Bisimulation, Games & Hennessy Milner logic

Lecture 1 of Modelli Matematici dei Processi Concorrenti

Paweł Sobociński

Univeristy of Southampton, UK

Classical language theory

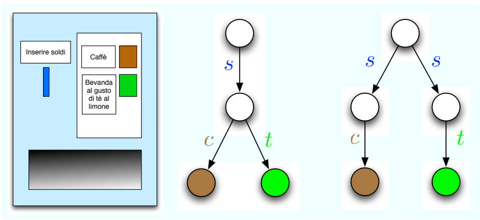
Is concerned primarily with languages, eg.

- finite automata $\leftrightarrow$ regular languages;
- pushdown automata $\leftrightarrow$ context-free languages;
- turing machines $\leftrightarrow$ recursively enumerable languages;

This is fine when we think of an automaton/TM as a **sequential** process which **has no interactions** with the outside world during its computation.

However, automata which accept the same languages can behave very differently to an outside observer.

The famous coffee machine example



We will discuss the observations one can make about such systems.

Labelled transition systems

A labelled transition system (LTS) $\mathcal{L}$ is a triple $\langle S, A, T \rangle$ where:

- S is a set of **states**;
- A is a set of **actions**;
- $T \subseteq S \times A \times S$ is the **transition relation**.

We will normally write $p \xrightarrow{a} p'$ for $(p, a, p') \in T$.

Labelled transition systems generalise both automata and trees. They are a central abstraction of concurrency theory.

Trace preorder

Given a state p of an LTS $\mathcal{L}$, the word $\sigma = \alpha_1 \alpha_2 \ldots \alpha_k \in A^*$ is a trace of p when $\exists$ transitions

$$p \xrightarrow{\alpha_1} p_1 \xrightarrow{\alpha_2} \ldots p_{k-1} \xrightarrow{\alpha_k} p'$$

We will use $p \xrightarrow{\sigma} p'$ as shorthand.

Suppose that $\mathcal{L}_1$ and $\mathcal{L}_2$ are LTSs. The **trace preorder** $\leq_{tr} \subset S_1 \times S_2$ is defined as follows:

$$p \leq_{tr} q \quad \Leftrightarrow \quad \forall \sigma \in A^*.\ p \xrightarrow{\sigma} p' \Rightarrow \exists q'.\ q \xrightarrow{\sigma} q'$$

Observation 1. *$\leq_{tr}$ is reflexive and transitive.*

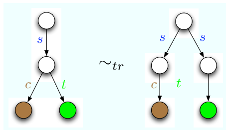
Trace equivalence

Trace equivalence is defined $\sim_{tr} = \leq_{tr} \cap \geq_{tr}$, ie

$$p \sim_{tr} q \stackrel{\text{def}}{=} p \leq_{tr} q \ \wedge \ q \geq_{tr} p$$

It is immediate that when $\mathcal{L}_1 = \mathcal{L}_2$, $\sim_{tr}$ is an equivalence relation on the states of an LTS

But traces are not enough: trace equivalence is very coarse, since the coffee machines have the same traces.



Simulation

Suppose that $\mathcal{L}_1$ and $\mathcal{L}_2$ are LTSs. A relation $R \subseteq S_{\mathcal{L}_1} \times S_{\mathcal{L}_2}$ is called a **simulation** whenever:

- if pRq and $p \xrightarrow{a} p'$ then there exists q' such that $q \xrightarrow{a} q'$ and $p'Rq'$.

Observation 2. *The empty relation is a simulation and arbitrary unions of simulations are simulations.*

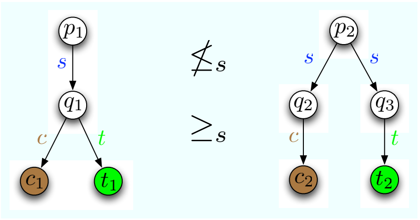
Similarity $\leq_s \subseteq S_1 \times S_2$ is defined as the largest simulation. Equivalently, $p \leq_s q$ iff there exists a simulation R such that $(p, q) \in R$.

Observation 3. *Similarity is reflexive and transitive.*

Observation 4. *Simulation equivalence* $\sim_s \stackrel{\text{def}}{=} \leq_s \cap \geq_s$.

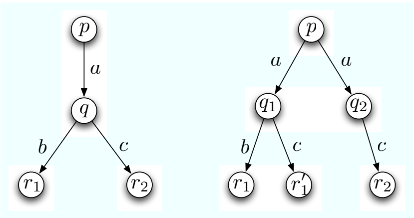
Simulation example 1

Simulation is more sensitive to branching (ie non-determinism) than traces:



Simulation example 2

But it is not entirely satisfactory.



