National School SIDRA 2017: Formal Methods for the Control of Large-scale Networked Nonlinear Systems with Logic Specifications

Lecture L5: Relations among metric transition systems*

Abstract. In this lecture we will introduce basic notions from formal methods. We will introduce the notions of simulation and bisimulation relations and their alternating variants, first in the exact case, then in the approximate case. Some examples are also offered. This lecture is based on [3, 4, 1, 2, 5].

1 Notation

The symbols $\mathbb{R}$, $\mathbb{R}^+$ and $\mathbb{R}_0^+$ denote the set of real, positive real, and nonnegative real numbers, respectively.

2 Transition systems relations and equivalences

In order to relate properties of infinite states transition systems to symbolic transition systems we need to recall some notions from formal methods. We start with the notion of simulation relation.

Definition 1. *[3, 4] Let $T_i = (X_i, X_{0,i}, U_i, \xrightarrow[i]{}, X_{m,i}, Y_i, H_i)$ $(i = 1, 2)$ be transition systems with the same output sets $Y_1 = Y_2$. A relation*

$$\mathcal{R} \subseteq X_1 \times X_2$$

is said to be a simulation relation from T_1 to T_2 if it satisfies the following conditions:

i) $\forall x_1 \in X_{0,1}$ $\exists x_2 \in X_{0,2}$ *such that* $(x_1, x_2) \in \mathcal{R}$*;*
ii) $\forall x_1 \in X_{m,1}$ $\exists x_2 \in X_{m,2}$ *such that* $(x_1, x_2) \in \mathcal{R}$*;*
iii) $\forall (x_1, x_2) \in \mathcal{R}$, $H_1(x_1) = H_2(x_2)$*;*
iv) $\forall (x_1, x_2) \in \mathcal{R}$ *if* $x_1 \xrightarrow[1]{u_1} x_1'$ *then there exists* $x_2 \xrightarrow[2]{u_2} x_2'$ *such that* $(x_1', x_2') \in \mathcal{R}$.

Transition system T_1 is simulated by transition system T_2, denoted

$$T_1 \preceq T_2,$$

if there exists a simulation relation from T_1 to T_2.

Intuitively, if T_2 simulates T_1 then the behavior of T_2 contains the behavior of T_1. Moreover,

Proposition 1. *If $T_1 \preceq T_2$ then $\mathcal{L}^y(T_1) \subseteq \mathcal{L}^y(T_2)$ and $\mathcal{L}_m^y(T_1) \subseteq \mathcal{L}_m^y(T_2)$.*

The converse implication in the result above is not true in general. The following example clarifies these issues.

Example 1. Consider transition systems T_1 and T_2 in Fig. 1. It is easy to see that $T_1 \preceq T_2$ with simulation relation

$$\mathcal{R} = \{(0, 0'), (1, 1'), (3, 1'), (2, 2'), (4, 3')\}.$$

Moreover,

$$\mathcal{L}^y(T_1) = \{\varepsilon, a, ab, abc, abd\} \subseteq \{\varepsilon, a, ab, abc, abd\} = \mathcal{L}^y(T_2);$$
$$\mathcal{L}_m^y(T_1) = \{abc, abd\} \subseteq \{abc, abd\} = \mathcal{L}_m^y(T_2).$$

Conversely, T_2 is not simulated by T_1 because there is no state in T_1 that can mimic the state $1'$ of T_2 (state $1'$ can reach two states with outputs c and d), while it is true that

$$\mathcal{L}^y(T_2) \subseteq \mathcal{L}^y(T_1);$$
$$\mathcal{L}_m^y(T_2) \subseteq \mathcal{L}_m^y(T_1).$$

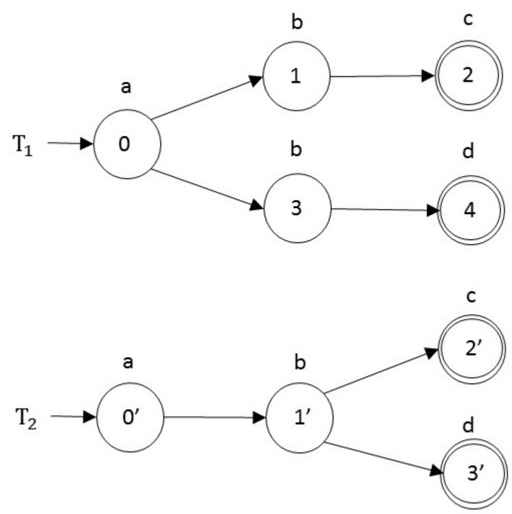

Fig. 1. Transition systems T_1 and T_2.

