Modeling Concurrent Systems

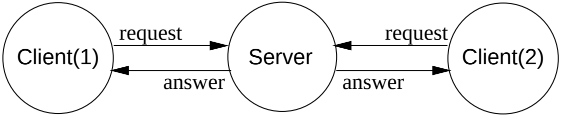
Wolfgang Schreiner
Wolfgang.Schreiner@risc.uni-linz.ac.at

Research Institute for Symbolic Computation (RISC)
Johannes Kepler University, Linz, Austria
http://www.risc.uni-linz.ac.at

1. **A Client/Server System**

2. **Modeling Concurrent Systems**

A Client/Server System



- System of one server and two clients.
  - Three concurrently executing system components.
- Server manages a resource.
  - An object that only one system component may use at any time.
- Clients request resource and, having received an answer, use it.
  - Server ensures that not both clients use resource simultaneously.
  - Server eventually answers every request.

Set of system requirements.

System Implementation

```
Server:
  local given, waiting, sender
begin
  given := 0; waiting := 0
  loop
    sender := receiveRequest()
    if sender = given then
      if waiting = 0 then
        given := 0
      else
        given := waiting; waiting := 0
        sendAnswer(given)
      endif
    elsif given = 0 then
      given := sender
      sendAnswer(given)
    else
      waiting := sender
    endif
  endloop
end Server
```

```
Client(ident):
  param ident
begin
  loop
    ...
    sendRequest()
    receiveAnswer()
    ... // critical region
    sendRequest()
  endloop
end Client
```

Desired System Properties

- Property: mutual exclusion.
  - At no time, both clients are in critical region.
    - Critical region: program region after receiving resource from server and before returning resource to server.
  - The system shall only reach states, in which mutual exclusion holds.
- Property: no starvation.
  - Always when a client requests the resource, it eventually receives it.
  - Always when the system reaches a state, in which a client has requested a resource, it shall later reach a state, in which the client receives the resource.
- Problem: each system component executes its own program.
  - Multiple program states exist at each moment in time.
  - Total system state is combination of individual program states.
  - Not easy to see which system states are possible.

How can we verify that the system has the desired properties?

1. A Client/Server System

2. Modeling Concurrent Systems

System States

At each moment in time, a system is in a particular state.

- A state $s : Var \rightarrow Val$
  - A state s is a mapping of every system variable x to its value $s(x)$.
    - Typical notation: $s = [x = 0, y = 1, \ldots] = [0, 1, \ldots]$.
  - Var ... the set of system variables
    - Program variables, program counters, ...
  - Val ... the set of variable values.
- The state space $State = \{s \mid s : Var \rightarrow Val\}$
  - The state space is the set of possible states.
    - The system variables can be viewed as the coordinates of this space.
  - The state space may (or may not) be finite.
    - If $|Var| = n$ and $|Val| = m$, then $|State| = m^n$.
    - A word of $\log_2 m^n$ bits can represent every state.

A system execution can be described by a path $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$ in the state space.

Deterministic Systems

In a sequential system, each state typically determines its successor state.

- The system is deterministic.
  - We have a (possibly not total) transition function F on states.
  - $s_1 = F(s_0)$ means "s_1 is the successor of s_0".
- Given an initial state s_0, the execution is thus determined.
  - $s_0 \rightarrow s_1 = F(s_0) \rightarrow s_2 = F(s_1) \rightarrow \ldots$
- A deterministic system (model) is a pair $\langle I, F \rangle$.
  - A set of initial states $I \subseteq State$
    - Initial state condition $I(s) :\Leftrightarrow s \in I$
  - A transition function $F : State \stackrel{partial}{\rightarrow} State$.
- A run of a deterministic system $\langle I, F \rangle$ is a (finite or infinite) sequence $s_0 \rightarrow s_1 \rightarrow \ldots$ of states such that
  - $s_0 \in I$ (respectively $I(s_0)$).
  - $s_{i+1} = F(s_i)$ (for all sequence indices i)
  - If s ends in a state s_n, then F is not defined on s_n.

Nondeterministic Systems

In a concurrent system, each component may change its local state, thus the successor state is not uniquely determined.

- The system is nondeterministic.
  - We have a transition relation R on states.
  - $R(s_0, s_1)$ means "s_1 is a (possible) successor of s_0.
- Given an initial state s_0, the execution is not uniquely determined.
  - Both $s_0 \rightarrow s_1 \rightarrow \ldots$ and $s_0 \rightarrow s_1' \rightarrow \ldots$ are possible.
- A non-deterministic system (model) is a pair $\langle I, R \rangle$.
  - A set of initial states (initial state condition) $I \subseteq State$.
  - A transition relation $R \subseteq State \times State$.
- A run s of a nondeterministic system $\langle I, R \rangle$ is a (finite or infinite) sequence $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ of states such that
  - $s_0 \in I$ (respectively $I(s_0)$).
  - $R(s_i, s_{i+1})$ (for all sequence indices i).
  - If s ends in a state s_n, then there is no state t such that $R(s_n, t)$.

