9

Approximate system relationships

The similarity relationships introduced in Chapter 4 provided the framework upon which most of the abstraction techniques in Part III relied. In this chapter, we take an important conceptual step forward by abandoning the exact nature of these relationships.

Notation

A metric on a set Z is a function $\mathbf{d} : Z \times Z \to \mathbb{R}_0^+$ satisfying: $\mathbf{d}(z, z') = 0$ iff $z = z'$; $\mathbf{d}(z, z') + \mathbf{d}(z', z'') \geq \mathbf{d}(z, z'')$; $\mathbf{d}(z, z') = \mathbf{d}(z', z)$. A metric $\mathbf{d}$ on the set Z induces a distance between points $z \in Z$ and sets $W \subseteq Z$ by $\mathbf{d}(z, W) = \min_{w \in W} \mathbf{d}(z, w)$. This distance can be used to define the ε-inflation of a set $W \subseteq Z$, denoted by W^ε, and defined by $W^\varepsilon = \{z \in Z \mid \mathbf{d}(z, W) \leq \varepsilon\}$ for any $\varepsilon \in \mathbb{R}_0^+$. The set W^ε contains all the points in Z whose distance to W is bounded by ε. Note that $W \subset W^\varepsilon$ since $\mathbf{d}(w, W) = 0$ for any $w \in W$. Every relation $Q \subseteq Z \times W$, admits $Q^{-1} = \{(w, z) \in W \times Z \mid (z, w) \in Q\}$ as its inverse relation.

9.1 Approximate similarity relationships

The notion of simulation relation, formalized in Definition 4.7, requires related states to be sent by the output maps to the same output. It may be argued that such requirement is too strong since in concrete physical systems this exact equality is seldom achieved. Noise in measurements, imprecisions in actuators, and numerical computation errors are some of the factors preventing an exact equality between the outputs. These arguments suggest that one could relax the equality requirement by allowing related states to correspond to different outputs provided that the mismatch is bounded by some desired precision $\varepsilon \in \mathbb{R}_0^+$. To quantify the desired precision we need a metric on the set of outputs.

P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*,
DOI: 10.1007/978-1-4419-0224-5_9,

Definition 9.1 (Metric system). *A system S is said to be a* metric system *if the set of outputs Y is equipped with a metric $\mathbf{d} : Y \times Y \to \mathbb{R}_0^+$.*

When referring to metric systems, equality between two sets of outputs Y_a and Y_b will also imply equality between the corresponding metrics, *i.e.*, $Y_a = Y_b$ entails $\mathbf{d}_a = \mathbf{d}_b$ where $\mathbf{d}_a$ is the metric on Y_a and $\mathbf{d}_b$ is the metric on Y_b. For metric systems it is possible to generalize Definition 4.7 by replacing the second requirement with an approximate version.

Definition 9.2 (Approximate Simulation Relation). *Consider two metric systems S_a and S_b with $Y_a = Y_b$, and let $\varepsilon \in \mathbb{R}_0^+$. A relation $R \subseteq X_a \times X_b$ is an* ε-approximate simulation relation *from S_a to S_b if the following three conditions are satisfied:*

1. *for every $x_{a0} \in X_{a0}$, there exists $x_{b0} \in X_{b0}$ with $(x_{a0}, x_{b0}) \in R$;*
2. *for every $(x_a, x_b) \in R$ we have $\mathbf{d}(H_a(x_a), H_b(x_b)) \leq \varepsilon$;*
3. *for every $(x_a, x_b) \in R$ we have that:*
   $x_a \xrightarrow[a]{u_a} x_a'$ in S_a implies the existence of $x_b \xrightarrow[b]{u_b} x_b'$ in S_b satisfying $(x_a', x_b') \in R$.

We say that S_a is ε-approximately simulated by S_b or that S_b ε-approximately simulates S_a, denoted by $S_a \preceq_S^\varepsilon S_b$, if there exists an ε-approximate simulation relation from S_a to S_b.

When $\varepsilon = 0$ the inequality $\mathbf{d}(H_a(x_a), H_b(x_b)) \leq \varepsilon$ implies $H_a(x_a) = H_b(x_b)$. In this sense, we can regard approximate simulations as a generalization of the exact simulations introduced in Chapter 4. Before proceeding further, we give an example to illustrate this concept.

