Concepts of Concurrent Computation

Spring 2015

Lecture 11: Bisimulations

Sebastian Nanz
Chris Poskitt

Chair of Software Engineering

ETH zürich

Strong Bisimulations

Behavioral equivalence

- Goal: Express the notion that two concurrent systems "behave in the same way"
- We are not interested in syntactical equivalence, but only in the fact that the processes have the same behavior
- Main idea: two processes are behaviorally equivalent if and only if an external observer cannot tell them apart
- Bisimulation [Park 1980]: Two processes are equivalent if they have the same traces and the states that they reach are also equivalent

Strong bisimilarity

- Let be an LTS $(Proc, Act, \{ \xrightarrow{\alpha} \mid \alpha \in Act\})$
- Strong Bisimulation
  - A binary relation $R \subseteq Proc \times Proc$ is a strong bisimulation iff whenever $(P, Q) \in R$ then for each $\alpha \in Act$
    - if $P \xrightarrow{\alpha} P'$ then $Q \xrightarrow{\alpha} Q'$ for some Q' such that $(P', Q') \in R$
    - if $Q \xrightarrow{\alpha} Q'$ then $P \xrightarrow{\alpha} P'$ for some P' such that $(P', Q') \in R$
- Strong Bisimilarity
  - Two processes $P_1, P_2 \in Proc$ are strongly bisimilar ($P_1 \sim P_2$) if and only if there exists a strong bisimulation R such that $(P_1, P_2) \in R$

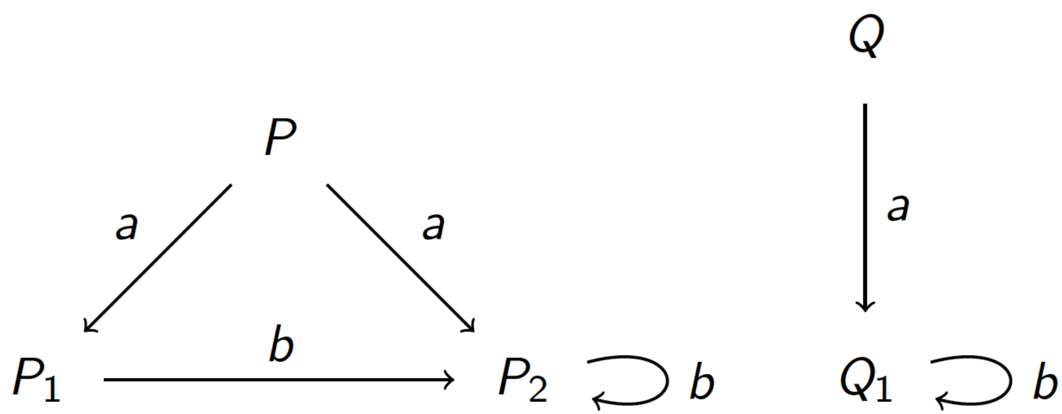
$$\sim \; = \; \cup\{R \mid R \text{ is a strong bisimulation}\}$$

Strong bisimilarity of CCS processes

- The concept of strong bisimilarity is defined for LTS
- The semantics of CCS is given in terms of LTS, whose states are CCS processes
- Thus, the definition also applies to CCS processes
  - Two processes are bisimilar if there is a concrete strong bisimulation relation that relates them
  - To show that two processes are bisimilar it suffices to exhibit such concrete relation

Example: Strong bisimulation

- Consider the processes P and Q with the following behavior:



- We claim that they are bisimilar

Example: Strong bisimulation

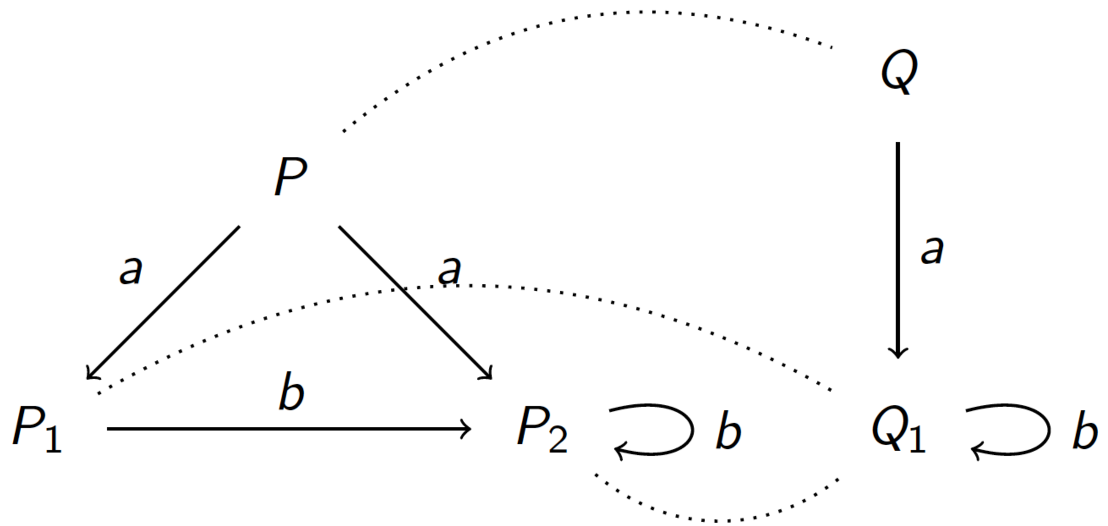
- To show our claim we exhibit the following strong bisimulation relation:

$$\mathcal{R} = \{(P, Q), (P_1, Q_1), (P_2, Q_1)\}$$

- $(P, Q) \in \mathcal{R}$
- $\mathcal{R}$ is a bisimulation:
    - For each pair of states in $\mathcal{R}$, all possible transitions from the first can be matched by corresponding transitions from the second
    - For each pair of states in $\mathcal{R}$, all possible transitions from the second can be matched by corresponding transitions from the first

Example: Strong bisimulation

- Graphically, we show $\mathcal{R}$ with dotted lines



- Now it is easy to see that
  - for each pair of states in $\mathcal{R}$, all possible transitions from the first can be matched by corresponding transitions from the second
  - for each pair of states in $\mathcal{R}$, all possible transitions from the second can be matched by corresponding transitions from the first

Exercise: Strong bisimulation

- Consider the processes

$$
\begin{aligned}
\mathrm{P} &\stackrel{\text{def}}{=} a.(b.0 + c.0) \\
\mathrm{Q} &\stackrel{\text{def}}{=} a.b.0 + a.c.0
\end{aligned}
$$

and show that $P \not\sim Q$

Weak Bisimulations

Refinement

- Further use of bisimulations: refinement of systems
- We would like to state that two processes *Spec* and *Imp* behave the same, where *Imp* specifies the computation in greater detail
- This is not possible with strong bisimulations, as every action needs to be matched in equivalent processes
- Key to a weaker notion of equivalence: abstract from internal actions
- Idea: an external observer who focuses on visible actions but ignores all internal behavior

Weak bisimulation (1)

- We write $P \stackrel{\alpha}{\Longrightarrow} Q$ if P can reach Q via an α-transition, preceeded and followed by zero or more τ-transitions:

$$P \xrightarrow{\tau}{}^{*} P' \xrightarrow{\alpha} P'' \xrightarrow{\tau}{}^{*} Q$$

- Furthermore, $P \stackrel{\tau}{\Longrightarrow} Q$ holds if $P = Q$
- This definition allows us to “erase” sequences of τ-transitions in a new definition of behavioral equivalence: weak bisimulation

Weak bisimulation (2)

- Let $(Proc, Act, \{ \xrightarrow{\alpha} \mid \alpha \in Act\})$ be an LTS.
- Weak bisimulation
  A binary relation $\mathcal{R} \subseteq Proc \times Proc$ is a weak bisimulation if $(P, Q) \in \mathcal{R}$ implies for all $\alpha \in Act$
  - if $P \xrightarrow{\alpha} P'$ then $Q \overset{\alpha}{\Longrightarrow} Q'$ for some Q' such that $(P', Q') \in \mathcal{R}$
  - if $Q \xrightarrow{\alpha} Q'$ then $P \overset{\alpha}{\Longrightarrow} P'$ for some P' such that $(P', Q') \in \mathcal{R}$
- Weak bisimilarity
  Two processes P and Q are weakly bisimilar, $P \approx Q$, if there is a weak bisimulation $\mathcal{R}$ such that $(P, Q) \in \mathcal{R}$

Example: Weak bisimulation

- Consider the following CCS processes:

  $P_0 = a.P_0 + b.P_1 + \tau.P_1$

  $P_1 = a.P_1 + \tau.P_2$

  $P_2 = b.P_0$

  $Q_1 = a.Q_1 + \tau.Q_2$

  $Q_2 = b.Q_1$

- Is $P_0 \approx Q_1$?

  Yes, since $\{(P_0, Q_1), (P_1, Q_1), (P_2, Q_2)\}$ is a weak bisimulation.