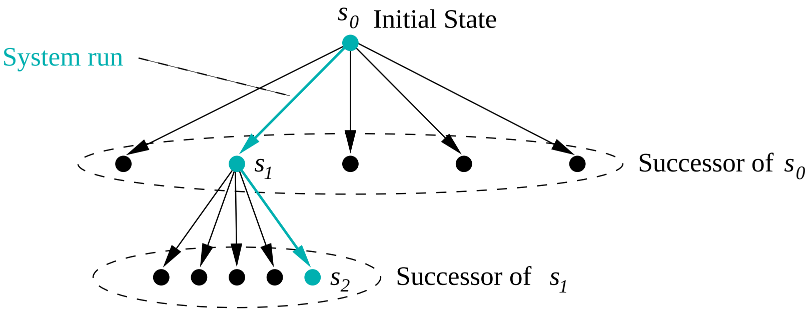
Derived Notions

- Successor and predecessor:
  - State t is a (direct) successor of state s, if $R(s, t)$.
  - State s is then a predecessor of t.
    - A finite run $s_0 \rightarrow \ldots \rightarrow s_n$ ends in a state which has no successor.
- Reachability:
  - A state t is reachable, if there exists some run $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$ such that $t = s_i$ (for some i).
  - A state t is unreachable, if it is not reachable.

Not all states are reachable (typically most are unreachable).

Reachability Graph

The transitions of a system can be visualized by a graph.



The nodes of the graph are the reachable states of the system.

Examples

6 1. Automata

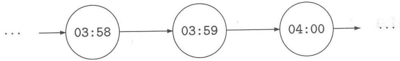


Fig. 1.1. A model of a watch

of $\mathcal{A}_{c3}$ correspond to the possible counter values. Its transitions reflect the possible actions on the counter. In this example we restrict our operations to increments (`inc`) and decrements (`dec`).

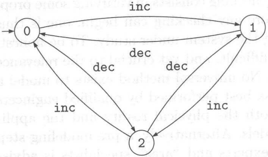


Fig. 1.2. $\mathcal{A}_{c3}$: a modulo 3 counter

B.Berard et al: "Systems and Software Verification", 2001.

Examples

- A deterministic system $W = (I_W, F_W)$ ("watch").
  - $State := \{\langle h, m\rangle : h \in \mathbb{N}_{24} \wedge m \in \mathbb{N}_{60}\}$.
    - $\mathbb{N}_n := \{i \in \mathbb{N} : i < n\}$.
  - $I_W(h, m) :\Leftrightarrow h = 0 \wedge m = 0$.
    - $I_W := \{\langle h, m\rangle : h = 0 \wedge m = 0\} = \{\langle 0, 0\rangle\}$.
  - $F_W(h, m) :=$
    if $m < 59$ **then** $\langle h, m + 1\rangle$
    else if $h < 24$ **then** $\langle h + 1, 0\rangle$
    else $\langle 0, 0\rangle$.
- A nondeterministic system $C = (I_C, R_C)$ (modulo 3 "counter").
  - $State := \mathbb{N}_3$.
  - $I_C(i) :\Leftrightarrow i = 0$.
  - $R_C(i, i') :\Leftrightarrow inc(i, i') \vee dec(i, i')$.
    - $inc(i, i') :\Leftrightarrow$ **if** $i < 2$ **then** $i' = i + 1$ **else** $i' = 0$.
    - $dec(i, i') :\Leftrightarrow$ **if** $i > 0$ **then** $i' = i - 1$ **else** $i' = 2$.

Composing Systems

Compose n components S_i to a concurrent system S.

- State space $State := State_0 \times \ldots \times State_{n-1}$.
  - $State_i$ is the state space of component i.
  - State space is Cartesian product of component state spaces.
  - Size of state space is product of the sizes of the component spaces.
- Example: three counters with state spaces $\mathbb{N}_2$ and $\mathbb{N}_3$ and $\mathbb{N}_4$.

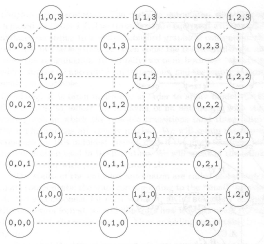


Fig. 1.9. The states of the product of the three counters

B.Berard et al: "Systems and Software Verification", 2001.

Initial States of Composed System

What are the initial states I of the composed system?

