Transition System

Define transition system as (S, I, r, A):

- S - the set containing all states of the system.
  If S is finite, we have a *finite-state system*
- $I \subseteq S$ is the set of possible initial states of the system
- $r \subseteq S \times A \times S$ - transition relation; $(s, a, s') \in r$ means:
  with the environment signal a, system can move in one step from state s to s'
  - we mostly assume that a is the input to the system
  - in the special case that $r : S \times A \rightarrow S$, we say the system is *deterministic*
- A - set of signals with which the system communicates with the environment

A Trace of the System $M = (S, I, r, A)$

A finite or infinite sequence $s_0, a_0, s_1, a_1, s_2, \ldots$ starting from $s_0 \in I$ with steps given by r:

$$
\begin{array}{cc}
\boxed{s_0} & s_0 \in I \\
\downarrow a_0 & a_0 \in A \\
\boxed{s_1} & (s_0, a_0, s_1) \in r \\
\downarrow a_1 & a_1 \in A \\
\boxed{s_2} & (s_1, a_1, s_2) \in r \\
\ldots &
\end{array}
$$

In general, we require $(s_i, a_i, s_{i+1}) \in r$ for all i in the length of the sequence.

Two Systems with Common Alphabet

$M_1 = (S_1, I_1, r_1, A)$ $\qquad$ $M_2 = (S_2, I_2, r_2, A)$

$\boxed{s_0}$	$s_0 \in I_1$	$\boxed{t_0}$	$t_0 \in I_2$
$\downarrow a_0$	$a_0 \in A$	$\downarrow a_0$	$a_0 \in A$
$\boxed{s_1}$	$(s_0, a_0, s_1) \in r_1$	$\boxed{t_1}$	$(t_0, a_0, t_1) \in r_2$
$\downarrow a_1$	$a_1 \in A$	$\downarrow a_1$	$a_1 \in A$
$\boxed{s_2}$	$(s_1, a_1, s_2) \in r_1$	$\boxed{t_2}$	$(t_1, a_1, t_2) \in r_2$
$\dots$		$\dots$	

When do two systems behave the same?

Two Systems with Common Alphabet

$M_1 = (S_1, I_1, r_1, A)$

$\boxed{s_0}$	$s_0 \in I_1$
$\downarrow a_0$	$a_0 \in A$
$\boxed{s_1}$	$(s_0, a_0, s_1) \in r_1$
$\downarrow a_1$	$a_1 \in A$
$\boxed{s_2}$	$(s_1, a_1, s_2) \in r_1$
$\dots$	

$M_2 = (S_2, I_2, r_2, A)$

$\boxed{t_0}$	$t_0 \in I_2$
$\downarrow a_0$	$a_0 \in A$
$\boxed{t_1}$	$(t_0, a_0, t_1) \in r_2$
$\downarrow a_1$	$a_1 \in A$
$\boxed{t_2}$	$(t_1, a_1, t_2) \in r_2$
$\dots$	

When do two systems behave the same? $=$ same sequences of a_i (regardless of s_i vs t_i)

Rationale: we cannot see what is inside, but we can observe A
Example: if states in S_2 are just renamed versions of those in S_1, that is,
$r_2 = \{(\alpha(s_1), a, \alpha(s_2)) \mid (s_1, a, s_2) \in r_1\}$ for some renaming function α.

M_1 is a refinement of M_2

Given

$$M_1 = (S_1, I_1, r_1, A) \qquad \text{and} \qquad M_2 = (S_2, I_2, r_2, A)$$

M_1 is a *refinement* of M_2, written $M_1 \sqsubseteq M_2$, iff
the external traces of M_1 are included in the external traces of M_2.

$\boxed{s_0}$	$s_0 \in I_1$	$\boxed{t_0}$	$t_0 \in I_2$
$\downarrow a_0$	$a_0 \in A$	$\downarrow a_0$	$a_0 \in A$
$\boxed{s_1}$	$(s_0, a_0, s_1) \in r_1$	$\boxed{t_1}$	$(t_0, a_0, t_1) \in r_2$
$\downarrow a_1$	$a_1 \in A$	$\downarrow a_1$	$a_1 \in A$
$\boxed{s_2}$	$(s_1, a_1, s_2) \in r_1$	$\boxed{t_2}$	$(t_1, a_1, t_2) \in r_2$
$\ldots$		$\ldots$	

An external trace is $a_0, a_1, \ldots$ the sequence of labels a_i in the trace (omitting states).

$$ETraces(M) = \{a_0 a_1 a_2 \ldots \mid \exists s_0 a_0 s_1 a_1 s_2 a_2 \ldots \in Traces(M)\}$$

$M_1 \sqsubseteq M_2$ is defined as $ETraces(M_1) \subseteq ETraces(M_2)$

M_1 is equivalent to M_2

We can say M_1 and M_2 are externally equivalent iff

$$M_1 \sqsubseteq M_2 \ \wedge \ M_2 \sqsubseteq M_1$$

It follows that this condition is the same as $ETraces(M_1) = ETraces(M_2)$.

