bisimilarity equivalence

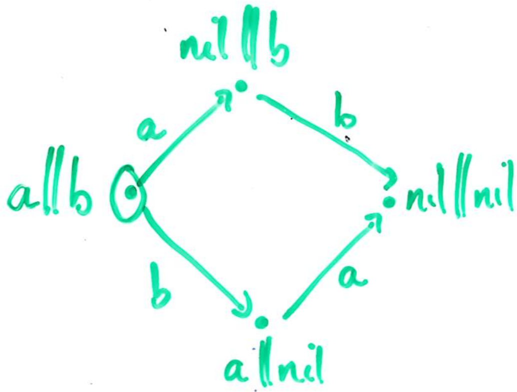
$p \sim q$ iff $p \, R \, q$ for some strong bisimulation R

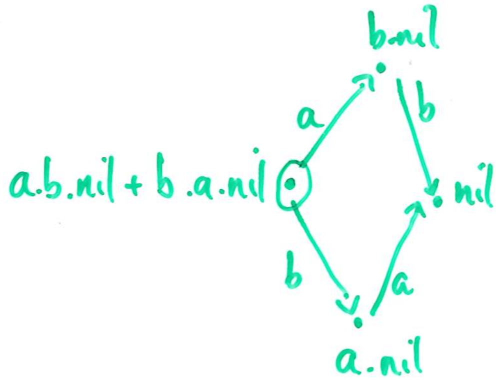
Exhibiting bisimilarity.

To show $p_1 \sim p_2$, must give a relation R s.t R is a bisimulation and $(p_1, p_2) \in R$.

Example

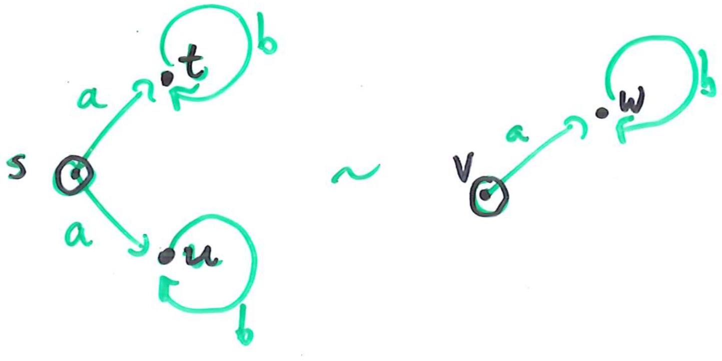
(Note: $a \equiv a.nil$)





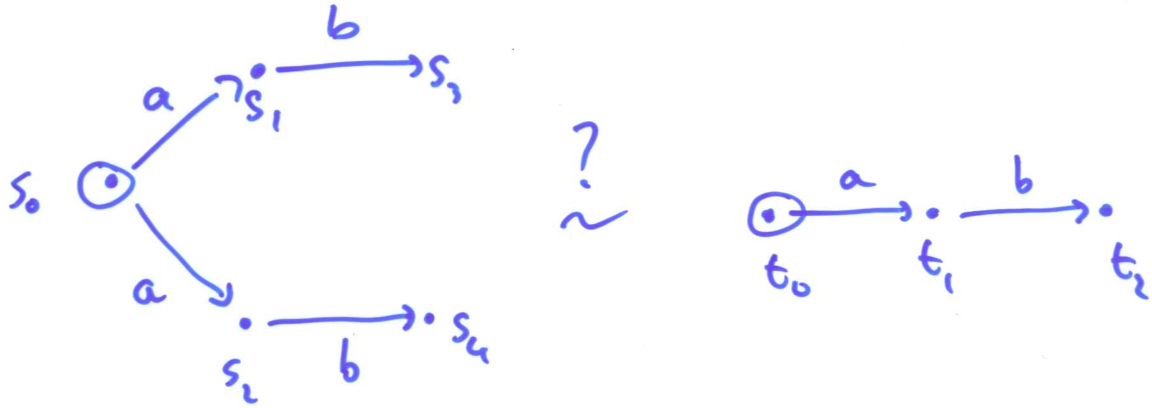
$$R = \{(a\|b,\ a.b + b.a),\ (nil\|b,\ b.nil),\ (a\|nil,\ a.nil),\ (nil\|nil,\ nil)\}$$