Bisimulation

Suppose that $\mathcal{L}_1$ and $\mathcal{L}_2$ are LTSs. A relation $R \subseteq S_{\mathcal{L}_1} \times S_{\mathcal{L}_2}$ is called a **bisimulation** whenever:

(i) if pRq and $p \xrightarrow{a} p'$ then there exists q' such that $q \xrightarrow{a} q'$ and $p'Rq'$;

(ii) if qRp and $q \xrightarrow{a} q'$ then there exists p' such that $p \xrightarrow{a} p'$ and $p'Rq'$.

Lemma 5. *R is a bisimulation iff R and R^{op} are simulations.*

Properties of bisimulations

Lemma 6. *$\varnothing$ is a bisimulation.*

Proof. Vacously true. □

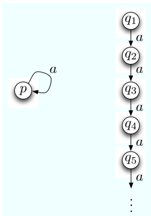
Lemma 7. *If $\{R_i\}_{i \in I}$ are a family of bisimulations then $\bigcup_{i \in I} R_i$ is a bisimulation.*

Proof. Let $\mathbf{R} = \bigcup_{i \in I} R_i$. Suppose $p\mathbf{R}q$ then there exists k such that pR_kq. In particular, qR_kp and so $q\mathbf{R}p$, thus $\mathbf{R}$ is symmetric.
If $p \xrightarrow{a} p'$ then there exists q' such that $q \xrightarrow{a} q'$ and $p'R_kq'$. But $p'R_kq'$ implies $p'\mathbf{R}q'$. □

Corollary 8. *There exists a largest bisimulation $\sim$. It is called **bisimilarity**.*

If $\mathcal{L}_1 = \mathcal{L}_2$ then bisimilarity is an equivalence relation.

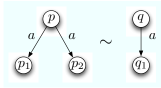
Examples of bisimulations, 1

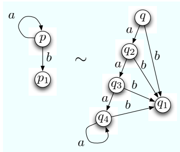


Lemma 9. $p \sim q_1$.

Proof. $R = \{\, (p, q_i) \mid i \in \mathbb{N} \,\}$ is a bisimulation. □

Examples of bisimulations, 2





Reasoning about bisimilarity

- To show that states p, q are bisimilar it suffices to find a bisimulaion R which relates p and q;
- It is less clear how to show that p and q are **not** bisimilar, one can:
  - enumerate all the relations which contain (p, q) and show that none of them are bisimulations;
  - enumerate all the bisimulation and show that none of them contain (p, q);
  - borrow some techiniques from game theory...

Bisimulation game, 1

We are given two LTSS $\mathcal{L}_1$, $\mathcal{L}_2$. The configuration is a pair of states (p, q), $p \in \mathcal{L}_1$, $q \in \mathcal{L}_2$. The bisimulation game has two players: $\mathscr{P}$ and $\mathscr{R}$. A round of the game proceeds as follows:

(i) $\mathscr{R}$ chooses either p or q;

(ii) assuming it chose p, it next chooses a transition $p \xrightarrow{a} p'$;

(iii) $\mathscr{P}$ must choose a transition with the same label in the other LTS, ie assuming $\mathscr{R}$ chose p, it must find a transition $q \xrightarrow{a} q'$;

(iv) the round is repeated, replacing (p, q) with (p', q').

Bisimulation game, 2

Rules: An infinite game is a win for $\mathscr{P}$. $\mathscr{R}$ wins iff the game gets into a round where $\mathscr{P}$ cannot respond with a transition in step (iii).

Observation 10. *For each configuration (p, q), either $\mathscr{P}$ or $\mathscr{R}$ has a winning strategy.*

Theorem 11. *$p \sim q$ iff $\mathscr{P}$ has a winning strategy. ($p \not\sim q$ iff $\mathscr{R}$ has a winning strategy.)*

$\mathscr{P}$ has a winning strategy $\Rightarrow p \sim q$

Let $GE \stackrel{\text{def}}{=} \{ (p, q) \mid \mathscr{P}$ has a winning strategy $\}$.

Suppose that $(p, q) \in GE$ and $p \xrightarrow{a} p'$. Suppose that there does not exist a transition $q \xrightarrow{a} q'$ such that $(p', q') \in GE$. Then $\mathscr{R}$ can choose the transition $p \xrightarrow{a} p'$ and $\mathscr{P}$ cannot respond in a way which keeps him in a winnable position. But this contradicts the fact that that $\mathscr{P}$ has a winning strategy for the game starting with (p, q). Thus GE is a bisimulation.