The following proposition states that the simulation relation is a preorder on the set of transition systems:

Proposition 2. *For any transition systems* $T_i = (X_i, X_{0,i}, U_i, \xrightarrow[i]{}, X_{m,i}, Y_i, H_i)$*,* $i = 1, 2, 3$ *with* $Y_1 = Y_2 = Y_3$*:*

i) $T_i \preceq T_i$*;*
ii) $T_i \preceq T_j$ *and* $T_j \preceq T_k$ *implies* $T_i \preceq T_k$*.*

Proof. Proof of i): Pick $\mathcal{R}$ as the identity relation, i.e. the relation composed by pairs of the form (x, x) for any state x of T_1.
Proof of ii): Let $\mathcal{R}_{12}$ and $\mathcal{R}_{23}$ denote simulation relations from T_1 to T_2 and from T_2 to T_3, respectively, and consider the relation $\mathcal{R}_{12} \circ \mathcal{R}_{23}$ obtained by the composition of $\mathcal{R}_{12}$ and $\mathcal{R}_{23}$ and defined by

$$\mathcal{R}_{12} \circ \mathcal{R}_{23} = \{(x_1, x_3) \in X_1 \times X_3 | \exists x_2 \in X_2 \text{ s.t. } (x_1, x_2) \in \mathcal{R}_{12} \text{ and } (x_2, x_3) \in \mathcal{R}_{23}\}.$$

The following proposition establishes connections between the notions of simulation relations and of subsystems:

Proposition 3. *If* $T_1 \sqsubseteq T_2$ *then* $T_1 \preceq T_2$*.*

Proof. Define the relation $\mathcal{R} \subseteq X_1 \times X_2$, where X_i is the set of states of T_i, as $(x_1, x_2) \in \mathcal{R}$ if and only if $x_1 = x_2$. Relation $\mathcal{R}$ is a simulation relation from T_1 to T_2.

The converse implication in the result above is clearly not true in general. We now introduce bisimulation equivalence:

Definition 2. *[3, 4] Let* $T_i = (X_i, X_{0,i}, U_i, \xrightarrow[i]{}, X_{m,i}, Y_i, H_i)$ *($i = 1, 2$) be transition systems with the same output sets* $Y_1 = Y_2$*. A relation*

$$\mathcal{R} \subseteq X_1 \times X_2$$

is said to be a bisimulation relation between T_1 *and* T_2 *if it satisfies the following conditions:*

- $\mathcal{R}$ *is simulation relation from* T_1 *to* T_2*;*
- $\mathcal{R}^{-1}$ *is a simulation relation from* T_2 *to* T_1*, where* $\mathcal{R}^{-1} \subseteq X_2 \times X_1$ *is the inverse relation of* $\mathcal{R}$*, defined by*

$$(x_2, x_1) \in \mathcal{R}^{-1} \iff (x_1, x_2) \in \mathcal{R}.$$

Transition system T_1 *and* T_2 *are bisimilar, denoted*

$$T_1 \cong T_2,$$

if there exists a bisimulation relation $\mathcal{R}$ *between* T_1 *and* T_2*.*

Intuitively, T_1 and T_2 are bisimilar if the behavior of T_1 is the same as the behavior of T_2. Moreover,

Proposition 4. *If* $T_1 \cong T_2$ *then* $\mathcal{L}^y(T_1) = \mathcal{L}^y(T_2)$ *and* $\mathcal{L}^y_m(T_1) = \mathcal{L}^y_m(T_2)$*.*

The converse implication in the result above is not true in general. Example 1 serves also to the purpose of illustrating this issue. However, it is possible to show that the converse implication is true in the case of output deterministic transition systems, see e.g. [6] for details.

The following result establishes connections between the notions of simulation and bisimulation.

