Chapter 5: Equivalences over processes

- **Observation equivalence**
  - i are considered invisible
  - concept of a weak bisimulation
- **Observation congruence**
- **Weaker equivalence**
  - Trace equivalence
- **Preorders**
  - Simulation
  - Safety-preorder and associated safety-equivalence
- **Branching bisimulation** (liveness properties preserving)

Observation equivalence and congruence are explained together with strong bisimulation in :

Robin Milner. Communication and Concurrency. Prentice Hall International Series in Computer Science, 1989.

Strong bisimulation ~

A relation $R \subseteq S \times S$ is a **strong bisimulation** iff:

If $<P, Q> \in R$ then, for all $a \in A$,

(i) whenever $P \xrightarrow{a} P'$ then $\exists Q' \bullet Q \xrightarrow{a} Q'$ and $<P', Q'> \in R$;

(ii) whenever $Q \xrightarrow{a} Q'$ then $\exists P' \bullet P \xrightarrow{a} P'$ and $<P', Q'> \in R$

P ~ Q if $\exists$ a strong bisimulation R such that $<P, Q> \in R$

~ is a congruence in LOTOS

Many interesting laws and expansion theorems exist for ~

P ~ Q can be checked in polynomial time over closed and finite processes

However:

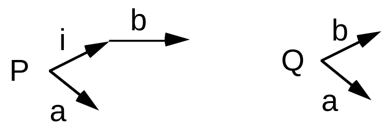
~ is deficient in a vital respect: it treats the internal action i on the same basis as all other actions, and properties which we would expect to hold if i is unobservable, such as a; i; P ~ a; P, **do not hold**

Unobservability of i

What does it mean for i to be silent, or unobservable ?

A first answer might be that two processes should be equivalent if they become strongly congruent when the i-actions are excised from their derivation trees.

Under this proposal we would equate P and Q below:



But, this leads to difficulty.

Unobservability of i means that i is uncontrollable by the environment.

So P can perform i autonomously and thus forego its ability to perform a

Q however preserves this ability

So i, though unobservable directly, can affect the observability of visible actions.

Towards an observation equivalence

We therefore seek an equivalence (denoted ≈) with the following property:

P and Q are equivalent iff
for all sequence $\sigma \in L^*$, **each** σ-descendant of P is equivalent to **some** σ-descendant of Q,
and conversely

Note that L = A — {i}

If $\sigma = a1.a2\ldots an \in A^*$ (it is defined on A* even if used on L* above)

A σ-descendant of P is any P' such that $P \overset{\sigma}{\Rightarrow} P'$

that is $P\ (\overset{i}{\rightarrow})^* \overset{a1}{\rightarrow} (\overset{i}{\rightarrow})^* \ldots (\overset{i}{\rightarrow})^* \overset{an}{\rightarrow} (\overset{i}{\rightarrow})^*\ P'$

So we are looking for the largest relation ≈ that satisfies:

P ≈ Q iff, for all $\sigma \in$ **L***,

(i) whenever $P \overset{\sigma}{\Rightarrow} P'$ then $\exists\, Q' \bullet Q \overset{\sigma}{\Rightarrow} Q'$ and $P' \approx Q'$;

(ii) whenever $Q \overset{\sigma}{\Rightarrow} Q'$ then $\exists\, P' \bullet P \overset{\sigma}{\Rightarrow} P'$ and $P' \approx Q'$

Weak bisimulation

It is not necessary to consider all $\sigma \in L^*$:

Considering **observable** sequences of **length** $\leq$ **1** is enough, i.e. $\sigma \in \mathbf{L} \cup \{\varepsilon\} = \mathbf{L} \cup \{i^*\}$

(ε is the empty sequence)

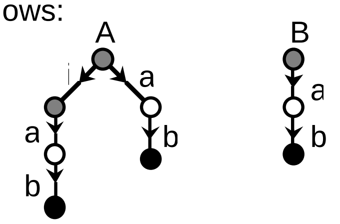
Definition

Let G be a function over binary relations $R \subseteq S \times S$ defined as follows:

$\langle P, Q\rangle \in G(R)$ iff, for all $\mathbf{a} \in \mathbf{L} \cup \{\varepsilon\}$,

(i) whenever $P \overset{a}{\Rightarrow} P'$ then $\exists Q' \bullet Q \overset{a}{\Rightarrow} Q'$ and $\langle P', Q'\rangle \in R$;

(ii) whenever $Q \overset{a}{\Rightarrow} Q'$ then $\exists P' \bullet P \overset{a}{\Rightarrow} P'$ and $\langle P', Q'\rangle \in R$



An example of a weak bisimulation:

R is composed of all the pairs of states of the same colour

Definition

$R \subseteq S \times S$ is a weak bisimulation iff $R \subseteq G(R)$

Observation equivalence

Definition

P and Q are observation equivalent (or weakly bisimilar), written $P \approx Q$,

if **there exists** a weak bisimulation R such that $\langle P, Q \rangle \in R$.

