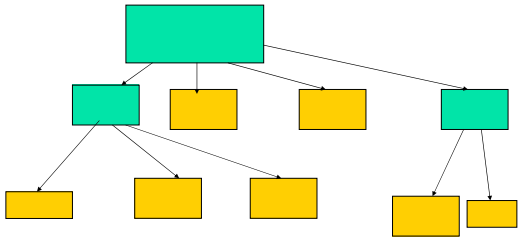
Modeling of Real-Time Systems

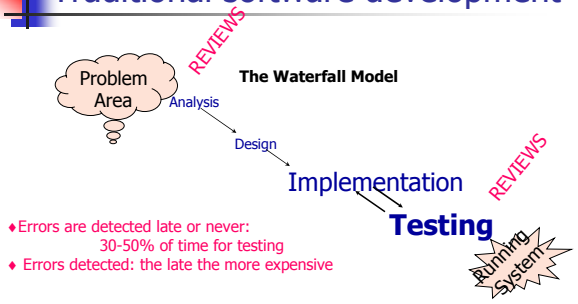
In practice

- a system may contain a large number of ”components” or subsystems
- each component/subsystem may contain a number of sub-components etc

Hierarchical system architecture

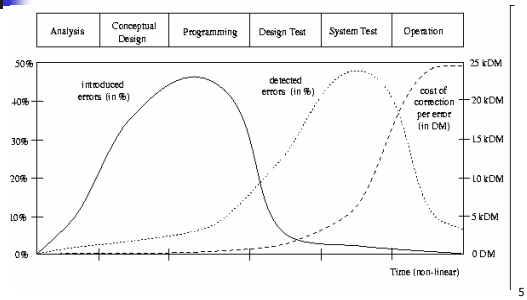


Traditional software development



- Errors are detected late or never: 30-50% of time for testing
- Errors detected: the late the more expensive

Introducing, Detecting and Correcting errors



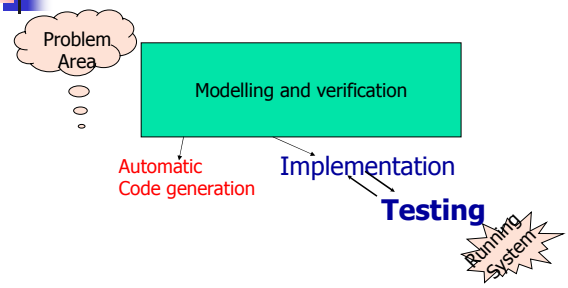
Finding errors as early as possible!

HOW?

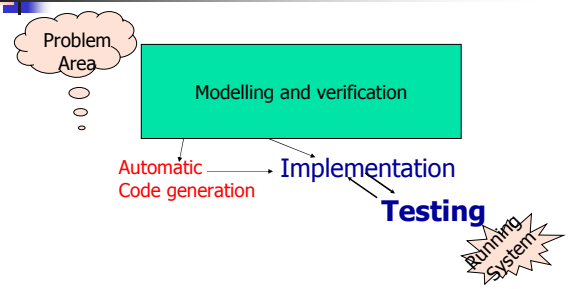
Modeling and Verification

- It is to provide a general and rigorous design method for system development
- ”modeling” is a design process: describe the abstract behaviour of a system
- ”verification” is to complement scheduling analysis to check system properties including safety and liveness-properties

