

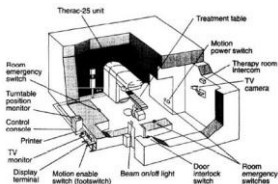
# Mathematical Foundations of Computer Science

Lecture # 1: Motivation, Background

Peter Fejer  
September 7, 2016

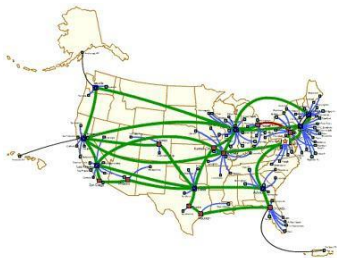
Note: Most of the material in these slides comes from slides produced by Prof. Joost-Pieter Katoen and is used with his permission.

## Therac-25 Radiation Overdosing (1985-87)



- Radiation machine for treatment of cancer patients
- At least 6 cases of overdose in period 1985–1987 ( $\approx$  100-times dose)
- Three cancer patients died
- Source: Design error in the control software (*race condition*)

## AT&T Telephone Network Outage (1990)



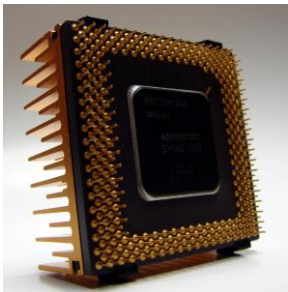
- January 1990: problem in New York City leads to 9 hour-outage of large parts of U.S. telephone network
- Cost: several \$100 million
- Source: software flaw (wrong interpretation of break statement in C)

## Ariane 5 Crash (1996)



- Crash of the European Ariane 5-missile in June 1996
- Costs: more than \$500 million
- Source: software flaw in the control software
- A data conversion from a 64-bit floating point to 16-bit signed integer
- Efficiency considerations had led to the disabling of the software handler (in Ada)

## Pentium FDIV Bug (1994)



- FDIV = floating point **d**ivision unit
- Certain floating point division operations performed produced incorrect results
- Byte Mag: 1 in 9 billion floating point divides with random parameters would produce inaccurate results
- Loss:  $\approx$  \$500 million (all flawed processors were replaced) + enormous image loss of Intel Corp.
- Source: missing entries in a table

# The Quest for Software Correctness

Speech@50-years Celebration CWI Amsterdam

“It is fair to state, that in this digital era correct systems for information processing are more valuable than gold.”



Henk Barendregt

## The Importance of Software Correctness

Rapidly increasing **integration of ICT** in different applications

- embedded systems
  - communication protocols
  - transportation systems
- ⇒ reliability increasingly depends on software!

Defects can be **fatal** and extremely **costly**

- products subject to mass-production
- safety-critical systems

# What is System Verification?

## Folklore “definition”

System verification amounts to check whether a system fulfills the qualitative requirements that have been identified

## Verification $\neq$ validation

- Verification = “check that we are building the thing **right**”
- Validation = “check that we are building the **right** thing”



# Software Verification Techniques

## Peer reviewing

- static technique: manual code inspection, no software execution detects
- between 31% and 93% of defects with median of about 60% subtle errors
- (concurrency and algorithm defects) hard to catch

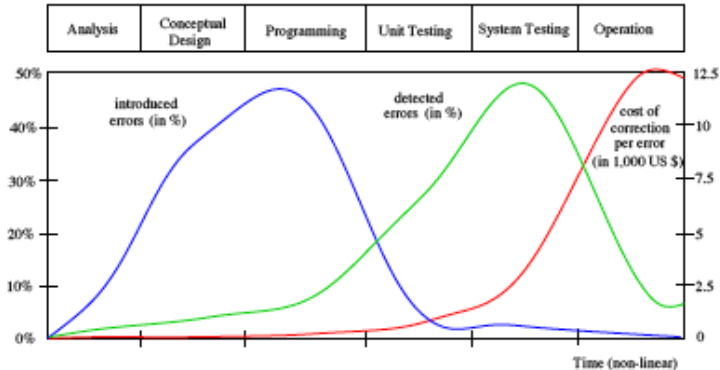
## Testing

- dynamic technique in which software is executed

## Some figures

- 30% to 50% of software project costs devoted to testing
- more time and effort is spent on validation than on construction
- accepted defect density: about 1 defects per 1,000 code lines

# Bug Hunting: the Sooner, the Better



# Formal Methods

## Intuitive description

Formal methods are the

“applied mathematics for modeling and analyzing ICT systems”

## Formal methods offer a large potential for:

- obtaining an **early integration** of verification in the design process
- providing **more effective** verification techniques (higher coverage)
- **reducing** the verification time

## Usage of formal methods

Highly recommended by IEC, FAA, and NASA for safety-critical software

# Formal Verification Techniques for Property $P$

## Deductive methods

- method: provide a formal **proof** that  $P$  holds
- tool: theorem prover/proof assistant or proof checker
- applicable if: system has form of a mathematical theory

## Model checking

- method: **systematic check** on  $P$  in all states
- tool: model checker (Spin, NuSMV, UppAal, ...)
- applicable if: system generates (finite) behavioral model

## Model-based simulation or testing

- method: test for  $P$  by **exploring possible behaviors**

# Simulation and Testing

## Basic procedure:

- take a model (simulation) or a realization (testing)
- stimulate it with certain inputs, i.e., the tests
- observe reaction and check whether this is “desired”