This may be equivalently expressed as follows: $\approx \; = \bigcup \{R \mid R \text{ is a weak bisimulation}\}$

Properties:

$\approx$ is the largest weak bisimulation

$\approx$ is the largest fixed point of G and is an equivalence

$\approx$ is weaker than $\sim$

So $\approx$ can be defined as **the largest relation** $\approx$ that satisfies the following property:

$P \approx Q$ iff, for all $a \in L \cup \{\varepsilon\}$,

(i) whenever $P \stackrel{a}{\Rightarrow} P'$ then $\exists\, Q' \bullet Q \stackrel{a}{\Rightarrow} Q'$ and $P' \approx Q'$;

(ii) whenever $Q \stackrel{a}{\Rightarrow} Q'$ then $\exists\, P' \bullet P \stackrel{a}{\Rightarrow} P'$ and $P' \approx Q'$

Simpler definition of a weak bisimulation

A relation $R \subseteq S \times S$ is a weak bisimulation iff:

If $\langle P, Q \rangle \in R$ **then**, for all $a \in L \cup \{\varepsilon\}$

(i) whenever $P \overset{a}{\Rightarrow} P'$ then $\exists\, Q' \bullet Q \overset{a}{\Rightarrow} Q'$ and $\langle P', Q' \rangle \in R$

(ii) whenever $Q \overset{a}{\Rightarrow} Q'$ then $\exists\, P' \bullet P \overset{a}{\Rightarrow} P'$ and $\langle P', Q' \rangle \in R$

When the two behaviour expressions are **closed** and the associated LTS are **finite-state**, there are algorithms to prove the observation equivalence of the LTS in polynomial time (with respect to the size of the LTS, not the size of the LOTOS expression).

Equational properties of ≈

All the laws for ~ are valid laws for ≈

Additional laws:

i; P	≈ P
exit >> P	≈ P
P >> exit	≈ P
P >> stop	≈ P ||| stop
P [] i; P	≈ P
a; (P [] i; Q) [] a; Q	≈ a; (P [] i; Q)

They can all be proved by exhibiting an appropriate weak bisimulation

Non congruence of ≈

Let C [•] be a LOTOS context of the following forms:

g; [•]

[•] |[Γ]| B or B |[Γ]| [•]

[•] >> B or B >> [•]

[•] [> B

hide Γ in [•]

[E] -> [•]

[•] [S] (relabelling)

let … in [•]

then if P ≈ Q then C [P] ≈ C [Q]

However the property is not valid in the following contexts:

[•] [] B or B [] [•] or choice … [] [•]

B [> [•]

and recursion contexts

Observation congruence

We must now tackle the difficulty that $\approx$ is not a congruence.
We look for a congruence which is as close to $\approx$ as possible.

The idea is to strenghten $\approx$ to get congruence in choice and right-disabling contexts:

Definition

P and Q are **observation congruent**, noted $P \approxeq Q$, iff for all **a** $\in$ **A = L** $\cup$ **{i}**,

(i) whenever $P \overset{a}{\Rightarrow} P'$ then $\exists\, Q' \bullet Q \overset{a}{\Rightarrow} Q'$ and $P' \approx Q'$

(ii) whenever $Q \overset{a}{\Rightarrow} Q'$ then $\exists\, P' \bullet P \overset{a}{\Rightarrow} P'$ and $P' \approx Q'$

Instead of L $\cup$ {ε} = L $\cup$ {i*}
Thus an initial i action in P (or Q) must be matched by at least an i-action of the other

$\approxeq$ is defined in terms of $\approx$
Difference in initial actions only

Could be $\overset{a}{\rightarrow}$

Congruence of $\underset{\sim}{\approx}$ and other properties

Let C [•] be a LOTOS context of the following forms:

[•] [] B or B [] [•] or choice … [] [•]

B [> [•]

then if P $\underset{\sim}{\approx}$ Q then C [P] $\underset{\sim}{\approx}$ C [Q]

Moreover, $\underset{\sim}{\approx}$ is preserved in recursion contexts. That is
if P (X) $\underset{\sim}{\approx}$ Q (X) for all substitutions of X, then
X where X := P(X) and Y where Y := Q(Y) are observation congruent

Other properties of $\underline{\approx}$

Other properties of $\underline{\approx}$

If $P \approx Q$ then $a; P \underline{\approx} a; Q$

If $P \approx Q$ and P and Q are both stable, then $P \underline{\approx} Q$

P is stable iff $\neg (P \xrightarrow{i})$

$P \approx Q$ iff ($P \underline{\approx} Q$ or $P \underline{\approx} i; Q$ or $Q \underline{\approx} i; P$)

Laws for $\approx$ that are not valid for $\underline{\approx}$

$i; P \underline{\approx} P$ does not hold	but $a; i; P \underline{\approx} a; P$ holds
exit >> $P \underline{\approx} P$ does not hold	but exit >> $P \underline{\approx} i; P$ holds
P [] $i; P \underline{\approx} P$ does not hold	but P [] $i; P \underline{\approx} i; P$ holds

A very weak notion of equivalence - The trace equivalence

We have studied two main equivalences: strong and weak bisimilarity.