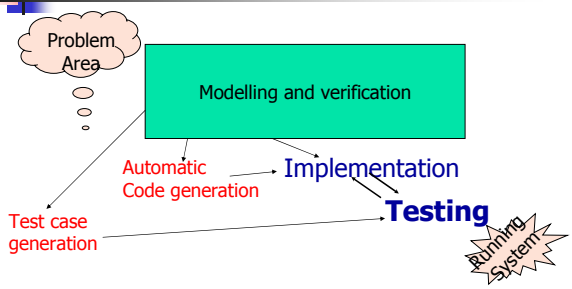
Software development: the future



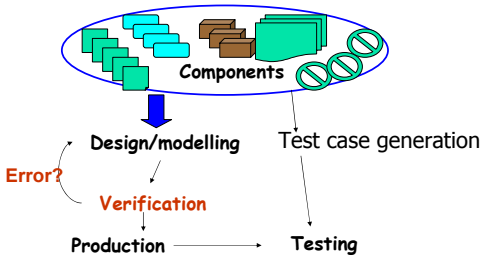
Software development: the future



Software development



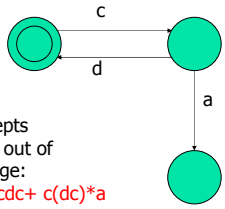
Software Development: the Future



Basic ideas

- Modeling
  - Use state-machines, also called automata, to describe system components
  - A system will be a network of automata
- Verification
  - Check properties of the automata using software tools like UPPAAL or TIMES

Finite State Automata



It has 3 states and 3 transitions

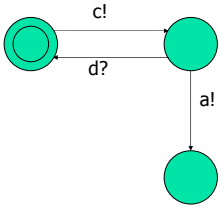
And it accepts sequences out of the language:
c + cd + cdc+ c(dc)*a

Automata as reactive objects

- We view an automaton as a reactive object where the action labels stand for synchronization actions e.g. Ada's rendezvous
- For example, the previous example could be a network protocol where c and d stand for "connect !" and "disconnect?" and a for "abort!"

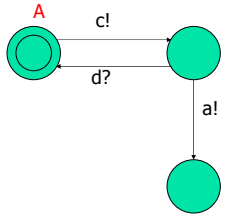
Input and Output Actions

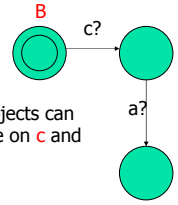
We use ? and ! to denote the pairs of complementary actions in rendezvous communication



Networks of automata

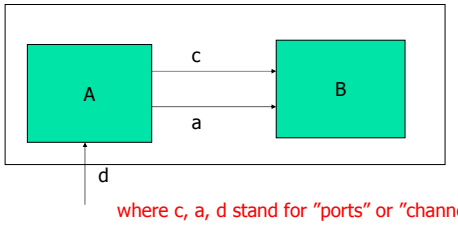
We use ? and ! to denote the pairs of complementary actions in rendezvous communication





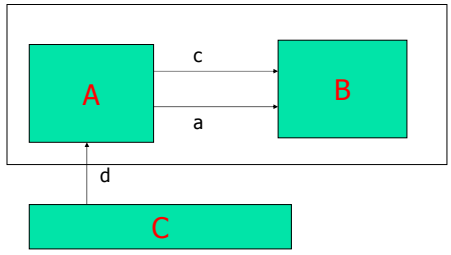
The two objects can synchronize on c and then a

The static architecture of a concurrent system: A || B



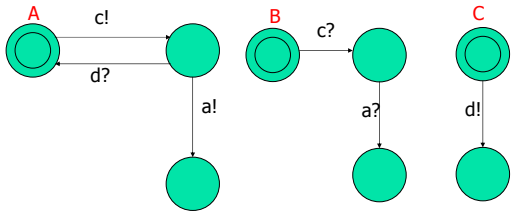
where c, a, d stand for "ports" or "channels"

The static architecture of a concurrent system: A || B || C



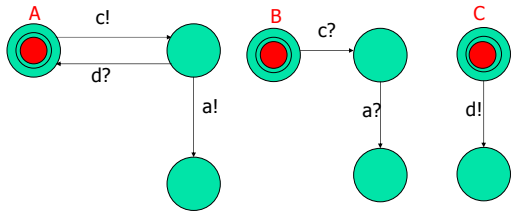
Networks of automata

We use ? and ! to denote the pairs of complementary actions in rendezvous communication



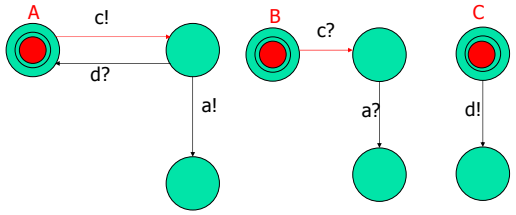
Networks of automata: initial state

We use ? and ! to denote the pairs of complementary actions in rendezvous communication



