


COMP424/524-06A

Topics in Software Engineering

Part I – Model Checking Algorithms

13. State Exploration

Robi Malik



DEPARTMENT OF COMPUTER SCIENCE
TARI ROROHIKO

Synchronous Product Algorithm

To build the synchronous product of A_1, \dots, A_n :

Create initial state $q_0 = (q_{01}, \dots, q_{0n})$
 Add q_0 to state set Q

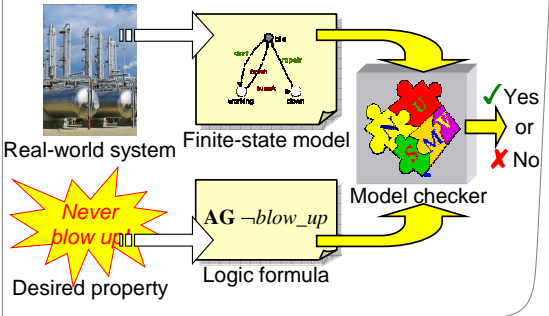
While there are unvisited states $q = (q_1, \dots, q_n) \in Q$:

For each event e that can be executed by each automaton A_i in state q_i :

Compute successor state $r = (r_1, \dots, r_n)$
 Add r to state set Q if not yet present
 Create transition from q to r labelled e

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-13 Slide 4

Model Checkers



Real-world system → Finite-state model

Desired property (Never blow up) → Logic formula (AG -blow_up) → Model checker

Model checker outputs: Yes or No

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-13 Slide 2

Controllability Check Algorithm

To check whether plants P_1, \dots, P_n are controllable with respect to specifications S_1, \dots, S_m :

Add initial state $q_0 = (q_{01}^P, \dots, q_{0n}^P, q_{01}^S, \dots, q_{0m}^S)$ to state set Q

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

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

If e is uncontrollable and there exists a specification S_j 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-13 Slide 5

Controllability

Plant

Spec

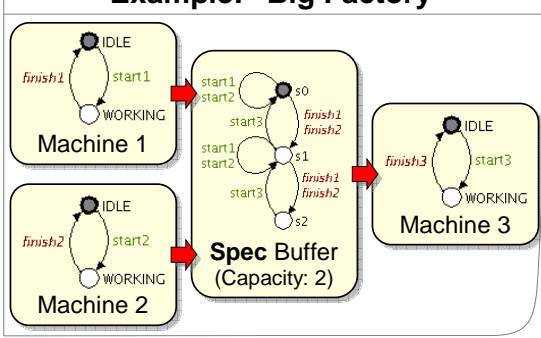
Definition

Let P and S be two automata.

S is called **controllable** with respect to P if, for every state (q_P, q_S) reachable in $P \parallel S$, every uncontrollable event e which is enabled in q_P also is enabled in q_S .

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-13 Slide 3

Example: "Big Factory"



Machine 1: IDLE, WORKING, finish1, start1

Machine 2: IDLE, WORKING, finish2, start2

Machine 3: IDLE, WORKING, finish3, start3

Spec Buffer (Capacity: 2): s0, s1, s2, start1, start2, start3, finish1, finish2

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-13 Slide 6