Program Verification: Lecture 25

José Meseguer
University of Illinois at Urbana-Champaign

Simulation and Bisimulation Maps of Transition Systems

Given two transition systems $\mathcal{A} = (A, \rightarrow_{\mathcal{A}})$ and $\mathcal{B} = (B, \rightarrow_{\mathcal{B}})$, a simulation map f from $\mathcal{A}$ to $\mathcal{B}$, denoted $f : \mathcal{A} \rightarrow \mathcal{B}$, is a function $f : A \rightarrow B$ that is "transition preserving" in the sense that any transition $a \rightarrow_{\mathcal{A}} a'$ in $\mathcal{A}$ is mapped by f to a corresponding transition $f(a) \rightarrow_{\mathcal{B}} f(a')$ in $\mathcal{B}$.

Simulation and Bisimulation Maps of Transition Systems

Given two transition systems $\mathcal{A} = (A, \to_{\mathcal{A}})$ and $\mathcal{B} = (B, \to_{\mathcal{B}})$, a simulation map f from $\mathcal{A}$ to $\mathcal{B}$, denoted $f : \mathcal{A} \to \mathcal{B}$, is a function $f : A \to B$ that is "transition preserving" in the sense that any transition $a \to_{\mathcal{A}} a'$ in $\mathcal{A}$ is mapped by f to a corresponding transition $f(a) \to_{\mathcal{B}} f(a')$ in $\mathcal{B}$.

A simulation map $f : \mathcal{A} \to \mathcal{B}$ is called a bisimulation iff, in addition, for any state of the form $f(a) \in B$ and any transition $f(a) \to_{\mathcal{B}} b$ there exists and $a' \in A$ and transition $a \to_{\mathcal{A}} a'$ such that $f(a') = b$.

Simulation and Bisimulation Maps of Transition Systems

Given two transition systems $\mathcal{A} = (A, \to_{\mathcal{A}})$ and $\mathcal{B} = (B, \to_{\mathcal{B}})$, a simulation map f from $\mathcal{A}$ to $\mathcal{B}$, denoted $f : \mathcal{A} \to \mathcal{B}$, is a function $f : A \to B$ that is "transition preserving" in the sense that any transition $a \to_{\mathcal{A}} a'$ in $\mathcal{A}$ is mapped by f to a corresponding transition $f(a) \to_{\mathcal{B}} f(a')$ in $\mathcal{B}$.

A simulation map $f : \mathcal{A} \to \mathcal{B}$ is called a bisimulation iff, in addition, for any state of the form $f(a) \in B$ and any transition $f(a) \to_{\mathcal{B}} b$ there exists and $a' \in A$ and transition $a \to_{\mathcal{A}} a'$ such that $f(a') = b$.

Given a transition system $\mathcal{A} = (A, \to_{\mathcal{A}})$ and subsets $U, V \subseteq A$, we are interested in the reachability property:

$$\exists x \in U,\ \exists y \in V,\ x \to_{\mathcal{A}}^{*} y$$

which we abbreviate to $\exists U \to^{*} V$. If this property holds for specific $U, V \subseteq A$ we write: $\mathcal{A} \models \exists U \to^{*} V$.

Simulation and Bisimulation Maps of Transition Systems

Given two transition systems $\mathcal{A} = (A, \to_{\mathcal{A}})$ and $\mathcal{B} = (B, \to_{\mathcal{B}})$, a simulation map f from $\mathcal{A}$ to $\mathcal{B}$, denoted $f : \mathcal{A} \to \mathcal{B}$, is a function $f : A \to B$ that is "transition preserving" in the sense that any transition $a \to_{\mathcal{A}} a'$ in $\mathcal{A}$ is mapped by f to a corresponding transition $f(a) \to_{\mathcal{B}} f(a')$ in $\mathcal{B}$.

A simulation map $f : \mathcal{A} \to \mathcal{B}$ is called a bisimulation iff, in addition, for any state of the form $f(a) \in B$ and any transition $f(a) \to_{\mathcal{B}} b$ there exists and $a' \in A$ and transition $a \to_{\mathcal{A}} a'$ such that $f(a') = b$.