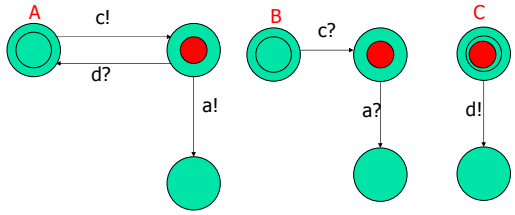
Networks of automata: enabled transition

We use ? and ! to denote the pairs of complementary actions in rendezvous communication



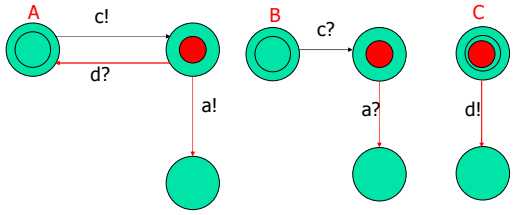
Networks of automata: transition taken

We use ? and ! to denote the pairs of complementary actions in rendezvous communication



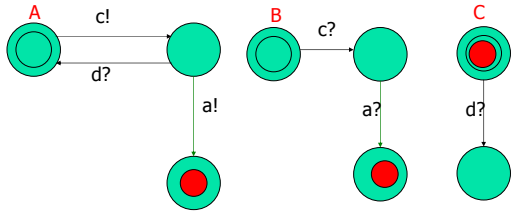
Networks of automata: nondeterministic choices (transitions)

We use ? and ! to denote the pairs of complementary actions in rendezvous communication



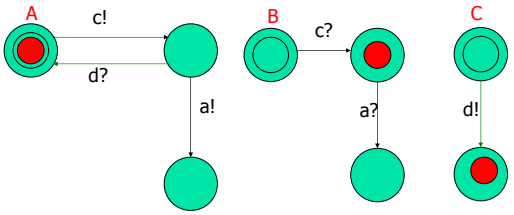
Networks of automata: non-deterministic transitions (1)

We use ? and ! to denote the pairs of complementary actions in rendezvous communication



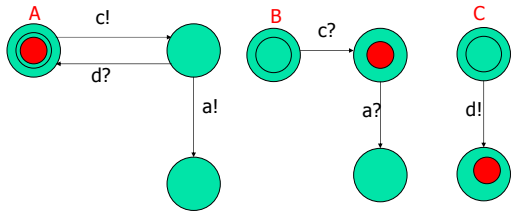
Networks of automata: non-deterministic transition (2)

We use ? and ! to denote the pairs of complementary actions in rendezvous communication



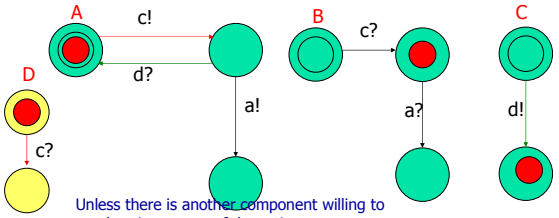
Networks of automata: deadlock!

We use ? and ! to denote the pairs of complementary actions in rendezvous communication



Networks of automata: deadlock!

We use ? and ! to denote the pairs of complementary actions in rendezvous communication

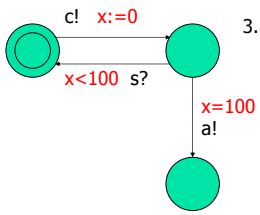


Unless there is another component willing to synchronize on any of the actions

Clocks and timing constraints

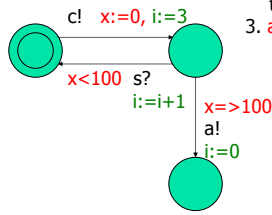
- Now we assume that the system has a finite number of (logical) clocks
  - The clocks start to run from 0 when the system starts, and they run at the same rate (they are perfect clocks with no drift!)
  - The clocks can be read and tested e.g. x<100
  - The clocks can be reset to 0 on a transition

Timed automata: timing constraints



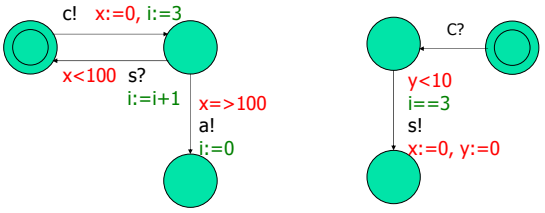
1. connect and reset x to 0
2. If succeed within 100ms, then go to initial
3. about after 100 ms !