Example 9.3. Consider the dynamical system Σ described by the differential equation:

$$\frac{d}{dt}\xi = -\xi, \quad \xi(t) \in \mathbb{R}, t \in \mathbb{R}_0^+ \tag{9.1}$$

that can be explicitly integrated to obtain $\xi_x(t) = e^{-t}x$. The closed form expression for ξ is used to show that for any $\varepsilon \in \mathbb{R}_0^+$, the relation $R_\varepsilon \subseteq \mathbb{R} \times \mathbb{R}$ defined by $(x, x') \in R_\varepsilon$ iff $\|x - x'\| \leq \varepsilon$ is an ε-approximate simulation relation from $S(\Sigma)$ to $S(\Sigma)$. Here, $S(\Sigma)$ is the system $(\mathbb{R}, \mathbb{R}_0^+, \longrightarrow)$ defined by $x \xrightarrow{\tau} x'$ if there exists a solution $\xi_x : [0, \tau] \to \mathbb{R}$ of (9.1) satisfying $\xi_x(\tau) = x'$. To see why R_ε is an ε-approximate simulation relation, consider a pair $(x, x') \in R_\varepsilon$ and a transition $x \xrightarrow{\tau} x''$ in $S(\Sigma)$. The definition of $\longrightarrow$ implies $x'' = \xi_x(\tau) = e^{-\tau}x$, and we claim that $(x'', x''') \in R_\varepsilon$ with $x''' = \xi_{x'}(\tau)$, or equivalently, $x' \xrightarrow{\tau} x'''$ in $S(\Sigma)$. To determine if $(x'', x''') \in R_\varepsilon$, we compute:

$$\|x'' - x'''\| = \|\xi_x(\tau) - \xi_{x'}(\tau)\| = \|e^{-\tau}x - e^{-\tau}x'\| \leq \|e^{-\tau}\|\|x - x'\| \leq \|x - x'\| \leq \varepsilon.$$

This simple argument is valid in far greater generality and it is at the heart of all the results to be proved in Part IV. $\lhd$

As the previous example suggests, approximate simulation relations are especially useful for infinite-state systems in which the output set is naturally endowed with a metric. One typical usage of approximate simulation relations is the simplification of verification problems. To understand how such simplification arises, we relate the reachable sets of systems related by approximate simulation relations.

Proposition 9.4. *For any two metric systems S_a and S_b with $Y_a = Y_b$, the following implication holds:*

$$S_a \preceq^{\varepsilon}_{\mathcal{S}} S_b \implies \text{Reach}(S_a) \subseteq \text{Reach}^{\varepsilon}(S_b).$$

Proof. Denote by R the ε-approximate simulation relation from S_a to S_b, and let $y_a \in \text{Reach}(S_a)$. By definition of reachable output, there exists an initialized finite internal behavior of S_a:

$$x_{a0} \xrightarrow[a]{u_{a0}} x_{a1} \xrightarrow[a]{u_{a1}} \cdots \xrightarrow[a]{u_{ak-1}} x_{ak}$$

with $H_a(x_{ak}) = y_a$. Repeating the argument in the proof of Proposition 4.11 we conclude the existence of an initialized internal behavior of S_b:

$$x_{b0} \xrightarrow[b]{u_{b0}} x_{b1} \xrightarrow[b]{u_{b1}} \cdots \xrightarrow[b]{u_{bk-1}} x_{bk}$$

satisfying $(x_{ai}, x_{bi}) \in R$ for $i = 0, 1, \ldots, k$. Hence, $y_b = H_b(x_{bk}) \in \text{Reach}(S_b)$ and it follows from the second requirement in the definition of approximate simulation relation that $\mathbf{d}(y_a, y_b) \leq \varepsilon$. Consequently, $y_a \in \text{Reach}^{\varepsilon}(S_b)$. □

Returning to verification problems, consider a system S_a and a set of unsafe outputs B. If a system S_b ε-approximately simulates system S_a, Proposition 9.4 can be used to conclude that $\text{Reach}^{\varepsilon}(S_b) \cap B = \varnothing$ implies $\text{Reach}(S_a) \cap B = \varnothing$. For reachability problems, showing $\text{Reach}(S_a) \cap Z \neq \varnothing$ for a set Z satisfying $Z^{\varepsilon} \subseteq B$, implies $\text{Reach}(S_b) \cap B \neq \varnothing$. Clearly, these implications are only useful if we are able to construct abstractions based on ε-approximate simulation relations that are simpler than the systems they abstract. In Chapters 10 and 11 we discuss the existence and construction of such abstractions. Before, however, we strengthen approximate simulation to approximate bisimulation.

Definition 9.5 (Approximate bisimulation). *Consider two metric systems S_a and S_b with $Y_a = Y_b$, and let $\varepsilon \in \mathbb{R}^+_0$. We say that system S_a is* ε-approximately bisimilar *to system S_b, denoted by $S_a \cong^{\varepsilon}_{\mathcal{S}} S_b$, if there exists a relation R satisfying:*

1. *R is an ε-approximate simulation relation from S_a to S_b;*
2. *R^{-1} is an ε-approximate simulation relation from S_b to S_a.*

Some care needs to be exerted when composing approximate (bi)simulation relations. Although it is a simple exercise to show that the composition of approximate (bi)simulation relations results in an approximate (bi)simulation relation, the precision is altered by composition. In detail, if ${}_aR_b$ is an ${}_a\varepsilon_b$-approximate (bi)simulation relation from S_a to S_b and if ${}_bR_c$ is an ${}_b\varepsilon_c$-approximate (bi)simulation relation from S_b to S_c, the composite ${}_bR_c \circ {}_aR_b$ is an $({}_a\varepsilon_b + {}_b\varepsilon_c)$-approximate (bi)simulation relation from S_a to S_c.