(Observation congruence is a third, but closely allied to weak bisimilarity)

We shall now study coarser (or more generous) equivalences, which of course abstract from internal actions as well.

Trace equivalence

This is the main equivalence studied in classical automata theory

P and Q are trace equivalent, noted P $\approx_{tr}$ Q iff, for all $\sigma \in L^*$, P $\overset{\sigma}{\Rightarrow}$ iff Q $\overset{\sigma}{\Rightarrow}$

That is Tr (P) = Tr (Q) where Tr (P) = { σ | P $\overset{\sigma}{\Rightarrow}$ }

Weak traces (no i)

It is a congruence

It is weaker than $\approx$

It satisfies the laws: a; (P [] Q) $\approx_{tr}$ a; P [] a; Q

(P [] Q) |[Γ]| R $\approx_{tr}$ (P |[Γ]| R) [] (Q |[Γ]| R)

Preorder relations over processes

Equivalence relations are often not adequate to compare processes at different levels of abstractions (e.g. a protocol and a service).

Preorders may be more appropriate.

An **equivalence** relation is a **reflexive**, **symmetric** and **transitive** relation

A **preorder** relation is a **reflexive** and **transitive** relation

If R is a preorder, then $R \cap R^{-1}$ is an equivalence

Example of a preorder:

- **The trace preorder (or trace inclusion** relation):

  $P \leq_{tr} Q$ iff ($P \overset{\sigma}{\Rightarrow}$ implies $Q \overset{\sigma}{\Rightarrow}$) iff $Tr(P) \subseteq Tr(Q)$

- **Trace equivalence**

  $P \approx_{tr} Q$ iff $P \leq_{tr} Q \wedge Q \leq_{tr} P$

Simulation versus bisimulation

There are **no** preorders associated with strong and weak bisimulations.
But there exists a concept of a **simulation**.
However, even if it sounds (and looks) like a "semi-bisimulation", it is **not**.

Let us first recall the definition of a bisimulation **over an alphabet** Λ.

A relation $R \subseteq S \times S$ is a **bisimulation** iff:

If $<P, Q> \in R$ then, for all $\lambda \in \Lambda$,

(i) whenever $P \xrightarrow{\lambda} P'$ then $\exists\, Q' \bullet Q \xrightarrow{\lambda} Q'$ and $<P', Q'> \in R$

(ii) whenever $Q \xrightarrow{\lambda} Q'$ then $\exists\, P' \bullet P \xrightarrow{\lambda} P'$ and $<P', Q'> \in R$

A relation $R \subseteq S \times S$ is a **simulation** iff:

If $<P, Q> \in R$ then, for all $\lambda \in \Lambda$,

whenever $P \xrightarrow{\lambda} P'$ then $\exists\, Q' \bullet Q \xrightarrow{\lambda} Q'$ and $<P', Q'> \in R$

Strong (bi)simulations

When Λ = A = L $\cup$ {i}

This leads to the **strong bisimulation**, and to ~ as the largest strong bisimulation

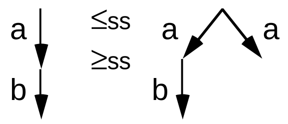
Similarly, we can define the largest **strong simulation** $\leq_{ss}$

$$\begin{array}{ccc} \mathbf{P} & \leq_{ss} & \mathbf{Q} \\ \lambda\downarrow & & \downarrow\lambda \\ \mathbf{P'} & \leq_{ss} & \mathbf{Q'} \end{array}$$

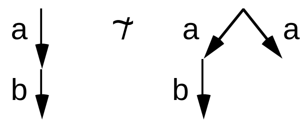
However $\leq_{ss} \cap \geq_{ss}$ is not equal to ~

In fact ~ is stronger than $\leq_{ss} \cap \geq_{ss}$

Example:



But:



Weak bisimulation versus safety equivalence

When Λ = {i*} $\cup$ {i*ai* | a $\in$ L}

This leads to the **weak bisimulation**, and to $\approx$ as the largest weak bisimulation

