

COMP424/524-06A Topics in Software Engineering

Part I – *Finite State Machines*

1. Reactive Systems

Robi Malik

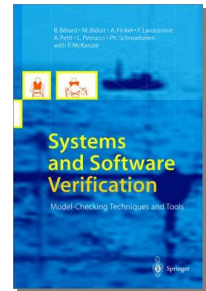


DEPARTMENT OF COMPUTER SCIENCE
TARI ROROHIKO

COMP424/524-06A: Part I

Recommended Textbook:

B. Bérard, M. Bidoit,
A. Finkel, F. Laroussinie,
A. Petit, L. Petrucci,
Ph. Schnoebelen: *Systems
and Software Verification.*
Springer, 1998.



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 4

COMP424/524-06A

I. Finite-State Machines and Model Checking

Robi Malik

Office: G 2.03

Phone: 07 838 4796

e-Mail: robi@cs.waikato.ac.nz

II. Refinement in Z

Steve Reeves

Office: G 1.23

Phone: 07 838 4398

e-Mail: stever@cs.waikato.ac.nz

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 2

COMP424/524-06A: Part I

Some more books on model checking:

- Christos G. Cassandras, Stéphane Lafortune: *Introduction to Discrete Event Systems.* Kluwer Academic Publishers, 1999.
- Kenneth L. McMillan: *Symbolic Model Checking.* Kluwer Academic Publishers, 1993.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 5

Assessment

- 6 Assignments
 - Assignment 1 due **Monday 13 March** 9:00 A.M.
 - Assignment 2 due **Monday 27 March** 9:00 A.M.
 - Assignment 3 due **Monday 10 April** 9:00 A.M.
 - Assignment 4 due **Monday 8 May** 9:00 A.M.
 - Assignment 5 due **Monday 22 May** 9:00 A.M.
 - Assignment 6 due **Monday 5 June** 9:00 A.M.
- Final Exam
- 5th year students: please contact lecturer

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 3

COMP424/524-06A: Part I

Model Checking Software

VALID Toolset

- Type `/home/robi/bin/valid` to run
- More instructions in class



NuSMV

- Type `NuSMV` to run
- Download and documentation at <http://nusmv.irst.itc.it>



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 6

Reactive Systems

Definition:

A “**reactive system**” is a computer program that continuously interacts with its environment.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 7

Graphical User Interfaces

- Input is presented while the system is running.
- User can continuously interact with the system.
- Correctness cannot be specified by correct output.



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 10

Transformational Systems

Definition:

A “**transformational system**” is a computer program that accepts some input, performs computation on it, produces output, and then terminates.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 8

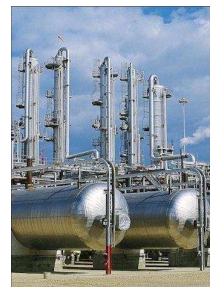
Embedded Systems

Technical devices

- Household equipment
- Automotive electronics
- Industrial plants

All these are ...

- often safety-critical
- reactive systems

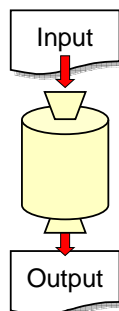


© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 11

Transformational Systems

Examples

- Compute the sum of a list of numbers.
- Read a text file, compute how often each word occurs, and display the results graphically.



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 9

Hardware

Dealing with Bugs ...

In Software

- Fix the bug
- Put a patch on your website

In Hardware

- Can be very expensive!



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 12

What is the Difference?

Transformational System	Reactive System

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 13

Reactive Systems

Reactive Systems are *very hard*

- to *design* ...
- to *implement* and ...
- to *get right*.

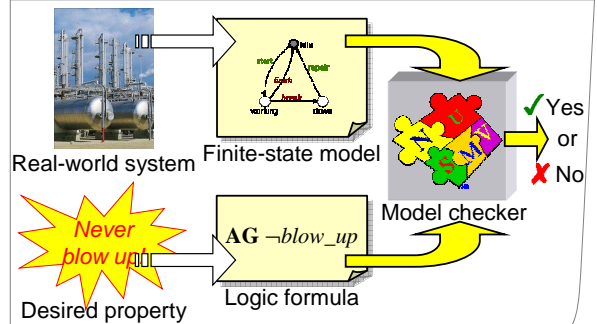
© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 16

Properties of Reactive Systems



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 14

Model Checkers



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 17

Properties of Reactive Systems



Letter Sorting Machine

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 15

Model Checkers

Input

- Finite-state model of a system
- Temporal logic property



Output

- "true" if the property is satisfied
- Otherwise a counterexample



© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-1 Slide 18