- Set $I := I_0 \times \ldots \times I_{n-1}$.
  - I_i is the set of initial states of component i.
  - Set of initial states is Cartesian product of the sets of initial states of the individual components.
- Predicate $I(s_0, \ldots, s_{n-1}) :\Leftrightarrow I_0(s_0) \wedge \ldots \wedge I_{n-1}(s_{n-1})$.
  - I_i is the initial state condition of component i.
  - Initial state condition is conjunction of the initial state conditions of the components on the corresponding projection of the state.

Size of initial state set is the product of the sizes of the initial state sets of the individual components.

Transitions of Composed System

Which transitions can the composed system perform?

- Synchronized composition.
  - At each step, every component must perform a transition.
    - R_i is the transition relation of component i.

      $$R(\langle s_0, \ldots, s_{n-1}\rangle, \langle s'_0, \ldots, s'_{n-1}\rangle) :\Leftrightarrow \\ R_0(s_0, s'_0) \wedge \ldots \wedge R_{n-1}(s_{n-1}, s'_{n-1}).$$
- Asynchronous composition.
  - At each moment, every component may perform a transition.
    - At least one component performs a transition.
    - Multiple simultaneous transitions are possible
    - With n components, $2^n - 1$ possibilities of (combined) transitions.

      $$R(\langle s_0, \ldots, s_{n-1}\rangle, \langle s'_0, \ldots, s'_{n-1}\rangle) :\Leftrightarrow \\ (R_0(s_0, s'_0) \wedge \ldots \wedge s_{n-1} = s'_{n-1}) \vee \\ \ldots \\ (s_0 = s'_0 \wedge \ldots \wedge R_{n-1}(s_{n-1}, s'_{n-1})) \vee \\ \ldots \\ (R_0(s_0, s'_0) \wedge \ldots \wedge R_{n-1}(s_{n-1}, s'_{n-1})).$$

Example

System of three counters with state space $\mathbb{N}_2$ each.

- Synchronous composition:

$$[0,0,0] \leftrightarrows [1,1,1]$$

- Asynchronous composition:

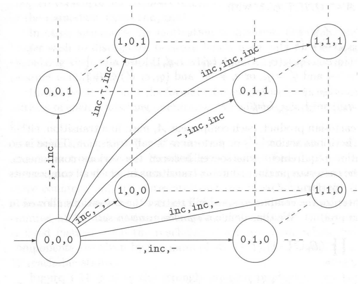


Fig. 1.10. A few transitions of the product of the three counters

B.Berard et al: "Systems and Software Verification", 2001.

Interleaving Execution

Simplified view of asynchronous execution.

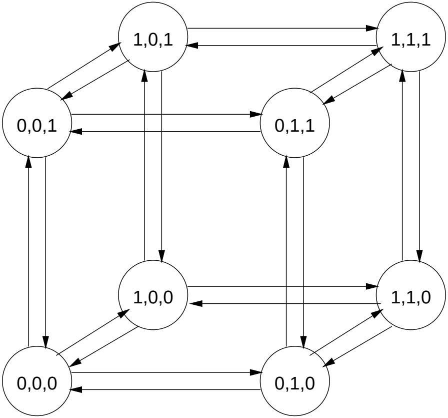
- At each moment, only one component performs a transition.
  - Do not allow simultaneous transition $t_i | t_j$ of two components i and j.
  - Transition sequences $t_i; t_j$ and $t_j; t_i$ are possible.
    - All possible interleavings of component transitions are considered.
    - Nondeterminism is used to simulate concurrency.
    - Essentially no change of system properties.
  - With n components, only n possibilities of a transition.

$$
\begin{aligned}
&R(\langle s_0, s_1, \ldots, s_{n-1}\rangle, \langle s'_0, s'_1, \ldots, s'_{n-1}\rangle) :\Leftrightarrow \\
&\quad (R_0(s_0, s'_0) \wedge s_1 = s'_1 \wedge \ldots \wedge s_{n-1} = s'_{n-1}) \vee \\
&\quad (s_0 = s'_0 \wedge R_1(s_1, s'_1) \wedge \ldots \wedge s_{n-1} = s'_{n-1}) \vee \\
&\quad \ldots \\
&\quad (s_0 = s'_0 \wedge s_1 = s'_1 \wedge \ldots \wedge R_{n-1}(s_{n-1}, s'_{n-1})).
\end{aligned}
$$

Interleaving model (respectively a variant of it) suffices in practice.

Example

System of three counters with state space $\mathbb{N}_2$ each.



Digital Circuits

Synchronous composition of system components.

- A modulo 8 counter $C = \langle I_C, R_C \rangle$.