Similarly, we can define the largest **weak simulation** $\leq_s$

This preorder is also called the **safety-preorder.**

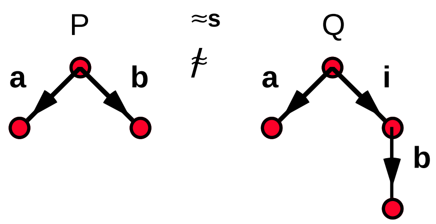
$$\begin{tikzcd} P \arrow[r, phantom, "\leq_s"] \arrow[d, "i^*"'] & Q \arrow[d, "i^*"] \\ P' \arrow[r, phantom, "\leq_s"] & Q' \end{tikzcd} \qquad \begin{tikzcd} P \arrow[r, phantom, "\leq_s"] \arrow[d, "i^*ai^*"'] & Q \arrow[d, "i^*ai^*"] \\ P' \arrow[r, phantom, "\leq_s"] & Q' \end{tikzcd}$$

The safety equivalence is **NOT** defined as a bisimulation but as follows:

P and Q are **safety-equivalent**, written P $\approx_s$ Q, iff P $\leq_s$ Q and Q $\leq_s$ P

$\approx_s$ is **not** equal to $\approx$

$\approx_s$ is weaker than $\approx$



The safety equivalence

The safety preorder is such that

if P $\leq_s$ Q then P satisfies at least all the safety properties of Q

(expressible in BSL: Branching time Safety Logic)

Intuitively, safety properties are properties stating 'nothing bad will happen'.

For example : mutual exclusion

Therefore the safety equivalence $\approx_s$ exactly characterizes the safety properties of systems:

Two LTS are **safety-equivalent** iff **they verify the same safety properties (expressible in BSL)**

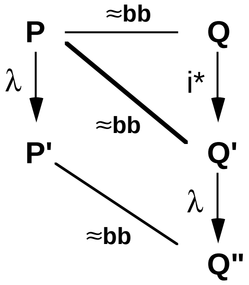
$\approx_s$ is stronger than the $\approx_{tr}$ but weaker than $\approx$

Summary

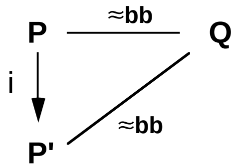
Λ	Simulation	Bisimulation	Simul. $\cap$ Simul.$^{-1}$
a and i	$\leq_{ss}$	$\sim$ **strong bisim.**	$\leq_{ss} \cap \geq_{ss}$
i* and i*ai*	$\leq_s$ **safety preorder**	$\approx$ **weak bisim.**	$\approx_s$ **safety equiv.**

$\sim \longrightarrow \approx \longrightarrow \approx_s$

Branching bisimulation



or



and conversely

Note that λ is any action, including i

Branching bisimulation is of course **weaker than strong bisimulation**

due to the i* transition which allows the removal of some i in a sequence.

For example: i; a; stop ≈bb a; stop

It is also **stronger than weak bisimulation** (see next slide)

Branching bisimulation : an equivalence that preserves liveness properties

P and Q are branching bisimilar, written $\approx_{bb}$, iff

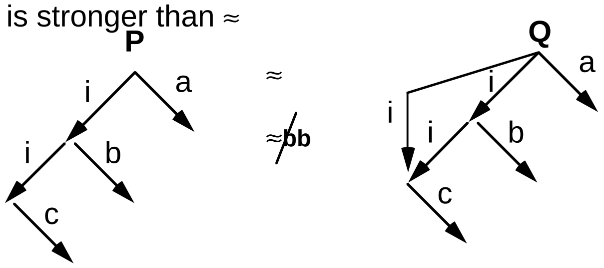
there exists a branching bisimulation R such that $\langle P, Q\rangle \in R$

In absence of divergences, this equivalence **preserves the liveness and safety properties**:

If two LTS are branching bisimilar, then **they verify the same properties** expressible in CTL* (a branching time temporal logic without next operator)

Intuitively, liveness properties are properties stating 'something good will happen'.

$\approx_{bb}$ is stronger than $\approx$



$\approx_{bb}$ is more sensitive to the branching structure than $\approx$

Consider the liveness property **"it is inevitable to reach a state where b is enabled before performing c"**

P satisfies it whereas Q does not

Conclusion

Many equivalences abstract away from internal actions:

- The weak bisimulation equivalence $\approx$ (and associated observation congruence $\underline{\approx}$)
- The trace equivalence $\approx_{tr}$
- The safety equivalence $\approx_{s}$
- The branching bisimulation $\approx_{bb}$

$$\sim \;\longrightarrow\; \approx_{bb} \;\longrightarrow\; \approx \;\longrightarrow\; \approx_{s} \;\longrightarrow\; \approx_{tr}$$

$\sim$: Preserves all properties and divergences

$\approx_{bb}$: Preserves CTL* properties if no divergence; loses divergences

$\approx_{s}$: Preserves BSL properties

For some of them, some preorders exist:

- The trace preorder $\leq_{tr}$
- The safety preorder $\leq_{s}$