Timed automata: integers

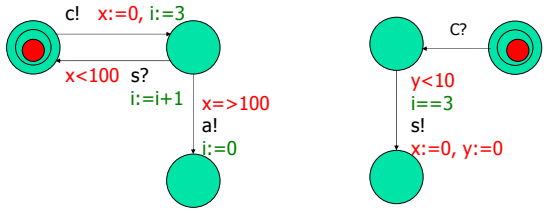


1. connect and reset x to 0
2. If succeed within 100ms, then go to initial
3. about after 100 ms !

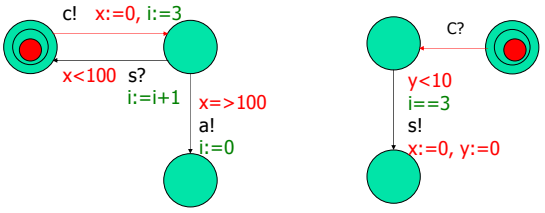
Network of Timed automata



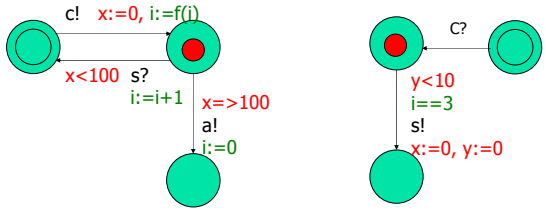
Network of Timed automata: initial states



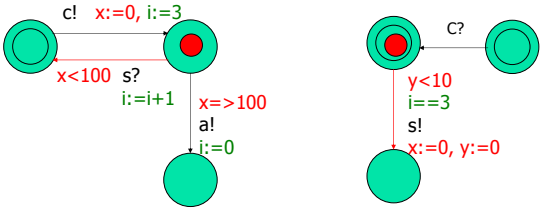
Network of Timed automata: enabled ransition



Network of Timed automata: transition taken

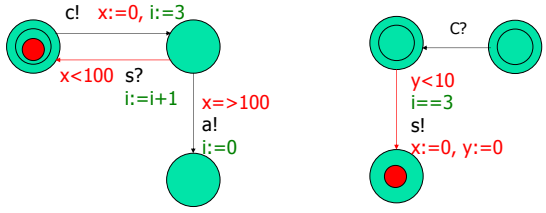


Network of Timed automata: enabled ransition



This depends on the values of x, y, and i

Network of Timed automata: transition taken



This depends on the values of x, y, and i

Timed automata (definition)

- a timed automaton is a finite graph
  - a finite many nodes N
  - a finite many edges between nodes E
  - an edge may be labelled with three elements
    - guard
    - action (a?, a!, or nothing)
    - assignment

  (they may not appear)

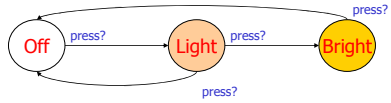
Guard

- a clock constraint
  - g ::= $x \leq n$ | $x \geq n$ | $x<n$ | $x>n$ | $g \wedge g$
  - where n is any natuaral number
- a predicate over data variables
  - "any logical expression" you may write in C

assignment

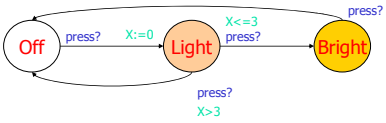
- a clock reset: x:=0 for any clock x
- a sequence of assignments in the form i:=e

Intelligent Light Control



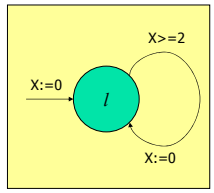
WANT: if press is issued twice quickly
then the light will get brighter; otherwise the light is turned off.