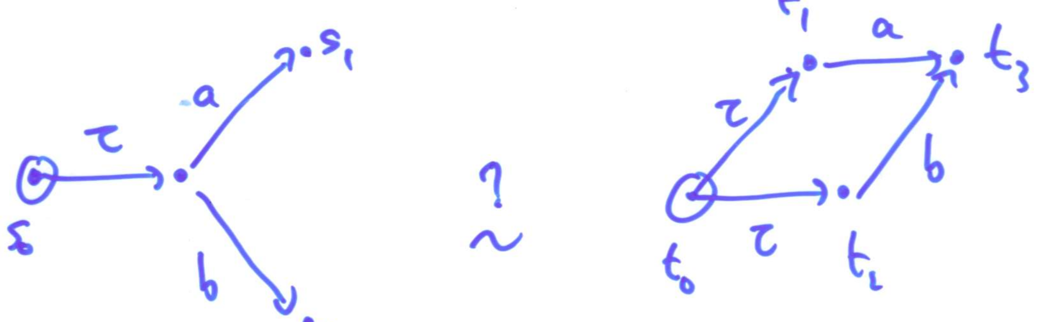
Note: It makes sense to talk about two transition systems being bisimilar – bisimulations between transition systems.



$$R = \{(s,v),\ (t,w),\ (u,w)\}$$

Examples.





If a = b?

If R, S and R_i, $i \in I$, are strong bisimulations, then so are

(1) Id identity relation on set of states of a trans. sys.

(2) R^{op} converse / opposite reln.

(3) $R \circ S$ composition (when trans. systems match up so composition makes sense)

(4) $\bigcup_{i \in I} R_i$ union (assuming the relns. are between same types of states)

(1), (2), (3) $\Rightarrow$ $\sim$ is an equivalence reln, and itself a bisimulation (by (4)).

Equational properties of bisimulation.

$+$ and $\|$ are commutative & associative w.r.t. $\sim$

If $p \sim q$, then

$\alpha.p \sim \alpha.q$,

$p + r \sim q + r$,

$p \| r \sim q \| r$,

$p \setminus L \sim q \setminus L$,

$p[f] \sim q[f]$.

Expansion laws for CCS

$$p \sim \sum \{ \alpha . p' \mid p \xrightarrow{\alpha} p' \}$$

Suppose $p \sim \sum_{i \in I} \alpha_i . p_i$ and $q \sim \sum_{j \in J} \beta_j . q_j$.

$$p \setminus L \sim \sum \{ \alpha_i . (p_i \setminus L) \mid \alpha_i \notin L \}$$

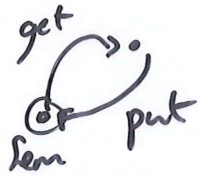
$$p[f] \sim \sum \{ f(\alpha_i) . (p_i[f]) \mid i \in I \}$$

$$p \| q \sim \sum_{i \in I} \alpha_i . (p_i \| q) + \sum_{j \in J} \beta_j (p \| q_j)$$

$$+ \sum \{ \tau . (p_i \| q_j) \mid \alpha_i = \overline{\beta_j} \}$$

Strong bisimilarity & specifications.

