

COMP424/524-06A Topics in Software Engineering

Part I – Model Checking Algorithms

14. Implementation Issues

Robi Malik

THE UNIVERSITY OF
WAIKATO DEPARTMENT OF COMPUTER SCIENCE
TARI ROROHIKO

Expanding a State

For each unvisited state we have to ...

- check controllability condition;
- compute successor states.

Assumptions:

- source state tuple in array $q[1], \dots, q[N]$
- target state to be put in $q'[1], \dots, q'[N]$

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-14 Slide 4

Controllability Check Algorithm

To check whether plants A_1, \dots, A_P are controllable with respect to specifications A_{P+1}, \dots, A_N :

Add initial state $q_0 = (q_{0,1}, \dots, q_{0,N})$ to state set Q

While there are unvisited states $q \in Q$ **do**

For each event e enabled by all plants in state q **do**

If e is uncontrollable and there exists a specification that cannot execute e in state q **then**
 return "The system is not controllable."

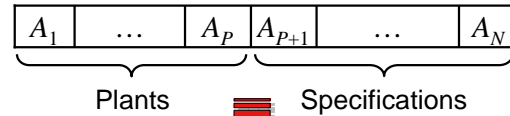
If e can be executed by all specifications **then**

 Compute successor state r such that $q \xrightarrow{e} r$
 Add r to state set Q if not yet present

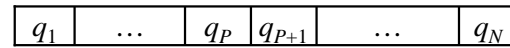
© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-14 Slide 2

Listing Automata

Automata:



State Tuples:



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-14 Slide 5

Data Structure for State Set Q

Requirements:

- new items to be added
- need to find whether items are contained
- need to get next unvisited state
- **can get very large!**

Available in Java:

- `java.util.LinkedList`
- `java.util.ArrayList`
- `java.util.HashMap`

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-14 Slide 3

Expanding a State continued

```

foreach event e
  for i := 1 ... N do
    if e is not in the Alphabet of  $A_i$  then
       $q'[i] := q[i]$ 
    else if  $q[i] \xrightarrow{e} q'$  in  $A_i$  then
       $q'[i] := q'$ 
    else if e is uncontrollable and  $i > P$  then
      return "The system is not controllable."
    else
      next event e
    end if
  end for
  store successor state tuple ( $q'[1], \dots, q'[N]$ )
end for

```

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-14 Slide 6