Intelligent Light Control (with timer)

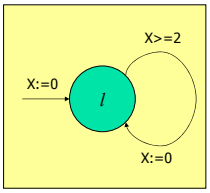


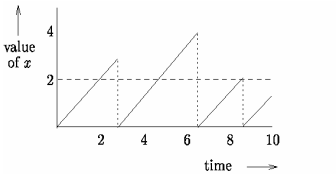
Solution: Add real-valued clock x

Timed Automata: Example

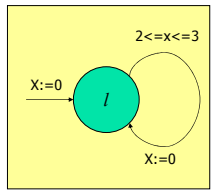


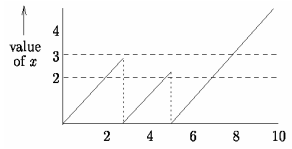
Timed Automata: Example



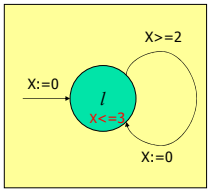


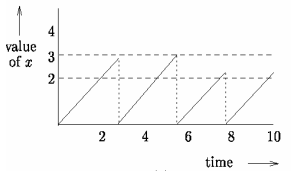
Timed Automata: Example





Timed Automata: Example

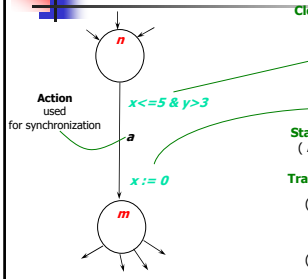




Timed Automata: Semantics

- States: (n, u) where
  - n stands for the current node or location
  - u stands for the current values of clocks and integers (i.e. the memory of a machine)
- Transitions: delay and actions
  - (n,u) moves to (n, u+d) after d time units
  - (n,u) moves to (m, v) when an action over channel "a" is taken, and v is the new values of clocks and integer variables

Timed Automata: Semantics



Clocks: *x, y*

Guard =clock constraint

Reset
Action perfomed on clocks

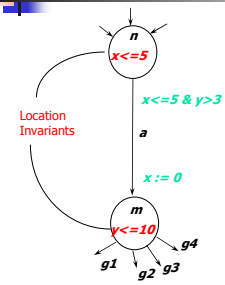
State
(***location*** , ***x***=v , ***y***=u) where v,u are in **R**

Transitions

(***n*** , ***x***=2.4 , ***y***=3.1415) —***a***→ (***m*** , ***x***=0 , ***y***=3.1415)

(***n*** , ***x***=2.4 , ***y***=3.1415) —*e(1.1)*→ (***n*** , ***x***=3.5 , ***y***=4.2415)

Timed Automata with *Invariants*



Clocks: *x, y*

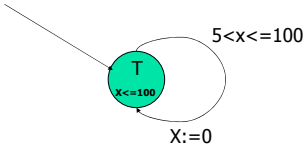
Transitions

(***n*** , ***x***=2.4 , ***y***=3.1415) —3.2→

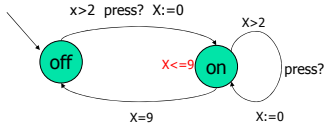
(***n*** , ***x***=2.4 , ***y***=3.1415) —1.1→ (***n*** , ***x***=3.5 , ***y***=4.2415)

Invariants insure progress!!

Timed Automata: Example (task with jitter)

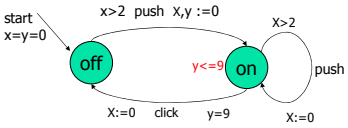


Timed Automata: Light Switch



- Switch may be turned on whenever at least 2 time units has elapsed since last "turn off"
- Light automatically switches off after 9 time units if it is not pressed.

Timed Automata: Example

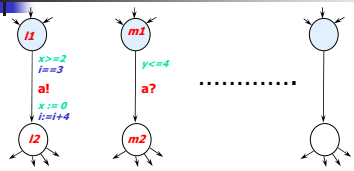


$$(off, x = y = 0) \xrightarrow{3.5} (off, x = y = 3.5) \xrightarrow{push}$$
$$(on, x = y = 0) \xrightarrow{\pi} (on, x = y = \pi) \xrightarrow{push}$$
$$(on, x = 0, y = \pi) \xrightarrow{3} (on, x = 3, y = \pi + 3) \xrightarrow{9-(\pi+3)}$$
$$(on, x = 9 - (\pi + 3), y = 9) \xrightarrow{click} (off, x = 0, y = 9) \ldots$$

Modeling Concurrency

- Products of automata
- Parallel composition

Networks of Timed Automata + Integer Variables + ...



