Labelled Transition Systems

Luís Soares Barbosa

Architecture & Calculi Course Unit

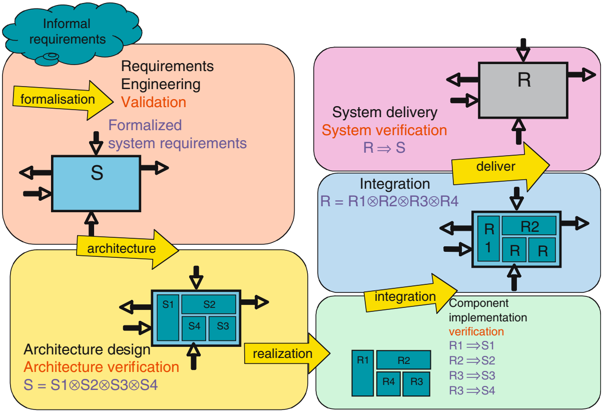
Universidade do Minho

Introduction to the Architecture & Calculi course unit

Software development as one of the most complex but at the same time most effective tasks in the engineering of innovative applications:

- Software drives innovation in many application domains
- Appropriate software provides engineering solutions that can calculate results, communicate messages, control devices, animate and reason about all kinds of information
- Actually software is becoming everyware ...

Introduction to the Architecture & Calculi course unit



Informal requirements

formalisation

Requirements Engineering

Validation

Formalized system requirements

S

architecture

S1 S2 S4 S3

Architecture design

Architecture verification

S = S1⊗S2⊗S3⊗S4

realization

R1 R2 R4 R3

Component implementation

verification

R1 ⟹S1

R2 ⟹S2

R3 ⟹S3

R3 ⟹S4

integration

Integration

R = R1⊗R2⊗R3⊗R4

R 1 R2 R R

deliver

System delivery

System verification

R ⟹ S

R

Software Engineering (illustration from [Broy, 2007])

Introduction to the Architecture & Calculi course unit

So, ... yet another module in the MFES profile?

Models and analysis of reactive systems

characterised by

- a methodological shift: an architectural perspective (compositionality; interaction; focus on observable behaviour)
- a focus: on reactive systems — nondeterministic, probabilistic, timed, cyber-physical

Introduction to the Architecture & Calculi course unit

Reactive system

system that computes by reacting to stimuli from its environment along its overall computation

- in contrast to sequential systems whose meaning is defined by the results of finite computations, the behaviour of reactive systems is mainly determined by interaction and mobility of non-terminating processes, evolving concurrently.
- observation $\equiv$ interaction
- behaviour $\equiv$ a structured record of interactions

Labelled Transition System

Definition

A LTS over a set N of names is a tuple $\langle S, N, \downarrow, \longrightarrow\rangle$ where

- $S = \{s_0, s_1, s_2, ...\}$ is a set of states
- $\downarrow \subseteq S$ is the set of terminating or final states

$$\downarrow s \;\equiv\; s \in \downarrow$$

- $\longrightarrow \subseteq S \times N \times S$ is the transition relation, often given as an N-indexed family of binary relations

$$s \xrightarrow{a} s' \;\equiv\; \langle s', a, s\rangle \in \longrightarrow$$

Labelled Transition System

Morphism

A morphism relating two LTS over N, $\langle S, N, \downarrow, \longrightarrow \rangle$ and $\langle S', N, \downarrow', \longrightarrow' \rangle$, is a function $h : S \longrightarrow S'$ st

$$\begin{array}{rcl} s \xrightarrow{a} s' & \Rightarrow & h\ s \xrightarrow{a}{}' \ h\ s' \\ s \downarrow & \Rightarrow & h\ s \downarrow' \end{array}$$

$\boxed{\text{morphisms preserve transitions and termination}}$

Labelled Transition System

System

Given a LTS $\langle S, N, \downarrow, \longrightarrow \rangle$, each state $s \in S$ determines a system over all states reachable from s and the corresponding restrictions of $\longrightarrow$ and $\downarrow$.