How to prove $ETraces(M_1) \subseteq ETraces(M_2)$?

Assume we have finite traces only.
Prove that the inclusion holds **by induction**!
Inductive case: let $a_0 \ldots a_{n-1} a_n \in ETraces(M_1)$. Thus, for some states, $s_0, a_0, s_1, \ldots, s_{n-1}, a_{n-1}, s_n, a_n, s_{n+1} \in Traces(M_1)$.
$a_0 \ldots a_{n-1} \in ETraces(M_1)$ so, by I.H., there exists a trace $t_0, a_0, t_1, \ldots, t_{n-1}, a_{n-1}, t_n \in Traces(M_2)$.
We wish to extend the trace and show $a_0 \ldots a_{n-1} a_n \in ETraces(M_2)$ that is, that there exists a trace $t_0, a_0, t_1, \ldots, t_{n-1}, a_{n-1}, t_n, a_n, t_{n+1} \in Traces(M_2)$.
So, we just need to know that there exists t_{n+1} such that $(t_n, a_n, t_{n+1}) \in r_2$.

Forward Simulation Relation

Existence of a *forward simulation relation* is a sufficient condition for such proof.

Definition. Given $M_1 = (S_1, I_1, r_1, A)$ and $M_2 = (S_2, I_2, r_2, A)$, we say $\alpha \subseteq S_1 \times S_2$ is a *forward simulation relation* from M_1 to M_2 iff both of these conditions hold:

1. initial states map to initial state: $\forall s \in I_1 . \exists t \in I_2 .\ (s, t) \in \alpha$
2. $\forall s, s' \in S_1 . \forall t \in S_2 .\ \forall a \in A.$

$$(s, a, s') \in r_1 \land (s, t) \in \alpha \quad \longrightarrow \quad \exists t' \in S_2 .\ ((t, a, t') \in r_2 \land (s', t') \in \alpha)$$

$$\begin{array}{c} \boxed{s_0} \\ \downarrow a_0 \\ \boxed{s_1} \\ \downarrow a_1 \\ \boxed{s_2} \\ \ldots \end{array} \qquad\qquad \begin{array}{c} \boxed{t_0} \\ \downarrow a_0 \\ \boxed{t_1} \\ \downarrow a_1 \\ \boxed{t_2} \\ \ldots \end{array}$$

Theorem: if there exists a simulation relation between M_1 and M_2, then $M_1 \sqsubseteq M_2$.

Proof sketch: $\forall$ trace of M_1, $\exists$ trace of M_2 with same labels such that $\forall i.\ (s_i, t_i) \in \alpha$.

Case when Forward Simulation Relation is a Function

General case:

1. $\forall s \in I_1 . \exists t \in I_2 .\ (s,t) \in \alpha$
2. $\forall s, s' \in S_1 . \forall t \in S_2 .\ \forall a \in A.$
   $$(s,a,s') \in r_1 \wedge (s,t) \in \alpha \quad \rightarrow \quad \exists t' \in S_2 .\ ((t,a,t') \in r_2 \wedge (s',t') \in \alpha)$$

Special case when $(s,t) \in \alpha$ is just $t = \alpha(s)$:

1. $\forall s \in I_1 .\ \alpha(s) \in I_2$
2. $\forall s, s' \in S_1 . \forall a \in A. \quad (s,a,s') \in r_1 \quad \rightarrow \quad (\alpha(t), a, \alpha(t')) \in r_2$

Slightly less special case: α is function on reachable states, else undefined:

1. $\forall s \in I_1 .\ \alpha(s) \in I_2$
2. $\forall s, s' \in Reach(M_1) . \forall a \in A. \quad (s,a,s') \in r_1 \quad \rightarrow \quad (\alpha(t), a, \alpha(t')) \in r_2$