Proposition 5. *If* $T_1 \cong T_2$ *then* $T_1 \preceq T_2$ *and* $T_2 \preceq T_1$*.*

The converse implication in the result above is not true in general as shown in the following

Example 2. Consider transition system T_2 in Fig. 1 and transition system T_3 in Fig. 2. We get:

- $T_3 \preceq T_2$ with simulation relation

$$\mathcal{R} = \{(0, 0'), (1, 1'), (3, 1'), (2, 2'), (4, 3')\};$$

- $T_2 \preceq T_3$ with simulation relation

$$\mathcal{R} = \{(0', 0), (1', 1), (2', 2), (3', 4)\};$$

- T_2 and T_3 are not bisimilar because there is no state in T_2 that can replicate the exact behavior of state 3 in T_3 (state 3 can only reach a state with output d while state $1'$ can reach two states with outputs c and d).

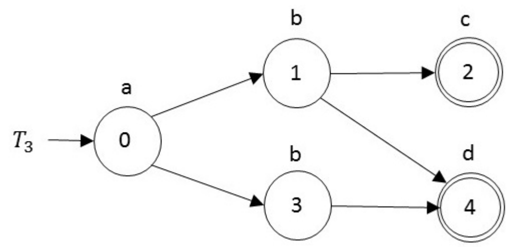

Fig. 2. Transition system T_3.

The following proposition states that bisimulation is an equivalence relation on the set of transition systems:

Proposition 6. *For any transition system* $T_i = (X_i, X_{0,i}, U_i, \xrightarrow[i]{}, X_{m,i}, Y_i, H_i)$, $i = 1, 2, 3$ *with* $Y_1 = Y_2 = Y_3$*:*

i) $T_1 \cong T_1$*;*
ii) If $T_1 \cong T_2$ *then* $T_2 \cong T_1$*;*
iii) $T_1 \cong T_2$ *and* $T_2 \cong T_3$ *implies* $T_1 \cong T_3$*.*

Proof. For the proofs of i) and iii) use the same arguments as those used in the proof of i) and ii) of Proposition 2. For the proof of ii) if $\mathcal{R}$ is a bisimulation relation between T_1 and T_2 then $\mathcal{R}^{-1}$ is a bisimulation relation between T_2 and T_1.

We now proceed a step further and introduce the notions of alternating simulation and alternating bisimulation relations. These notions were introduced in [1] as a tool to address control design for nondeterministic transition systems. We start with the following

Example 3. Consider the transition system T_1 in Fig. 3. Note that T_1 is nondeterministic. Suppose you want to find a control strategy bringing the state of T_1 from 0 to 1 or to 2 in one step. This is a basic reachability control problem. We now want to use simulation relations to simplify control design. Consider the transition system T_2 in Fig. 3. It is easy to see that T_2 is a subsystem of T_1, i.e. $T_2 \sqsubseteq T_1$, and hence, by Proposition 3, $T_2 \preceq T_1$. Indeed relation

$$\mathcal{R} = \{(0,0), (1,1), (2,2)\}$$

is a simulation relation from T_2 to T_1. Since by definition of simulation relation, for any transition $x_2 \xrightarrow[2]{u_2} x_2'$ in T_2 there exists a transition $x_1 \xrightarrow[1]{u_1} x_1'$ in T_1 such that $(x_2', x_1') \in \mathcal{R}$, I want to use T_2 that is with fewer transitions than T_1 to find a control strategy enforcing my reachability specification on T_1. By looking at T_2 I found the control strategy: When I am in state 0, I pick either input u

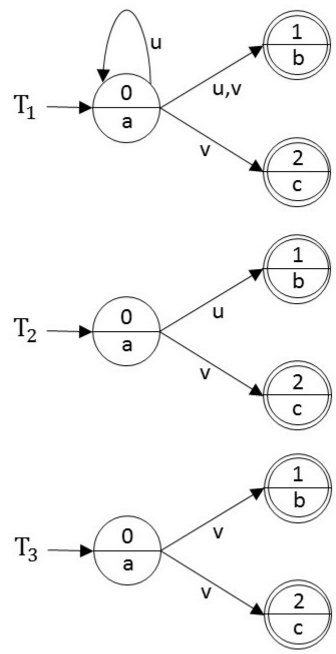

Fig. 3. Transition systems T_1, T_2 and T_3.

or input v; indeed, in both cases I reach states 1 and 2 in one step, as requested by my specification. What happens if I apply this control strategy to T_1? It does not work because starting from 0 and applying input u, I can jump to state 0, thus violating the specification.

The example above shows that simulation relation is not appropriate to address control design for nondeterministic transition systems. This happens because the notion of simulation relation treats disturbances (parametrizing nondeterminism) as cooperative inputs while they need to be considered as adversarial inputs. This problem has been solved in [1] with the notions of alternating simulation and alternating bisimulation relations that we now introduce.