An example: Semaphores.



$$Sem \stackrel{def}{=} get \,.\, put \,.\, Sem$$

$$P_1 \stackrel{def}{=} \overline{get} \,.\, a_1 \,.\, a_2 \,.\, \overline{put} \,.\, P_1$$

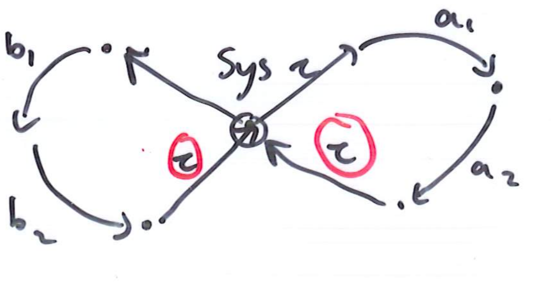
$$P_2 \stackrel{def}{=} \overline{get} \,.\, b_1 \,.\, b_2 \,.\, \overline{put} \,.\, P_2$$

$$Sys \stackrel{def}{=} (Sem \parallel P_1 \parallel P_2) \setminus \{get, put\}$$

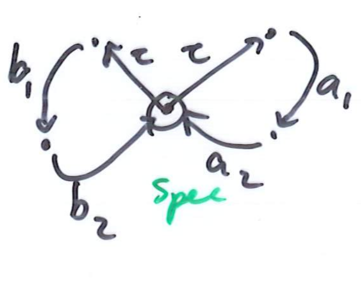
$$Spec \stackrel{def}{=} \begin{array}{l} \tau . a_1 . a_2 . Spec \\ + \\ \tau . b_1 . b_2 . Spec \end{array}$$

? $Sys \overset{?}{\sim} Spec$?

No... τ-actions at non-branching points

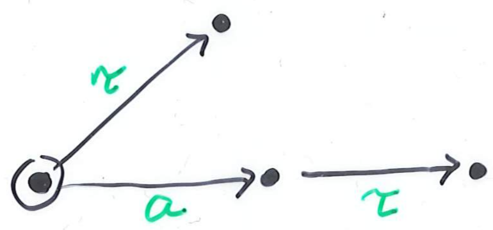


$\not\sim$



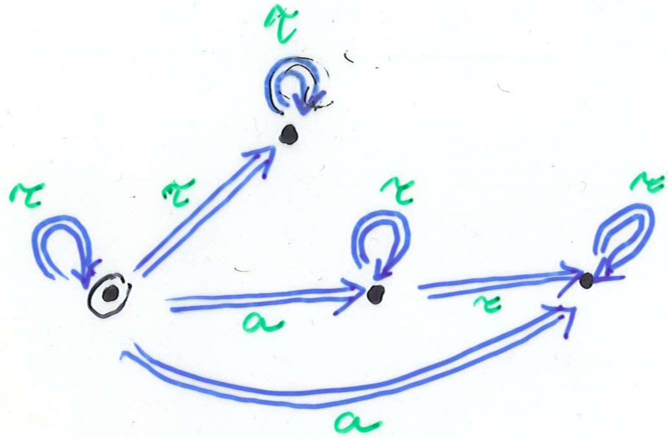
Weak bisimulation

Hiding τ-actions



$$\overset{\tau}{\Longrightarrow} \;=_{def}\; (\xrightarrow{\tau})^*$$

$$\overset{a}{\Longrightarrow} \;=_{def}\; \overset{\tau}{\Longrightarrow}\xrightarrow{a}\overset{\tau}{\Longrightarrow}$$



weak bisimulation is bisim. w.r.t. $\Longrightarrow$

A weak bisimulation is a reln. R s.t.

If $p R q$, then

$$\forall \alpha, p'.\; p \overset{\alpha}{\Longrightarrow} p' \;\Rightarrow\; \exists q'.\; q \overset{\alpha}{\Longrightarrow} q' \;\&\; p' R q'$$

&

$$\forall \alpha, q'.\; q \overset{\alpha}{\Longrightarrow} q' \;\Rightarrow\; \exists p'.\; p \overset{\alpha}{\Longrightarrow} p' \;\&\; p' R q'.$$

A congruence but for sum!

$\rightsquigarrow$ observation congruence.