LTS classification

- deterministic
- non deterministic
- finite
- finitely branching
- image finite
- ...

Reachability

Definition

The reachability relation, $\longrightarrow^* \subseteq S \times N^* \times S$, is defined inductively

- $s \xrightarrow{\epsilon}^* s$ for each $s \in S$, where $\epsilon \in N^*$ denotes the empty word;
- if $s \xrightarrow{a} s''$ and $s'' \xrightarrow{\sigma}^* s'$ then $s \xrightarrow{a\sigma}^* s'$, for $a \in N, \sigma \in N^*$

Reachable state

$t \in S$ is reachable from $s \in S$ iff there is a word $\sigma \in N^*$ st $s \xrightarrow{\sigma}^* t$

Labelled Transition System

Alternative characterization (coalgebraic)

A morphism $h : \langle S, \mathrm{next} \rangle \longrightarrow \langle S', \mathrm{next}' \rangle$ is a function $h : S \longrightarrow S'$ st the following diagram commutes

$$\begin{tikzcd}
S \times N \arrow[r, "\mathrm{next}"] \arrow[d, "h \times id"'] & \mathcal{P}S \arrow[d, "\mathcal{P}h"] \\
S' \times N \arrow[r, "\mathrm{next}'"] & \mathcal{P}S'
\end{tikzcd}$$

i.e.,

$$\mathcal{P}h \cdot \mathrm{next} \quad = \quad \mathrm{next}' \cdot (h \times id)$$

or, going pointwise,

$$\{h\ x \mid x \in \mathrm{next}\ \langle s, a \rangle\} \quad = \quad \mathrm{next}'\ \langle h\ s, a \rangle$$

Labelled Transition System

Alternative characterization (coalgebraic)

A morphism $h : \langle S, \mathrm{next}\rangle \longrightarrow \langle S', \mathrm{next}'\rangle$

- preseves transitions:

$$s' \in \mathrm{next}\ \langle s, a\rangle \Rightarrow h\ s' \in \mathrm{next}'\ \langle h\ s, a\rangle$$

- reflects transitions:

$$r' \in \mathrm{next}'\ \langle h\ s, a\rangle \Rightarrow \langle \exists\ s' \in S\ :\ s' \in \mathrm{next}\ \langle s, a\rangle :\ r' = h\ s'\rangle$$

(why?)

Comparison

- Both definitions coincide at the object level:

$$\langle s, a, s' \rangle \in T \quad \equiv \quad s' \in \mathsf{next}\ \langle s, a \rangle$$

- Wrt morphisms, the relational definition is more general, corresponding, in coalgebraic terms to

$$\mathcal{P}h \cdot \mathsf{next} \quad \subseteq \quad \mathsf{next}' \cdot (h \times id)$$

Looking for suitable notions of equivalence of behaviours

Intuition

Two LTS should be equivalent if they cannot be distinguished by interacting with them.

Equality of functional behaviour

is not preserved by parallel composition: non compositional semantics, cf,

`x:=4; x := x+1` and `x:=5`

Graph isomorphism

is too strong (why?)

Trace

Definition

Let $T = \langle S, N, \longrightarrow \rangle$ be a labelled transition system. The set of traces $\mathrm{Tr}(s)$, for $s \in S$ is the minimal set satisfying

$$(1) \quad \epsilon \in \mathrm{Tr}(s)$$

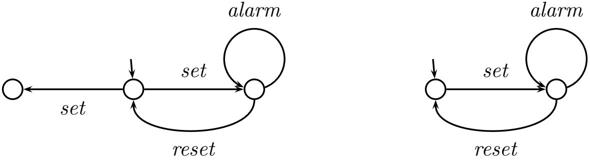
$$(3) \quad a\sigma \in \mathrm{Tr}(s) \;\Rightarrow\; \langle \exists\, s' \;:\; s' \in S :\; s \xrightarrow{a} s' \wedge \sigma \in \mathrm{Tr}(s') \rangle$$

Trace equivalence

Definition

Two states s, r are trace equivalent iff $\mathsf{Tr}(s) = \mathsf{Tr}(r)$
(i.e. they can perform the same finite sequences of transitions)

Example



Trace equivalence applies when one can neither interact with a system, nor distinguish a slow system from one that has come to a stand still.