Given a transition system $\mathcal{A} = (A, \to_{\mathcal{A}})$ and subsets $U, V \subseteq A$, we are interested in the reachability property:

$$\exists x \in U,\ \exists y \in V,\ x \to^*_{\mathcal{A}} y$$

which we abbreviate to $\exists U \to^* V$. If this property holds for specific $U, V \subseteq A$ we write: $\mathcal{A} \models \exists U \to^* V$. Note that $\mathcal{A} \not\models \exists U \to^* V$ iff $\forall x \in U,\ \forall y \in V,\ x \not\to^*_{\mathcal{A}} y$ holds in $\mathcal{A}$, abbreviated $\mathcal{A} \models \forall U \not\to^* V$.

Preservation of Reachability Properties by (Bi)Simulations

The proofs of these two theorems are given in the Appendix.

Preservation of Reachability Properties by (Bi)Simulations

The proofs of these two theorems are given in the Appendix.

Theorem

Let $f : \mathcal{A} \rightarrow \mathcal{B}$ be a simulation map, then for any $U, V \subseteq A$, $\mathcal{A} \models \exists U \rightarrow^{*} V$ implies $\mathcal{B} \models \exists f(U) \rightarrow^{*} f(V)$. Equivalently, $\mathcal{B} \models \forall f(U) \not\rightarrow^{*} f(V)$ implies $\mathcal{A} \models \forall U \not\rightarrow^{*} V$.

Preservation of Reachability Properties by (Bi)Simulations

The proofs of these two theorems are given in the Appendix.

Theorem

Let $f : \mathcal{A} \to \mathcal{B}$ be a simulation map, then for any $U, V \subseteq A$, $\mathcal{A} \models \exists U \to^* V$ implies $\mathcal{B} \models \exists f(U) \to^* f(V)$. Equivalently, $\mathcal{B} \models \forall f(U) \not\to^* f(V)$ implies $\mathcal{A} \models \forall U \not\to^* V$.

Theorem

Let $f : \mathcal{A} \to \mathcal{B}$ be a bisimulation map, then for any $U, V \subseteq A$, $\mathcal{A} \models \exists U \to^* V$ iff $\mathcal{B} \models \exists f(U) \to^* f(V)$. Equivalently, $\mathcal{A} \models \forall U \not\to^* V$ iff $\mathcal{B} \models \forall f(U) \not\to^* f(V)$.

Preservation of Reachability Properties by (Bi)Simulations

The proofs of these two theorems are given in the Appendix.

Theorem

Let $f : \mathcal{A} \to \mathcal{B}$ *be a simulation map, then for any* $U, V \subseteq A$, $\mathcal{A} \models \exists U \to^* V$ *implies* $\mathcal{B} \models \exists f(U) \to^* f(V)$. *Equivalently,* $\mathcal{B} \models \forall f(U) \not\to^* f(V)$ *implies* $\mathcal{A} \models \forall U \not\to^* V$.

Theorem

Let $f : \mathcal{A} \to \mathcal{B}$ *be a bisimulation map, then for any* $U, V \subseteq A$, $\mathcal{A} \models \exists U \to^* V$ *iff* $\mathcal{B} \models \exists f(U) \to^* f(V)$. *Equivalently,* $\mathcal{A} \models \forall U \not\to^* V$ *iff* $\mathcal{B} \models \forall f(U) \not\to^* f(V)$.

Note the for $U, I \subseteq A$, I is an invariant from U iff $\mathcal{A} \models \forall U \not\to^* A \setminus I$. Thus, we can verify the invariant by proving $\mathcal{B} \models \forall f(U) \not\to^* f(A \setminus I)$.

Preservation of Reachability Properties by (Bi)Simulations

The proofs of these two theorems are given in the Appendix.

Theorem

Let $f : \mathcal{A} \to \mathcal{B}$ be a simulation map, then for any $U, V \subseteq A$, $\mathcal{A} \models \exists U \to^* V$ implies $\mathcal{B} \models \exists f(U) \to^* f(V)$. Equivalently, $\mathcal{B} \models \forall f(U) \not\to^* f(V)$ implies $\mathcal{A} \models \forall U \not\to^* V$.