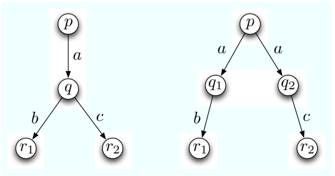
$p \sim q \Rightarrow \mathscr{P}$ has a winning strategy

Bisimulations are winning strategies:

If $p \sim q$ then there exists a bisimulation R such that $(p, q) \in R$. Whatever move $\mathscr{R}$ makes, $\mathscr{P}$ can always make a move such that the result is in R. Clearly, this is a winning strategy for P.

Examples of non bisimilar states

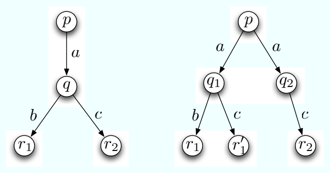
Bisimilarity is branching-sensitive.



Similarity and bisimilarity

Theorem 12. $\sim \subset \leq \cap \geq$ *and in general the inclusion is strict.*

Proof. Any bisimulation and its opposite are clearly simulations. On the other hand, the following example shows that bisimilarity is finer than simulation equivalence.



□

Recap: equivalences

$$\sim \subset \sim_s \subset \sim_{tr}$$

Bisimilarity is the finest (=equates less) equivalence we have considered.

Claim 13. *Bisimilarity is the finest "reasonable" equivalence, where "reasonable" means that we can observe only the behaviour and not the state-space.*

We will give a language, the so-called Hennessy Milner logic, which describes observations/experiments on LTSs.

Hennessy Milner logic

Suppose that A is a set of actions. Let

$$L \ ::= \ [a]L \mid \langle a \rangle L \mid \neg L \mid L \vee L \mid L \wedge L \mid \top \mid \bot$$

Given an LTS we define the semantics by structural induction over the formula φ:

- $q \vDash [A]\varphi$ if for all q' such that $q \xrightarrow{a} q'$ we have $q' \vDash \varphi$;
- $q \vDash \langle A \rangle \varphi$ if there exists q' such that $q \xrightarrow{a} q'$ and $q' \vDash \varphi$;
- $q \vDash \neg\varphi$ if it is not the case that $q \vDash \varphi$;
- $q \vDash \varphi_1 \vee \varphi_2$ if $q \vDash \varphi_1$ or $q \vDash \varphi_2$;
- $q \vDash \varphi_1 \wedge \varphi_2$ if $q \vDash \varphi_1$ and $q \vDash \varphi_2$;
- $q \vDash \top$ always;
- $q \vDash \bot$ never;

HM logic example formulas

- $\langle a \rangle \top$ – can perform a transition labelled with a;
- $[a]\bot$ – cannot perform a transition labelled with a;
- $\langle a \rangle [b] \bot$ – can perform a transition labelled with a to a state from which there are no b labelled transitions.
- $\langle a \rangle ([b]\bot \wedge \langle c \rangle \top)$ – ?

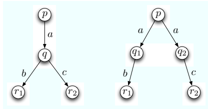
Basic properties of HM logic

Lemma 14 ("De Morgan" laws for HM logic)**.**

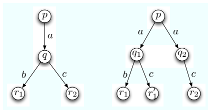
- $[a] = \neg\langle a \rangle \neg$;
- $\langle a \rangle = \neg[a]\neg$;
- $\wedge = \neg(\neg \vee \neg)$;
- $\vee = \neg(\neg \wedge \neg)$;
- $\top = \neg\bot$;
- $\bot = \neg\top$.

In particular, to get the full logic it suffices to consider just the subsets $\{\langle a \rangle, \vee, \bot, \neg\}$ or $\{[a], \wedge, \top, \neg\}$ or $\{\langle a \rangle, [a], \vee, \wedge, \top, \bot\}$.

Distinguishing formulas



$\models \langle a\rangle(\langle b\rangle \wedge \langle c\rangle)$ $\qquad$ $\not\models \langle a\rangle(\langle b\rangle \wedge \langle c\rangle)$



$\not\models \langle a\rangle(\neg\langle b\rangle)$ $\qquad$ $\models \langle a\rangle(\neg\langle b\rangle)$

Logical equivalence

Definition 15. *The logical preorder $\leq_L$ is a relation on the states of an* LTS *defined as follows:*

$$p <_L q \quad \textit{iff} \quad \forall\varphi.\ p \models \varphi \Rightarrow q \models \varphi$$

It is clearly reflexive and transitive.