Simulation

the quest for a behavioural equality:
able to identify states that cannot be distinguished by any realistic
form of observation

Simulation

A state q simulates another state p if every transition from q is corresponded by a transition from p and this capacity is kept along the whole life of the system to which state space q belongs to.

Simulation

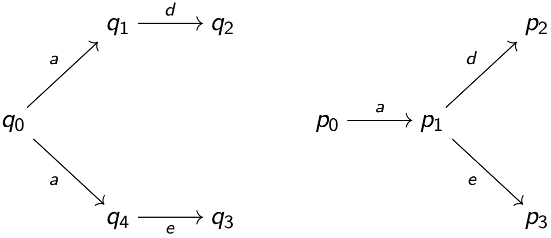
Definition

Given $\langle S_1, N, \longrightarrow_1\rangle$ and $\langle S_2, N, \longrightarrow_2\rangle$ over N, relation $R \subseteq S_1 \times S_2$ is a simulation iff, for all $\langle p, q\rangle \in R$ and $a \in N$,

$$(2)\quad p \xrightarrow{a}_1 p' \;\Rightarrow\; \langle \exists\, q' \;:\; q' \in S_2 : \; q \xrightarrow{a}_2 q' \wedge \langle p', q'\rangle \in R\rangle$$

$$\begin{tikzcd}
p \arrow[d, "a"] & R & q & \Rightarrow & & & q \arrow[d, "a"] \\
p' & & & & p' & R & q'
\end{tikzcd}$$

Example



$q_0 \lesssim p_0$ cf. $\{\langle q_0, p_0\rangle, \langle q_1, p_1\rangle, \langle q_4, p_1\rangle, \langle q_2, p_2\rangle, \langle q_3, p_3\rangle\}$

Similarity

Definition

$$p \lesssim q \;\equiv\; \langle \exists\, R \;::\; R \text{ is a simulation and } \langle p, q \rangle \in R \rangle$$

Lemma

The similarity relation is a preorder
(i.e. reflexive and transitive)

Bisimulation

Definition

Given $\langle S_1, N, \longrightarrow_1\rangle$ and $\langle S_2, N, \longrightarrow_2\rangle$ over N, relation $R \subseteq S_1 \times S_2$ is a bisimulation iff both R and its converse R° are simulations.
I.e. whenever $\langle p, q\rangle \in R$ and $a \in N$,

$$(1)\quad p \xrightarrow{a}_1 p' \;\Rightarrow\; \langle \exists\, q' \;:\; q' \in S_2 :\; q \xrightarrow{a}_2 q' \wedge \langle p', q'\rangle \in R\rangle$$

$$(2)\quad q \xrightarrow{a}_2 q' \;\Rightarrow\; \langle \exists\, p' \;:\; p' \in S_1 :\; p \xrightarrow{a}_1 p' \wedge \langle p', q'\rangle \in R\rangle$$

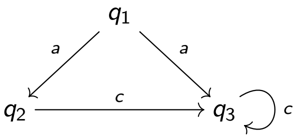
Bisimulation

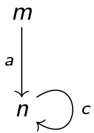
The Game characterization

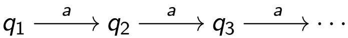
Two players R and I discuss whether the transition structures are mutually corresponding