Theorem

Let $f : \mathcal{A} \to \mathcal{B}$ be a bisimulation map, then for any $U, V \subseteq A$, $\mathcal{A} \models \exists U \to^* V$ iff $\mathcal{B} \models \exists f(U) \to^* f(V)$. Equivalently, $\mathcal{A} \models \forall U \not\to^* V$ iff $\mathcal{B} \models \forall f(U) \not\to^* f(V)$.

Note the for $U, I \subseteq A$, I is an invariant from U iff $\mathcal{A} \models \forall U \not\to^* A \setminus I$. Thus, we can verify the invariant by proving $\mathcal{B} \models \forall f(U) \not\to^* f(A \setminus I)$. But we could have $\mathcal{B} \models \exists f(U) \to^* f(A \setminus I)$, while $\mathcal{A} \models \forall U \not\to^* A \setminus I$ (spurious counterexample).

Preservation of Reachability Properties by (Bi)Simulations

The proofs of these two theorems are given in the Appendix.

Theorem

Let $f : \mathcal{A} \to \mathcal{B}$ be a simulation map, then for any $U, V \subseteq A$, $\mathcal{A} \models \exists U \to^* V$ implies $\mathcal{B} \models \exists f(U) \to^* f(V)$. Equivalently, $\mathcal{B} \models \forall f(U) \not\to^* f(V)$ implies $\mathcal{A} \models \forall U \not\to^* V$.

Theorem

Let $f : \mathcal{A} \to \mathcal{B}$ be a bisimulation map, then for any $U, V \subseteq A$, $\mathcal{A} \models \exists U \to^* V$ iff $\mathcal{B} \models \exists f(U) \to^* f(V)$. Equivalently, $\mathcal{A} \models \forall U \not\to^* V$ iff $\mathcal{B} \models \forall f(U) \not\to^* f(V)$.

Note the for $U, I \subseteq A$, I is an invariant from U iff $\mathcal{A} \models \forall U \not\to^* A \setminus I$. Thus, we can verify the invariant by proving $\mathcal{B} \models \forall f(U) \not\to^* f(A \setminus I)$. But we could have $\mathcal{B} \models \exists f(U) \to^* f(A \setminus I)$, while $\mathcal{A} \models \forall U \not\to^* A \setminus I$ (spurious counterexample). However, if f is a bisimulation no spurious counterexamples can exist.

Equational Abstractions

Simulation and bisimulation maps can be very useful to verify properties of concurrent systems specified as (not necessarily topmost) rewrite theories $\mathcal{R} = (\Sigma, E \cup B, R)$, not by reasoning directly on $\mathcal{R}$, but by shifting our ground and reasoning on a quotient of $\mathcal{R}$.

Equational Abstractions

Simulation and bisimulation maps can be very useful to verify properties of concurrent systems specified as (not necessarily topmost) rewrite theories $\mathcal{R} = (\Sigma, E \cup B, R)$, not by reasoning directly on $\mathcal{R}$, but by shifting our ground and reasoning on a quotient of $\mathcal{R}$. Specifically, we can add more equations, say $G = E' \cup B'$ to $\mathcal{R}$ to identify more states.

Equational Abstractions

Simulation and bisimulation maps can be very useful to verify properties of concurrent systems specified as (not necessarily topmost) rewrite theories $\mathcal{R} = (\Sigma, E \cup B, R)$, not by reasoning directly on $\mathcal{R}$, but by shifting our ground and reasoning on a quotient of $\mathcal{R}$. Specifically, we can add more equations, say $G = E' \cup B'$ to $\mathcal{R}$ to identify more states. We then call the resulting rewrite theory $(\Sigma, E \cup B \cup G, R)$ an equational abstraction of $\mathcal{R}$, denoted $\mathcal{R}/G$.

Equational Abstractions

Simulation and bisimulation maps can be very useful to verify properties of concurrent systems specified as (not necessarily topmost) rewrite theories $\mathcal{R} = (\Sigma, E \cup B, R)$, not by reasoning directly on $\mathcal{R}$, but by shifting our ground and reasoning on a quotient of $\mathcal{R}$. Specifically, we can add more equations, say $G = E' \cup B'$ to $\mathcal{R}$ to identify more states. We then call the resulting rewrite theory $(\Sigma, E \cup B \cup G, R)$ an equational abstraction of $\mathcal{R}$, denoted $\mathcal{R}/G$.