  $State := \mathbb{N}_2 \times \mathbb{N}_2 \times \mathbb{N}_2.$

  $I_C(v_0, v_1, v_2) :\Leftrightarrow v_0 = v_1 = v_2 = 0.$

  $R_C(\langle v_0, v_1, v_2 \rangle, \langle v_0', v_1', v_2' \rangle) :\Leftrightarrow$
  $\quad R_0(v_0, v_0') \wedge$
  $\quad R_1(v_0, v_1, v_1') \wedge$
  $\quad R_2(v_0, v_1, v_2, v_2').$

  $R_0(v_0, v_0') :\Leftrightarrow v_0' = \neg v_0.$
  $R_1(v_0, v_1, v_1') :\Leftrightarrow v_1' = v_0 \oplus v_1.$
  $R_2(v_0, v_1, v_2, v_2') :\Leftrightarrow v_2' = (v_0 \wedge v_1) \oplus v_2.$

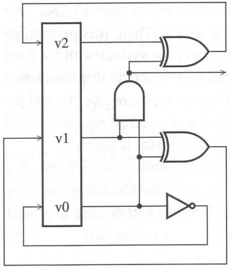


Figure 2.1
Synchronous modulo 8 counter.

Edmund Clarke et al: "Model Checking", 1999.

Concurrent Systems

Asynchronous composition of system components.

$$
\begin{array}{ll}
P :: l_0 : \textbf{while } \text{true } \textbf{do} & \\
\quad NC_0 : \textbf{wait } turn = 0 & \\
\quad CR_0 : turn := 1 & \\
\textbf{end} &
\end{array}
\quad || \quad
\begin{array}{ll}
Q :: l_1 : \textbf{while } \text{true } \textbf{do} & \\
\quad NC_1 : \textbf{wait } turn = 1 & \\
\quad CR_1 : turn := 0 & \\
\textbf{end} &
\end{array}
$$

- A mutual exclusion program $M = \langle I_M, R_M \rangle$.

$State := PC \times PC \times \mathbb{N}_2$. // shared variable

$I_M(p, q, turn) :\Leftrightarrow p = l_0 \wedge q = l_1$.

$R_M(\langle p, q, turn\rangle, \langle p', q', turn'\rangle) :\Leftrightarrow$

$\quad (P(\langle p, turn\rangle, \langle p', turn'\rangle) \wedge q' = q) \vee (Q(\langle q, turn\rangle, \langle q', turn'\rangle) \wedge p' = p)$.

$P(\langle p, turn\rangle, \langle p', turn'\rangle) :\Leftrightarrow$

$\quad (p = l_0 \wedge p' = NC_0 \wedge turn' = turn) \vee$

$\quad (p = NC_0 \wedge p' = CR_0 \wedge turn = 0 \wedge turn' = turn) \vee$

$\quad (p = CR_0 \wedge p' = l_0 \wedge turn' = 1)$.

$Q(\langle q, turn\rangle, \langle q', turn'\rangle) :\Leftrightarrow$

$\quad (q = l_1 \wedge q' = NC_1 \wedge turn' = turn) \vee$

$\quad (q = NC_1 \wedge q' = CR_1 \wedge turn = 1 \wedge turn' = turn) \vee$

$\quad (q = CR_1 \wedge q' = l_1 \wedge turn' = 0)$.

Concurrent Systems

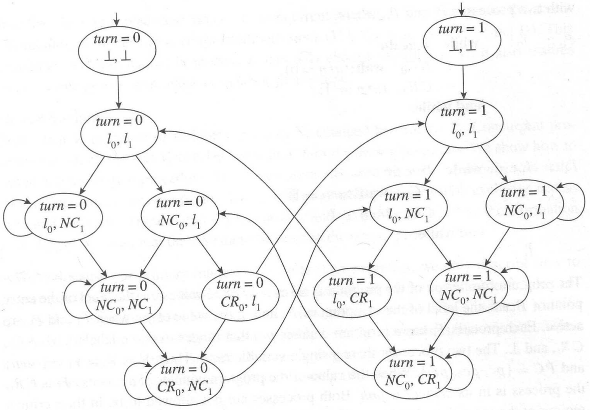


Figure 2.2
Reachable states of Kripke structure for mutual exclusion example.

Edmund Clarke et al: "Model Checking", 1999.

Model guarantees mutual exclusion.

Summary

We have now seen how to model a concurrent system.

- A system is described by
  - its (finite or infinite) state space,
  - the initial state condition (set of input states),
  - the transition relation on states.
- State space of composed system is product of component spaces.
  - Variable shared among components occurs only once in product.
- System composition can be
  - synchronous: conjunction of individual transition relations.
    - Suitable for digital hardware.
  - asynchronous: disjunction of relations.
    - Interleaving model: each relation conjoins the transition relation of one component with the identity relations of all other components.
    - Suitable for concurrent systems.