9.2 Approximate alternating similarity relationships

When discussing problems of control, ε-approximate similarity relationships need to be replaced with ε-approximate alternating similarity relationships. This generalization from exact to approximate consists again in relaxing the equality requirement on the outputs of related states.

Definition 9.6 (Approximate alternating simulation relation). *Let S_a and S_b be metric systems with $Y_a = Y_b$ and let $\varepsilon \in \mathbb{R}_0^+$. A relation $R \subseteq X_a \times X_b$ is an* ε-approximate alternating simulation relation *from S_a to S_b if the following three conditions are satisfied:*

1. *for every $x_{a0} \in X_{a0}$ there exists $x_{b0} \in X_{b0}$ with $(x_{a0}, x_{b0}) \in R$;*
2. *for every $(x_a, x_b) \in R$ we have $\mathbf{d}(H_a(x_a), H_b(x_b)) \leq \varepsilon$;*
3. *for every $(x_a, x_b) \in R$ and for every $u_a \in U_a(x_a)$ there exists $u_b \in U_b(x_b)$ such that for every $x'_b \in \mathrm{Post}_{u_b}(x_b)$ there exists $x'_a \in \mathrm{Post}_{u_a}(x_a)$ satisfying $(x'_a, x'_b) \in R$.*

We say that S_a is ε-approximately alternatingly simulated by S_b or that S_b ε-approximately alternatingly simulates S_a, denoted by $S_a \preceq^{\varepsilon}_{\mathcal{AS}} S_b$, if there exists an ε-approximate alternating simulation relation from S_a to S_b.

Approximate alternating simulation relations are used to define approximate feedback composition in Chapter 11. To that purpose, we introduce now the extended ε-approximate alternating simulation relation associated with an ε-approximate alternating simulation relation.

Definition 9.7 (Extended approximate alternating simulation relation). *Let R be an ε-approximate alternating simulation relation from metric system S_a to metric system S_b. The* extended ε-approximate alternating simulation relation $R^e \subseteq X_a \times X_b \times U_a \times U_b$ *associated with R is defined by all the quadruples $(x_a, x_b, u_a, u_b) \in X_a \times X_b \times U_a \times U_b$ for which the following three conditions hold:*

1. *$(x_a, x_b) \in R$;*
2. *$u_a \in U_a(x_a)$;*
3. *$u_b \in U_b(x_b)$ and for every $x'_b \in \mathrm{Post}_{u_b}(x_b)$ there exists $x'_a \in \mathrm{Post}_{u_a}(x_a)$ satisfying $(x'_a, x'_b) \in R$.*

Note that the third requirement in the previous definition is no more than the third requirement in Definition 9.6.

Approximate alternating bisimulations can be obtained by introducing the adjective approximate in the definition of alternating bisimulation or by symmetrizing the definition of approximate alternating simulation.

Definition 9.8 (Approximate alternating bisimulation). *Given two metric systems S_a and S_b with $Y_a = Y_b$, and given $\varepsilon \in \mathbb{R}_0^+$, we say that S_a is ε-approximately alternatingly bisimilar to S_b, denoted by $S_a \cong^{\varepsilon}_{\mathcal{AS}} S_b$, if there exists a relation R satisfying:*

1. *R is an ε-approximate alternating simulation relation from S_a to S_b;*
2. *R^{-1} is an ε-approximate alternating simulation relation from S_b to S_a.*

Approximate alternating simulations and bisimulations are instrumental to refine controllers synthesized for symbolic abstractions based on approximate simulations and bisimulations. We return to this topic in Chapter 11.

9.3 Notes

Approximate equivalence was first discussed in the context of timed-automata [GHJ97] and probabilistic systems [DGJP99]. In both cases, it was formalized by resorting to metrics and metric systems. Although in a different context, metric systems had been studied much earlier, see for example [vB98]. Most of the work that followed the papers [GHJ97, DGJP99] focused on probabilistic systems and the notion of approximate simulation for dynamical and control systems only appeared recently. In [GP05, GP07], approximate bisimulation was introduced by resorting to a metric on the set of outputs. A different formalization of approximate simulation appeared in [Tab05, Tab06] through the use of set-valued output maps. The discussion in this chapter is based on [GP07, PGT08].