Definition 3. *[1] Let* $T_i = (X_i, X_{0,i}, U_i, \underset{i}{\longrightarrow}, X_{m,i}, Y_i, H_i)$ $(i = 1, 2)$ *be transition systems with the same output sets* $Y_1 = Y_2$*. A relation*

$$\mathcal{R} \subseteq X_1 \times X_2$$

is said to be an alternating simulation relation *from* T_1 *to* T_2 *if it satisfies conditions i), ii) and iii) of Definition 1 and the following one:*

iv') $\forall (x_1, x_2) \in \mathcal{R}\ \forall u_1 \in U_1(x_1)\ \exists u_2 \in U_2(x_2)$ *such that* $\forall x_2 \xrightarrow[2]{u_2} x_2'\ \exists x_1 \xrightarrow[1]{u_1} x_1'$ *such that* $(x_1', x_2') \in \mathcal{R}$*.*

Transition system T_1 is alternatingly simulated by transition system T_2, denoted

$$T_1 \preceq^{\mathrm{alt}} T_2,$$

if there exists an alternating simulation relation from T_1 to T_2.

We now come back to Example 3.

Example 3. (Continued.) Consider the transition system T_3 in Fig. 3. It is easy to see that $T_3 \preceq^{\mathrm{alt}} T_1$ with alternating simulation relation

$$\mathcal{R}' = \{(0,0),(1,1),(2,2)\}.$$

By looking at T_3 I found the control strategy: When I am in state 0, I pick input v. If I apply this control strategy to T_1, it indeed enforces the desired specification. This is because alternating simulation relations consider correctly the role of disturbances.

Definition 4. *[1] Let $T_i = (X_i, X_{0,i}, U_i, \underset{i}{\longrightarrow}, X_{m,i}, Y_i, H_i)$ $(i = 1,2)$ be transition systems with the same output sets $Y_1 = Y_2$. A relation*

$$\mathcal{R} \subseteq X_1 \times X_2$$

is said to be an alternating bisimulation relation between T_1 to T_2 if it satisfies the following conditions:

- *$\mathcal{R}$ is an alternating simulation relation from T_1 to T_2;*
- *$\mathcal{R}^{-1}$ is an alternating simulation relation from T_2 to T_1.*

Transition systems T_1 and T_2 are alternatingly bisimilar, denoted

$$T_1 \cong^{\mathrm{alt}} T_2,$$

if there exists an alternating bisimulation relation $\mathcal{R}$ between T_1 and T_2.

It is easy to see that, as in the non alternating case:

- The notion of alternating simulation is a preorder on the set of transition systems;
- The notion of alternating bisimulation is an equivalence relation on the set of transition systems.

There is no formal relationship between the notions of simulation and bisimulation relations and their alternating variants, as shown in Example 4.21 of [6]. However, as also pointed out in [6]:

Proposition 7. *If T_1 and T_2 are deterministic then $T_1 \preceq T_2$ if and only if $T_1 \preceq^{\mathrm{alt}} T_2$.*

The notion of simulation and bisimulation relations and its alternating variants, we have introduced so far, are also called 'exact' because they require the outputs of two states x_1 and x_2 in the relation to be exactly the same, see condition iii) of Definition 1. We now extend the notion above to an approximating setting where condition

$$H_1(x_1) = H_2(x_2)$$

is replaced by

$$\mathbf{d}(H_1(x_1), H_2(x_2)) \leq \mu,$$

where $\mathbf{d}$ is a metric placed on the output sets of the transition systems involved and $\mu \in \mathbb{R}_0^+$ is a desired accuracy.
We can now give the following

Definition 5. *[2] Let* $T_i = (X_i, X_{0,i}, U_i, \underset{i}{\longrightarrow}, X_{m,i}, Y_i,\ H_i)$ $(i = 1, 2)$ *be metric transition systems with the same output sets* $Y_1 = Y_2$ *and metric* $\mathbf{d}$*, and let* $\mu \in \mathbb{R}_0^+$ *be a given accuracy. A relation*

$$\mathcal{R} \subseteq X_1 \times X_2$$

is said to be a μ*–simulation relation from* T_1 *to* T_2 *if it satisfies properties i), ii) and iv) of Definition 1 and the following one:*

iii') $\forall (x_1, x_2) \in \mathcal{R}$, $\mathbf{d}(H_1(x_1), H_2(x_2)) \leq \mu$.