The following theorem follows trivially from the fact that if $t \rightarrow_{R/E \cup B} t'$, then, a fortiori, $t \rightarrow_{R/E \cup B \cup G} t'$.

Equational Abstractions

Simulation and bisimulation maps can be very useful to verify properties of concurrent systems specified as (not necessarily topmost) rewrite theories $\mathcal{R} = (\Sigma, E \cup B, R)$, not by reasoning directly on $\mathcal{R}$, but by shifting our ground and reasoning on a quotient of $\mathcal{R}$. Specifically, we can add more equations, say $G = E' \cup B'$ to $\mathcal{R}$ to identify more states. We then call the resulting rewrite theory $(\Sigma, E \cup B \cup G, R)$ an equational abstraction of $\mathcal{R}$, denoted $\mathcal{R}/G$.

The following theorem follows trivially from the fact that if $t \rightarrow_{R/E \cup B} t'$, then, a fortiori, $t \rightarrow_{R/E \cup B \cup G} t'$.

Theorem

Given a rewrite theory $\mathcal{R} = (\Sigma, E \cup B, R)$, Σ-equations $G = E' \cup B'$, and a top sort State, the unique surjective Σ-homomorphism $[\_]_{E \cup B \cup G} : \mathbb{T}_{\Sigma/E \cup B} \rightarrow \mathbb{T}_{\Sigma/E \cup B \cup G}$ induces a simulation map $[\_]_{E \cup B \cup G} : (T_{\Sigma/E \cup B, State}, \rightarrow_{R/E \cup B}) \rightarrow (T_{\Sigma/E \cup B \cup G, State}, \rightarrow_{R/E \cup B \cup G})$.

Equational Abstractions (II)

Equational abstractions can make the set of reachable states from an initial state *init* finite. In this way, invariants and, more generally, LTL properties that cannot be verified by explicit-state model checking can be verified using an equational abstraction $\mathcal{R}/G$.

Equational Abstractions (II)

Equational abstractions can make the set of reachable states from an initial state $init$ finite. In this way, invariants and, more generally, LTL properties that cannot be verified by explicit-state model checking can be verified using an equational abstraction $\mathcal{R}/G$.

I refer to §12.4 and §13.4 of *All About Maude* for further details on the use of equational abstraction for explicit-state model checking of (respectively) invariants and LTL properties.

Equational Abstractions (II)

Equational abstractions can make the set of reachable states from an initial state *init* finite. In this way, invariants and, more generally, LTL properties that cannot be verified by explicit-state model checking can be verified using an equational abstraction $\mathcal{R}/G$.

I refer to §12.4 and §13.4 of *All About Maude* for further details on the use of equational abstraction for explicit-state model checking of (respectively) invariants and LTL properties.

In what follows we shall focus on the use of equational abstractions for symbolic model checking. Therefore, I will assume a topmost rewrite theory $\mathcal{R} = (\Sigma, E \cup B, R)$ such that $E \cup B$ is FVP. We shall then be interested in equational abstractions of the form $\mathcal{R}/G$, where $G = E' \cup B'$ is such that $E \cup E' \cup B \cap B'$ is also FVP modulo $B \cap B'$.

Equational Abstractions (II)

Equational abstractions can make the set of reachable states from an initial state *init* finite. In this way, invariants and, more generally, LTL properties that cannot be verified by explicit-state model checking can be verified using an equational abstraction $\mathcal{R}/G$.

I refer to §12.4 and §13.4 of *All About Maude* for further details on the use of equational abstraction for explicit-state model checking of (respectively) invariants and LTL properties.

In what follows we shall focus on the use of equational abstractions for symbolic model checking. Therefore, I will assume a topmost rewrite theory $\mathcal{R} = (\Sigma, E \cup B, R)$ such that $E \cup B$ is FVP. We shall then be interested in equational abstractions of the form $\mathcal{R}/G$, where $G = E' \cup B'$ is such that $E \cup E' \cup B \cap B'$ is also FVP modulo $B \cap B'$.