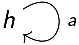
- R starts by chosing a transition
- I replies trying to match it
- if I succeeds, R plays again
- R wins if I fails to find a corresponding match
- I wins if it replies to all moves from R and the game is in a configuration where all states have been visited or R can't move further. In this case is said that I has a wining strategy

Examples

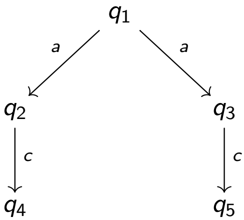


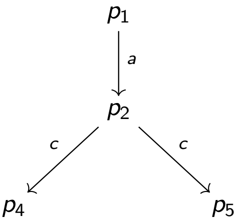


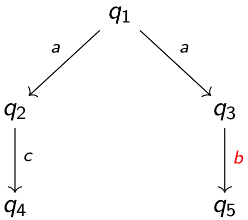


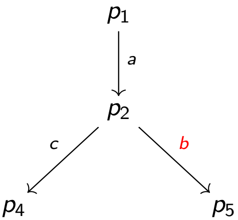


Examples


q_1
a
a
q_2
q_3
c
c
q_4
q_5


p_1
a
p_2
c
c
p_4
p_5


q_1
a
a
q_2
q_3
c
b
q_4
q_5


p_1
a
p_2
c
b
p_4
p_5

After thoughts

- Follows a $\forall, \exists$ pattern: p in all its transitions challenge q which is called to find a matchh to each of those (and conversely)
- Tighter correspondence with transitions
- Based on the information that the transitions convey, rather than on the shape of the LTS
- Local checks on states
- Lack of hierarchy on the pairs of the bisimulation (no temporal order on the checks is required)

which means bisimilarity can be used to reason about infinite or circular behaviours.

After thoughts

Compare the definition of bisimilarity with

$p == q$ if, for all $a \in N$

$$
\begin{array}{ll}
(1) & p \xrightarrow{a}_1 p' \;\Rightarrow\; \langle \exists\, q' \;:\; q' \in S_2 :\; q \xrightarrow{a}_2 q' \wedge p' == q' \rangle \\
(2) & q \xrightarrow{a}_2 q' \;\Rightarrow\; \langle \exists\, p' \;:\; p' \in S_1 :\; p \xrightarrow{a}_1 p' \wedge p' == q' \rangle
\end{array}
$$

After thoughts

$p == q$ if, for all $a \in N$

$$(1)\quad p \downarrow_1 \; \Leftrightarrow q \downarrow_2$$

$$(2.1)\quad p \xrightarrow{a}_1 p' \;\Rightarrow\; \langle \exists\, q' \;:\; q' \in S_2 :\; q \xrightarrow{a}_2 q' \wedge p' == q' \rangle$$
$$(2.1)\quad q \xrightarrow{a}_2 q' \;\Rightarrow\; \langle \exists\, p' \;:\; p' \in S_1 :\; p \xrightarrow{a}_1 p' \wedge p' == q' \rangle$$

- The meaning of $==$ on the pair $\langle p, q \rangle$ requires having already established the meaning of $==$ on the derivatives
- ... therefore the definition is ill-founded if the state space reachable from $\langle p, q \rangle$ is infinite or contain loops
- ... this is a local but inherently inductive definition (to revisit later)

After thoughts

Proof method

To prove that two behaviours are bisimilar, find a bisimulation containing them ...

- ... impredicative character
- coinductive vs inductive definition

Properties

Definition

$$p \sim q \;\equiv\; \langle \exists\, R \;::\; R \text{ is a bisimulation and } \langle p, q\rangle \in R \rangle$$

Lemma

1. The identity relation *id* is a bisimulation
2. The empty relation $\perp$ is a bisimulation
3. The converse R° of a bisimulation is a bisimulation
4. The composition $S \cdot R$ of two bisimulations S and R is a bisimulation
5. The $\bigcup_{i \in I} R_i$ of a family of bisimulations $\{R_i \mid i \in I\}$ is a bisimulation

Properties

Lemma

The bisimilarity relation is an equivalence relation
(i.e. reflexive, symmetric and transitive)

Lemma

The class of all bisimulations between two LTS has the structure of a complete lattice, ordered by set inclusion, whose top is the bisimilarity relation $\sim$.