Value Passing

Value-passing CCS

- For modeling, it is often helpful to be able to express that values can be passed when processes are synchronizing
- For example, a buffer of size one can be modeled as follows:

  $Buffer = append(x).\overline{remove}(x).Buffer$
- The value transmitted over channel *append* is bound to variable *x*
- For example, if the value is *d* then we get in the next step:

  $\overline{\mathrm{remove}}(\mathrm{d}).\mathrm{Buffer}$

Example: Producers-consumers in CCS

- Buffer of size two

$$Buffer = append(x).Buffer1(x)$$

$$Buffer1(x) = \overline{remove}(x).Buffer + append(y).Buffer2(x, y)$$

$$Buffer2(x, y) = \overline{remove}(x).Buffer1(y)$$

- Producers and Consumers

$$Producer(x) = \overline{append}(x).Producer(x + 1)$$

$$Consumer = remove(x).Consumer$$

- Full system

$$(Producer(0) \mid Buffer \mid Consumer) \setminus \{append, remove\}$$

Superfluity of value-passing

- It can be shown that the original calculus is just as expressive as the value-passing calculus
- We demonstrate the main argument of this proof by example: we translate a process with value-passing into one without

  $Buffer = append(x).Buffer1(x)$

  $Buffer1(x) = \overline{remove}(x).Buffer$

- Fix a set of values, e.g. Booleans, to be stored in the buffer; then the following process is equivalent:

  $Buffer = append_0.Buffer1_0 + append_1.Buffer1_1$

  $Buffer1_0 = \overline{remove_0}.Buffer$

  $Buffer1_1 = \overline{remove_1}.Buffer$

- In general, this requires infinite summations and infinitely many equations

The π-calculus

Limitations of CCS

- In CCS all communication links are static
- This leads to problems when trying to model dynamically changing systems
- Example: a server *S* increments every value it receives

  $S = a(x).\overline{a}(x + 1).0 \mid S$
- If processes try to access the server, the responses may not be correctly matched

  $\overline{a}(3).a(x).P(x) \mid \overline{a}(5).a(y).Q(y) \mid S \longrightarrow \ \ldots \longrightarrow P(6) \mid Q(4) \mid \ldots$

Names

- To remove the limitation of CCS, the π-calculus allows values to include channel names
- The incrementation server can be reprogrammed as

  $S = a(x, b).\overline{b}\langle x + 1\rangle.0 \mid S$

- Note the use of angle brackets ⟨ ... ⟩ to denote the output tuple

Restriction

- The restriction operator $P \setminus L$ of CCS is overly restrictive
- We would also like that channels can be passed outside their original scope
- In the π-calculus, the restriction (or creation) operator is written

  $(new\ x)\ P$

  and creates a new name x with scope P
- The name can however be communicated outside its original scope (scope extrusion), changing the scope of the binder:

  $(new\ y)(\ \overline{x}\langle y\rangle \mid y(v).P(v)\ ) \quad \mid \quad x(u).\overline{u}\langle 2\rangle$

  $\longrightarrow (new\ y)\ (\ y(v).P(v) \mid \overline{y}\langle 2\rangle)$

  $\longrightarrow (new\ y)(\ P(2)\ )$

Syntax of the π-calculus

- Action prefixes

$\pi ::= x(y)$ — receive y along x

$\quad |\ \overline{x}\langle y\rangle$ — send y along x

$\quad |\ \tau$ — unobservable action

- Process syntax

$P ::= \sum \pi_i.P_i$ — summation

$\quad |\ P_1 \mid P_2$ — parallel

$\quad |\ (new\ x)\ P$ — new name creation

$\quad |\ !P$ — replication

Structural congruence

- Two expressions are structurally congruent, written $P \equiv Q$, if they can be transformed into the other using the following rules:
  1. Renaming of bound variables (alpha-conversion)
  2. Reordering of terms in a summation
  3. Associativity and commutativity of parallel
     $P \mid 0 \equiv P$
  4. $(new\ x)\ (P \mid Q) \equiv P \mid (new\ x)\ Q$ if x not free in P
     $(new\ x)\ 0 \equiv 0$
     $(new\ x)\ (new\ y)\ P \equiv (new\ y)\ (new\ x)\ P$
  5. $!P \equiv P \mid !P$

Reaction semantics

TAU $\tau.P + M \to P$

REACT $x(y).P + M \mid \overline{x}\langle z\rangle.Q + N \to P[z/y] \mid Q$

PAR $$\frac{P \to P'}{P \mid Q \to P' \mid Q}$$

RES $$\frac{P \to P'}{(\text{new } x)\ P \to (\text{new } x)\ P'}$$

STRUCT $$\frac{Q \equiv P \quad P \to P' \quad P' \equiv Q'}{Q \to Q'}$$

Equivalence

- An appropriate notion of process equivalence $P \simeq Q$ for the π-calculus:
  - preserves the equivalence in all contexts
  - means that we can make the same observations for P and for Q
  - implies that P and Q mimic their reaction steps
- The equivalence can be developed formally as in the case of CCS, with some complications due to the reaction semantics (other than in the labeled semantics, the observables are not exposed by the transitions)

Expressiveness

- Small calculus, but very expressive:
  - encoding of data structures
  - encoding functions as processes
  - encoding higher-order behavior
  - encoding polyadic with monadic communication
  - ...

Conclusion

- Many “fundamental” models of concurrency: CCS, π-calculus, CSP (Communicating Sequential Processes)
- The reason for this is that there are many forms of concurrency one might like to describe
- The π-calculus takes mobility into account, which is not the case for CCS and CSP