Since for each pattern term with variables p, the quotient homomorphism $[\_]_{E \cup B \cup G} : \mathbb{T}_{\Sigma/E \cup B}(X) \to \mathbb{T}_{\Sigma/E \cup B \cup G}(X)$ maps each $[p]_{E \cup B}$ to $[p]_{E \cup B \cup G}$, p in $\mathcal{R}/G$ just describes the image under $[\_]_{E \cup B \cup G}$ of p in $\mathcal{R}$ as the symbolic description of the set $[\![p]\!]_{\mathcal{R}}$ of all $E \cup B$-equivalence classes of ground instances of p, which is just $[\![p]\!]_{\mathcal{R}/G}$.

Equational Abstractions (III)

In particular, if the complement of an invariant I in $\mathcal{R}$ is symbolically described by a finite set of pattern terms $p_1, \ldots, p_k$, in case the symbolic state space to reach an instance of some p_i from a symbolic initial state u is infinite, we can use a topmost equational abstraction $\mathcal{R}/G$ whose equations are FVP to try to make the symbolic search space finite.

Equational Abstractions (III)

In particular, if the complement of an invariant I in $\mathcal{R}$ is symbolically described by a finite set of pattern terms $p_1, \ldots, p_k$, in case the symbolic state space to reach an instance of some p_i from a symbolic initial state u is infinite, we can use a topmost equational abstraction $\mathcal{R}/G$ whose equations are FVP to try to make the symbolic search space finite.

Then, by the first Theorem in pg. 3 of this 3 of this lecture, we can use symbolic model checking from a symbolic initial state u to show in $\mathcal{R}/G$ that $\forall u \not\to^* p_i$, $1 \leq i \leq k$. However, in some cases we might get some spurious counterexample.

Equational Abstractions (III)

In particular, if the complement of an invariant I in $\mathcal{R}$ is symbolically described by a finite set of pattern terms $p_1, \ldots, p_k$, in case the symbolic state space to reach an instance of some p_i from a symbolic initial state u is infinite, we can use a topmost equational abstraction $\mathcal{R}/G$ whose equations are FVP to try to make the symbolic search space finite.

Then, by the first Theorem in pg. 3 of this 3 of this lecture, we can use symbolic model checking from a symbolic initial state u to show in $\mathcal{R}/G$ that $\forall u \not\to^* p_i$, $1 \leq i \leq k$. However, in some cases we might get some spurious counterexample.

But by the second Theorem in page 3 of this lecture, no spurious counterexamples will exist if the homomorphism $[\_]_{E \cup B \cup G} : \mathbb{T}_{\Sigma/E \cup B} \to \mathbb{T}_{\Sigma/E \cup B \cup G}$ actually defines a bisimulation. I shall focus on bisimulations in what follows.

Bisimilar Equational Abstractions

We say that an equational abstraction $\mathcal{R}/G$ defines an bisimilar equational abstraction of $\mathcal{R}$ iff the simulation map

$$[\_]_{E \cup B \cup G} : (T_{\Sigma/E \cup B, State}, \rightarrow_{R/E \cup B}) \rightarrow (T_{\Sigma/E \cup B \cup G, State}, \rightarrow_{R/E \cup B \cup G})$$

is actually a bisimulation.

Bisimilar Equational Abstractions

We say that an equational abstraction $\mathcal{R}/G$ defines an bisimilar equational abstraction of $\mathcal{R}$ iff the simulation map

$$[\_]_{E \cup B \cup G} : (T_{\Sigma/E \cup B, State}, \rightarrow_{R/E \cup B}) \rightarrow (T_{\Sigma/E \cup B \cup G, State}, \rightarrow_{R/E \cup B \cup G})$$

is actually a bisimulation. We are interested in finding checkable conditions ensuring that G defines a bisimilar equational abstraction. See the Appendix for a proof of the following theorem:

Bisimilar Equational Abstractions

We say that an equational abstraction $\mathcal{R}/G$ defines an bisimilar equational abstraction of $\mathcal{R}$ iff the simulation map