Properties

Lemma

In a deterministic labelled transition system, two states are bisimilar iff they are trace equivalent, i.e.,

$$s \sim s' \;\Leftrightarrow\; \mathrm{Tr}(s) = \mathrm{Tr}(s')$$

Hint: define a relation R as

$$\langle x, y \rangle \in R \;\Leftrightarrow\; \mathrm{Tr}(x) = \mathrm{Tr}(y)$$

and show R is a bisimulation.

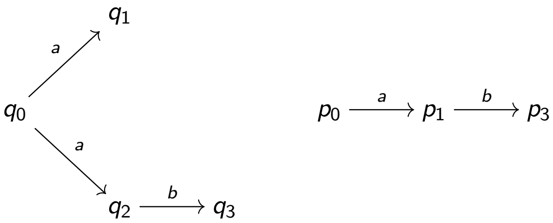
Properties

Warning

The bisimilarity relation $\sim$ is not the symmetric closure of $\lesssim$

Example

$$q_0 \lesssim p_0,\ p_0 \lesssim q_0 \quad \text{but} \quad p_0 \not\sim q_0$$



Notes

Similarity as the greatest simulation

$$\lesssim \ \widehat{=} \ \bigcup\{S \mid S \text{ is a simulation}\}$$

Bisimilarity as the greatest bisimulation

$$\sim \ \widehat{=} \ \bigcup\{S \mid S \text{ is a bisimulation}\}$$

Automata

Back to old friends?

$$\boxed{\text{automaton behaviour} \;\equiv\; \text{accepted language}}$$

Recall that finite automata recognize regular languages, i.e. generated by

- $L_1 + L_2 \;\widehat{=}\; L_1 \cup L_2$ (union)
- $L_1 \cdot L_2 \;\widehat{=}\; \{st \mid s \in L_1, t \in L_2\}$ (concatenation)
- $L^* \;\widehat{=}\; \{\epsilon\} \cup L \cup (L \cdot L) \cup (L \cdot L \cdot L) \cup \ldots$ (iteration)

Automata

There is a syntax to specify such languages:

$$E \quad ::= \quad \epsilon \mid a \mid E + E \mid E\, E \mid E^*$$

where $a \in \Sigma$.

- which regular expression specifies $\{a, bc\}$?
- and $\{ca, cb\}$?

and an algebra of regular expressions:

$$\begin{aligned} (E_1 + E_2) + E_3 &= E_1 + (E_2 + E_3) \\ (E_1 + E_2)\, E_3 &= E_1\, E_3 + E_2\, E_3 \\ E_1\, (E_2\, E_1)^* &= (E_1\, E_2)^*\, E_1 \end{aligned}$$

Automata

There is a syntax to specify such languages:

$$E \;::=\; \epsilon \mid a \mid E + E \mid E\,E \mid E^*$$

where $a \in \Sigma$.

- which regular expression specifies $\{a, bc\}$?
- and $\{ca, cb\}$?

and an algebra of regular expressions:

$$\begin{aligned} (E_1 + E_2) + E_3 &= E_1 + (E_2 + E_3) \\ (E_1 + E_2)\,E_3 &= E_1\,E_3 + E_2\,E_3 \\ E_1\,(E_2\,E_1)^* &= (E_1\,E_2)^*\,E_1 \end{aligned}$$

After thoughts

... need more general models and theories:

- Several interaction points ($\neq$ functions)
- Need to distinguish normal from anomalous termination (eg deadlock)
- Nondeterminisim should be taken seriously: the reactive character of systems entail that not only the generated language is important, but also the states traversed during an execution of the automata.
- New systems from old: going compositional