Formal verification - Tutorial 05

23/03/2026

Simplifying transitions

Exercise 1. *Consider a nondeterministic finite automaton A. Let $\sqsubseteq$ be any underapproximation of the language inclusion preorder: $p \sqsubseteq q$ implies $L(p) \subseteq L(q)$. Can we use $\sqsubseteq$ to simplify the transition structure of the automaton?*

Solution. For each state $p \in Q$ and input symbol $a \in \Sigma$, it suffices to consider only transitions $p \xrightarrow{a} q$ where q is $\sqsubseteq$-maximal. □

Simulation relations

Exercise 2. *Fix an automaton A. Show that*

1. *The identity relation $\{(p, p) \mid p \in Q\}$ is a simulation.*
2. *The union of an arbitrary family of simulations is a simulation.*
3. *The composition of two simulations is a simulation.*

Solution. The first point is trivial. For the second point, let $\{R_i\}_{i \in I}$ be a family of simulations and consider their union $R = \bigcup_{i \in I} R_i$. We show that R is a simulation. Let $(p, q) \in R$ and $p \xrightarrow{a} p'$. By definition of R, there exists $i \in I$ such that $(p, q) \in R_i$. Since R_i is a simulation, there exists q' such that $q \xrightarrow{a} q'$ and $(p', q') \in R_i$. Since $R_i \subseteq R$, we have $(p', q') \in R$, as required. For the third point, let R and S be two simulations and consider their composition $R \circ S$. We show that $R \circ S$ is a simulation. Let $(p, q) \in R \circ S$ and $p \xrightarrow{a} p'$. By definition of composition, there exists r such that $(p, r) \in R$ and $(r, q) \in S$. Since R is a simulation, there exists r' such that $r \xrightarrow{a} r'$ and $(p', r') \in R$. Since S is a simulation, there exists q' such that $q \xrightarrow{a} q'$ and $(r', q') \in S$. Since $(p', r') \in R$ and $(r', q') \in S$, we have $(p', q') \in R \circ S$, as required. □

Exercise 3. *Fix an automaton A. Let $\preceq$ be the union of all simulations on A.*

1. *Show that $\preceq$ is a simulation.*
2. *Show that $\preceq$ is a preorder.*

Solution. □

Exercise 4. *Let A be a total deterministic automaton. Show that the language inclusion preorder on A coincides with the simulation preorder $\preceq$.*

Solution. It suffices to show that language inclusion is a simulation. Consider a pair of states (p, q) such that $L(p) \subseteq L(q)$. Consider a transition $p \xrightarrow{a} p'$. Since the automaton is total and deterministic, there exists a unique transition $q \xrightarrow{a} q'$ from q on input a. Let $w \in L(p')$. Then, $aw \in L(p)$ and thus $aw \in L(q)$ by the assumption. Since the automaton is deterministic, $w \in L(q')$, as required. □

Exercise 5. *Show an example of an automaton A s.t. simulation preorder $\preceq$ is* strictly included *in the language inclusion preorder.*

Solution. By the previous exercise we know that A must be nondeterministic. Consider the automaton A with states p, q, r and p', q_b, q_c, r. State r is accepting. There are transitions $p \xrightarrow{a} q \xrightarrow{b,c} r$ and $p' \xrightarrow{a} q_b$, $p' \xrightarrow{a} q_c$, $q_b \xrightarrow{b} r$, $q_c \xrightarrow{c} r$. Clearly $L(p) = L(p') = \{ab, ab\}$ however p' does not simulate p. □

Exercise 6. *Let A be a nondeterministic finite automaton with states Q and consider its (deterministic) powerset automaton B with states $\mathcal{P}(Q)$. Consider the state-inclusion preorder $\subseteq$ on the states of B.*

1. *Show that $\subseteq$ is a simulation on B.*
2. *Does $\subseteq$ coincide with the simulation preorder on B?*
3. *Is there a way to* lift *simulation preorder on A to a simulation relation on B coarser than the state-inclusion preorder $\subseteq$?*

Solution. The first point follows directly from the definition of the powerset automaton. For the second point, we provide an example that simulation preorder on B can be strictly coarser than $\subseteq$. In fact, it suffices to consider a deterministic automaton A ($= B$) and two distinct states p and q s.t. q simulates p. For the third point, one can consider a binary relation on powerset states $p, q \subseteq Q$ defined as $p \preceq q$ iff for all $p' \in p$ there exists $q' \in q$ such that $p' \sqsubseteq q'$ in the simulation preorder on A. □

Exercise 7. *Fix a nondeterministic finite automaton A with states Q and consider the following operator T on binary relations on Q: For a binary relation $R \subseteq Q \times Q$, we have $(p, q) \in T(R)$ iff*

(a) $p \in F$ implies $q \in F$, and

(b) For all transitions $p \xrightarrow{a} p'$, there exists a transition $q \xrightarrow{a} q'$ s.t. $(p', q') \in R$.

1. *Show that the operator T is monotone w.r.t. set inclusion.*
2. *Show that R is a simulation iff R is a* post-fixpoint *of T, i.e., $R \subseteq T(R)$.*
3. *Show that simulation preorder $\preceq$ is the greatest (post-)fixpoint of T.*
4. *Use the previous points to design an algorithm to compute the simulation preorder on A.*

Solution. The first point is straightforward. The second point follows directly from the definition of simulation. THe third point follows from fixed point theory. This leads us to the last point. We design a Kleene iteration scheme to compute the greatest fixpoint of T. For every $n \in \mathbb{N}$, let $R_n := T^n(Q \times Q)$. For instance, we have $R_0 = Q \times Q$ and $R_1 = F \times F \cup (Q \backslash F) \times Q$. By monotonicity of T,

we have a nonincreasing chain $R_0 \supseteq R_1 \supseteq R_2 \supseteq \cdots$. Then $\preceq = \bigcap_{n\in\mathbb{N}} R_n$ is the greatest fixpoint of T and thus the simulation preorder on A. The computation terminates since $R_n = R_{n+1} = \cdots$ for some $n \leqslant |Q|^2$. □

Bisimulation relations

Exercise 8. *Show an example of an automaton A and a pair of states p, q such that p simulates q and q simulates p but p and q are not bisimilar.*

Solution. The crucial point is that for R to be a bisimulation it needs to be the case that both R and its inverse R^{-1} are simulations. However, two states p and q can simulate each other via two *different* simulations R and S. □