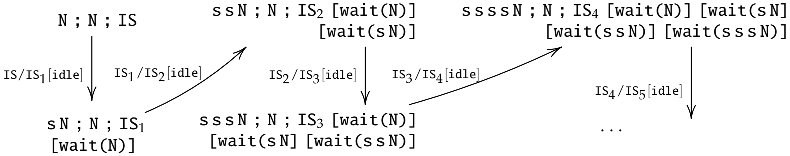
$$[\_]_{E \cup B \cup G} : (T_{\Sigma/E \cup B, State}, \rightarrow_{R/E \cup B}) \rightarrow (T_{\Sigma/E \cup B \cup G, State}, \rightarrow_{R/E \cup B \cup G})$$

is actually a bisimulation. We are interested in finding checkable conditions ensuring that G defines a bisimilar equational abstraction. See the Appendix for a proof of the following theorem:

Theorem

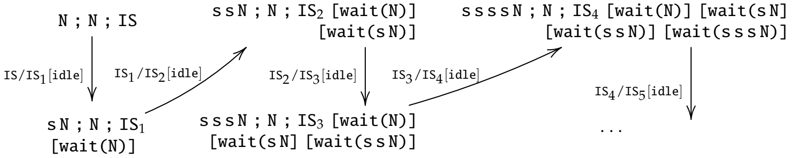
Let $\mathcal{R} = (\Sigma, E \cup B, R)$ be a topmost rewrite theory such that $G = E \cup B$ is FVP, and $G' = E' \cup B'$ is such that $E \cup E' \cup B \cup B'$ is FVP modulo $B \cup B'$. $\mathcal{R}/G'$ defines a bisimilar equational abstraction of $\mathcal{R}$ if for each $(u_0^i = u_1^i) \in G'$, $1 \leq i \leq p$, and $(t_0^j \rightarrow t_1^j) \in R$, $1 \leq j \leq q$, and each $\sigma \in Unif_G(t_{b'}^j = u_b^i)$, $0 \leq b \leq 1$, $0 \leq b' \leq 1$, there exists a θ such that $u_{b' \oplus 1}^i \sigma =_G t_b^j \theta \ \wedge \ t_{b \oplus 1}^j \theta =_G t_{b \oplus 1}^j \sigma$, where $\oplus$ denotes exclusive or.

Bakery Algorithm: Infinite-State for some Initial States



(Infinite Folding Logical Transition System : infinite initial state - infinite state space)

Bakery Algorithm: Infinite-State for some Initial States



(Infinite Folding Logical Transition System : infinite initial state - infinite state space)

- Many verification problems for infinite-state systems are due to unbounded number of processes
- All approaches use a symbolic finite representation of an infinite number of processes
- Bisimulation proofs written by hand or hard to reuse

An Equational Abstraction of the Bakery Algorithm

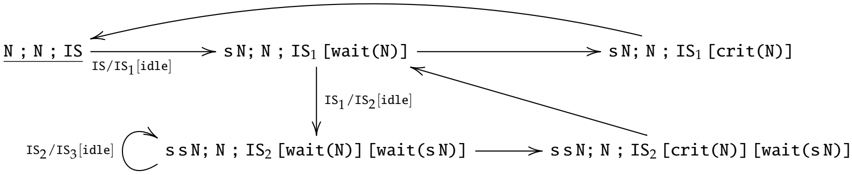
- For our bakery protocol we can obtain a bisimilar equational abstraction by restricting the abstraction only to the following equation G', which intuitively collapses extra waiting processes that does not introduce any new behaviors:

An Equational Abstraction of the Bakery Algorithm

- For our bakery protocol we can obtain a bisimilar equational abstraction by restricting the abstraction only to the following equation G', which intuitively collapses extra waiting processes that does not introduce any new behaviors:
- G':

  $\texttt{eq (s s s L M) ; M ; PS}_0\ \texttt{[wait(s L M)] [wait(s s L M)]}$

  $\texttt{= (s s L M) ; M ; PS}_0\ \texttt{[wait(s L M)] .}$



(Abstract Bisimilar Folding Logical Transition System)