Definition 16. **Logical equivalence** *is $\sim_L \stackrel{\text{def}}{=} \leq_L \cap \geq_L$. It is an equivalence relation.*

Observation 17. *Actually, for HM, $\leq_L = \sim_L = \geq_L$. This is a consequence of having negation.*

Proof. Suppose $p \leq_L q$ and $q \models \varphi$. If $p \not\models \varphi$ then $p \models \neg\varphi$, hence $q \vdash \neg\varphi$ hence $q \not\models \varphi$, a contradiction. Hence $p \models \varphi$. □

Hennessy Milner & Bisimulation

Definition 18. *An LTS is said to have* **finite image** *when from any state, the number of states reachable is finite.*

Theorem 19 (Hennessy Milner)**.** *Let $\mathcal{L}$ be an LTS with finite image. Then $\sim_L = \sim$.*

To prove this, we need to show:

- **Soundness** ($\sim_L \subseteq \sim$): If two states satisfy the same formulas then they are bisimilar.
- **Completeness** ($\sim \subseteq \sim_L$): If two states are bisimilar then they satisfy the same formulas.

Remark 20. *Completeness holds in general. The finite image assumption is needed only for soundness.*

Soundness

$\sim_L \subseteq \sim$ (Soundness)
It suffices to show that $\sim_L$ is a bisimulation. We will rely on image finiteness.

Suppose that $p \sim_L q$ and $p \xrightarrow{a} p'$. Then $p \models \langle a\rangle\top$ and so $q \models \langle a\rangle\top$ – thus there is at least one q' such that $q \xrightarrow{a} q'$. The set of all such q' is also finite by the extra assumption – let this set be $\{q_1, \ldots, q_k\}$. Suppose that for all q_i we have that $p' \not\sim_L q_i$. Then $\exists\varphi_i$ such that $p' \models \varphi_i$ and $q_i \not\models \varphi_i$. Thus while $p \models \langle a\rangle \bigwedge_{i\leq k}\varphi_i$ we must have $q \not\models \langle a\rangle \bigwedge_{i\leq k}\varphi_i$, a contradiction. Hence there exists q_i such that $q \xrightarrow{a} q_i$ and $p' \sim_L q_i$.

Completeness 1

$\sim \subseteq \sim_L$ (Completeness)
We will show this $p <_L q$ by structural induction on formulas.
Base: $p \models \top$ then $q \models \top$. Also, $p \models \bot$ then $q \models \bot$.
Induction:

- Modalities ($\langle a\rangle$ and $[a]$):
  - If $p \models \langle a\rangle\varphi$ then $p \xrightarrow{a} p'$ and $p' \models \varphi$. By assumption, there exists q' such that $q \xrightarrow{a} q'$ and $p' \sim q'$. By inductive hypothesis $q' \models \varphi$ and so $q \models \langle a\rangle\varphi$.
  - If $p \models [a]\varphi$ then whenever $p \xrightarrow{a} p'$ then $p' \models \varphi$. First, notice that $p \sim q$ implies that if $q \xrightarrow{a} q'$ then there exists p' such that $p \xrightarrow{a} p'$ with $p' \sim q'$. Since $p' \models \varphi$, also $q' \models \varphi$. Hence $q \models [a]\varphi$.

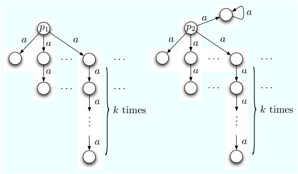
Completeness 2

- Propositional connectives ($\vee$ and $\wedge$):
  - if $p \models \varphi_1 \vee \varphi_2$ then $p \models \varphi_1$ or $p \models \varphi_2$. If it is the first then by the inductive hypothesis $q \models \varphi_1$, if the second then $q \models \varphi_2$; thus $q \models \varphi_1 \vee \varphi_2$.
  - if $p \models \varphi_2 \wedge \varphi_2$ is similar.

Note that completeness does not need the finite image assumption – thus bisimilar states *always* satisfy the same formulas. In the proof, we used the fact that $\{\langle a\rangle, [a], \vee, \wedge, \top, \bot\}$ is enough for all of HM logic.

Image finiteness

The theorem breaks down without this assumption:



Easy to check, using the bisimulation game, that $p_1 \nsim p_2$.

Solution: Introduce infinite conjunction to the logic.

Sublogics of HM

$$L_{tr} \ ::= \ \langle a \rangle L_{tr} \mid \top$$

Theorem 21. *Logical preorder on L_{tr} coincides with the trace preorder.*

$$L_s \ ::= \ \langle a \rangle L_s \mid L_s \wedge L_s \mid \top$$

Theorem 22. *Logical preorder on L_s conicides with the simulation preorder.*