Two-way synchronization on *complementary* actions.

Closed Systems!

Example transitions

(*l1, m1,*....., x=2, y=3.5, i=3,.....) ⟶ (*l2,m2,*.....,x=0, y=3.5, i=7,.....)

Modeling Ada Programs

Rendezvous

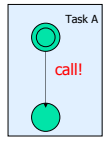
```
task body A is
begin
...
B.Call;
...
end A
```

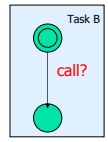
```
task body B is
begin
...
accept Call do
....
end Call
...
end A
```


Rendezvous

```
task body A is
begin
...
B.Call;
...
end A
```

```
task body B is
begin
...
accept Call do
....
end Call
...
end A
```





Buffer

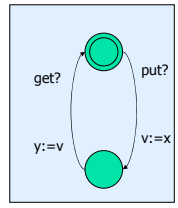
```
task buffer is
entry put(X: in integer)
entry get(x: out integer)
end;

task body buffer is
 v: integer;
 begin
 loop accept put(x: in integer) do v:= x end put;
       accpet get(x: out integer) do x:= v end get;
 end loop;
 end buffer;
---
buffer.put(...)      <---------- other tasks (users)!!
buffer get(...)
----
```


Buffer

```
task buffer is
entry put(X: in integer)
entry get(x: out integer)
end;

task body buffer is
 v: integer;
 begin
 loop accept put(x: in integer) do v:= x end put;
       accpet get(y: out integer) do y:= v end get;
 end loop;
 end buffer;
---
buffer.put(...)      <---------- other tasks (users)!!
buffer get(...)
----
```

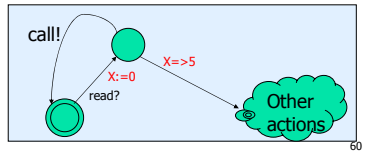


Conditional/Timed entry call

```
loop
   --get temperature
   select
        Controller.Call(T);      -- put new temperature
   or  delay 5                   --other actions
   end select;
end loop;
```


Conditional/Timed entry call

```
loop
   --get temperature
   select
        Controller.call(T);      -- put new temperature
   or  delay 5                   --other actions
   end select;
end loop;
```

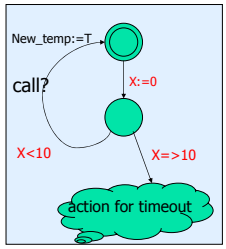


Timeout and message passing

```
loop
   select
        accept Call(T : temperature) do
                New_temp:=T;
        end Call;
   or
        delay 10.0;
                --action for timeout
   end select;
   --other actions
end loop;
```


Timeout and message passing

```
loop
   select
        accept Call(T : temperature) do
                New_temp:=T;
        end Call;
   or
        delay 10.0;
                --action for timeout
   end select;
   --other actions
end loop;
```

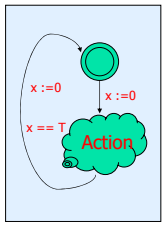


Periodic Activity

```
task body T is
  Interval : constant Duration := 5.0;
  Next_Time : Time;
begin
  Next_Time := Clock + Interval;
  loop
    Action;
    delay until Next_Time;
    Next_Time := Next_Time + Interval;
  end loop;
end T;
```

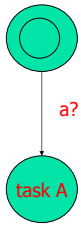

Periodic Activity

```
task body TaskP is
  T : constant Duration := 5.0;
  Next_Time : Time;
begin
  Next_Time := Clock + T;
  loop
    Action;
    delay until Next_Time;
    Next_Time := Next_Time + T;
  end loop;
end TaskP;
```



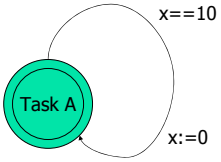
In TIMES, periodic tasks can be easily modeled using "Automata with tasks"

Automata with Tasks



Whenever a occurs, task A is set to ready!

Periodic tasks



Every 10 time units,
A is released one instance