Metric transition system T_1 *is* μ*–simulated by metric transition system* T_2*, denoted*

$$T_1 \preceq_\mu T_2,$$

if there exists a μ*–simulation relation from* T_1 *to* T_2*.*

Definition 6. *[2] Let* $T_i = (X_i, X_{0,i}, U_i, \underset{i}{\longrightarrow}, X_{m,i}, Y_i,\ H_i)$ $(i = 1, 2)$ *be metric transition systems with the same output sets* $Y_1 = Y_2$ *and metric* $\mathbf{d}$*, and let* $\mu \in \mathbb{R}_0^+$ *be a given accuracy. A relation*

$$\mathcal{R} \subseteq X_1 \times X_2$$

is said to be a μ*-bisimulation relation between* T_1 *to* T_2 *if it satisfies the following conditions:*

- $\mathcal{R}$ *is* μ*–simulation relation from* T_1 *to* T_2*;*
- $\mathcal{R}^{-1}$ *is a* μ*–simulation relation from* T_2 *to* T_1*.*

Metric transition systems T_1 *and* T_2 *are* μ*–bisimilar, denoted*

$$T_1 \cong_\mu T_2,$$

if there exists a μ*–bisimulation relation* $\mathcal{R}$ *between* T_1 *and* T_2*.*

Definition 7. *[5] Let* $T_i = (X_i, X_{0,i}, U_i, \underset{i}{\longrightarrow}, X_{m,i}, Y_i, H_i)$ $(i = 1, 2)$ *be metric transition systems with the same output sets* $Y_1 = Y_2$ *and metric* $\mathbf{d}$*, and let* $\mu \in \mathbb{R}_0^+$ *be a given accuracy. A relation*

$$\mathcal{R} \subseteq X_1 \times X_2$$

is said to be an alternating μ-simulation relation *from* T_1 *to* T_2 *if it satisfies conditions i), ii) and iii') of Definition 5 and condition iv') of Definition 3. Metric transition system* T_1 *is alternatingly* μ*-simulated by metric transition system* T_2*, denoted*

$$T_1 \preceq_{\mu}^{\mathrm{alt}} T_2,$$

if there exists an alternating μ*–simulation relation from* T_1 *to* T_2*.*

Definition 8. *[5] Let* $T_i = (X_i, X_{0,i}, U_i, \underset{i}{\longrightarrow}, X_{m,i}, Y_i, H_i)$ $(i = 1, 2)$ *be metric transition systems with the same output sets* $Y_1 = Y_2$ *and metric* $\mathbf{d}$*, and let* $\mu \in \mathbb{R}_0^+$ *be a given accuracy. A relation*

$$\mathcal{R} \subseteq X_1 \times X_2$$

is said to be an alternating μ*-bisimulation relation between* T_1 *to* T_2 *if it satisfies the following conditions:*

- $\mathcal{R}$ *is an alternating* μ*–simulation relation from* T_1 *to* T_2*;*
- $\mathcal{R}^{-1}$ *is an alternating* μ*–simulation relation from* T_2 *to* T_1*.*

Metric transition systems T_1 *and* T_2 *are alternatingly* μ*–bisimilar, denoted*

$$T_1 \cong_{\mu}^{\mathrm{alt}} T_2,$$

if there exists an alternating μ*–bisimulation relation* $\mathcal{R}$ *between* T_1 *and* T_2*.*

References

1. R. Alur, T. Henzinger, O. Kupferman, and M. Vardi. Alternating refinement relations. In *Proceedings of the 8th International Conference on Concurrence Theory*, number 1466 in Lecture Notes in Computer Science, pages 163–178. Springer, 1998.
2. A. Girard and G.J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, 52(5):782–798, 2007.
3. R. Milner. *Communication and Concurrency.* Prentice Hall, 1989.
4. D.M.R. Park. Concurrency and automata on infinite sequences. volume 104 of *Lecture Notes in Computer Science*, pages 167–183, 1981.
5. G. Pola and P. Tabuada. Symbolic models for nonlinear control systems: Alternating approximate bisimulations. *SIAM Journal on Control and Optimization*, 48(2):719–733, 2009.
6. P. Tabuada. *Verification and Control of Hybrid Systems: A Symbolic Approach.* Springer, 2009.