## Important drawbacks:

- number of possible behaviors is very large (or even infinite)
- unexplored behaviors may contain the fatal bug

## About testing . . .

testing/simulation can show the presence of errors, **not** their absence

# Milestones in Formal Verification

- **Mathematical program correctness** (Turing, 1949)
- **Proof-based technique for sequential programs** (Hoare, 1969)
  - for a given input, does a computer program generate the correct output?
  - based on compositional proof rules expressed in predicate logic
- **Proof-based technique for concurrent programs** (Pnueli, 1977)
  - handles properties referring to states during the computation
  - based on proof rules expressed in temporal logic
- **Automated verification of concurrent programs**
  - model-based instead of proof-rule based approach
  - does the concurrent program satisfy a given (logical) property?

# Example Proof Rules

## Backward axiom

$$\frac{}{\{A[e/x]\} x := e \{A\}}$$

## Invariant rule

$$\frac{\{I \wedge b\} P \{I\}}{\{I\} \text{ while } b \text{ do } P \{I \wedge \neg b\}}$$

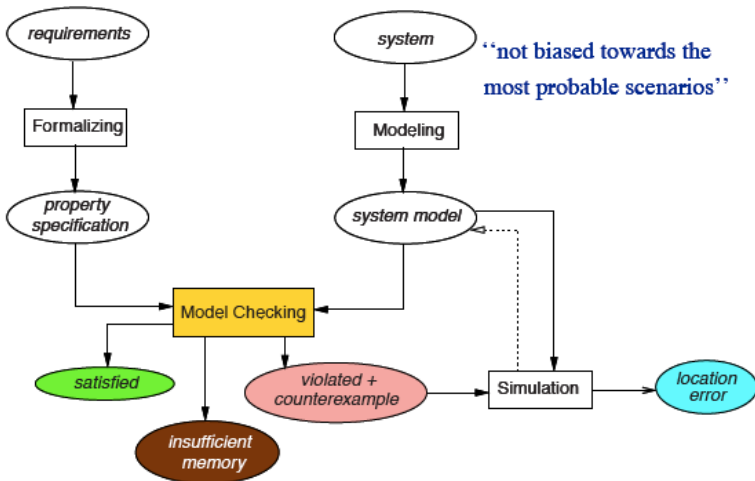
## Cut rule

$$\frac{\{A\} P \{B\} \quad \{B\} Q \{C\}}{\{A\} P; Q \{C\}}$$

## Logical rule

$$\frac{A \Rightarrow A' \quad \{A'\} P \{B'\} \quad B' \Rightarrow B}{\{A\} P \{B\}}$$

# Model Checking Overview





## Paris Kanellakis Theory and Practice Award 1998



Randal  
Bryant



Edmund  
Clarke



E. Allen  
Emerson



Ken  
McMillan

For their invention of "symbolic model checking," a method of formally checking system designs, which is widely used in the computer hardware industry and starts to show significant promise also in software verification and other areas.

Some other winners: Rivest et al., Paige and Tarjan, Buchberger, . . .

# Gödel Prize 2000



Moshe Vardi



Pierre Wolper

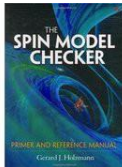
“For work on model checking with finite automata.”

Some other winners: Shor, Sénizergues, Agrawal et al., ...

# ACM System Software Award 2001



Gerard J. Holzmann



SPIN book

SPIN is a popular open-source software tool, used by thousands of people worldwide, that can be used for the formal verification of distributed software systems.

Some other winners: TeX, Postscript, UNIX, TCP/IP, Java, Smalltalk

## ACM Turing Award 2007



Edmund Clarke



E. Allen Emerson

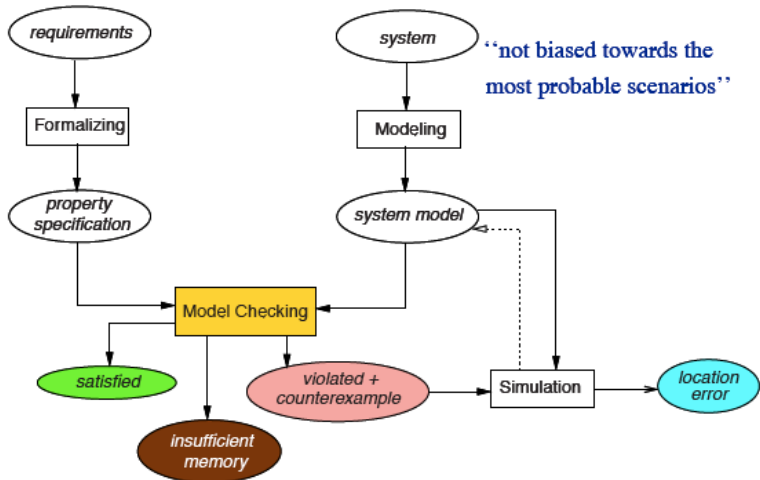


Joseph Sifakis

“For their role in developing Model-Checking into a highly effective verification technology, widely adopted in the hardware and software industries.”

Some other winners: Dijkstra, Cook, Hoare, Rabin and Scott

# Model Checking Overview

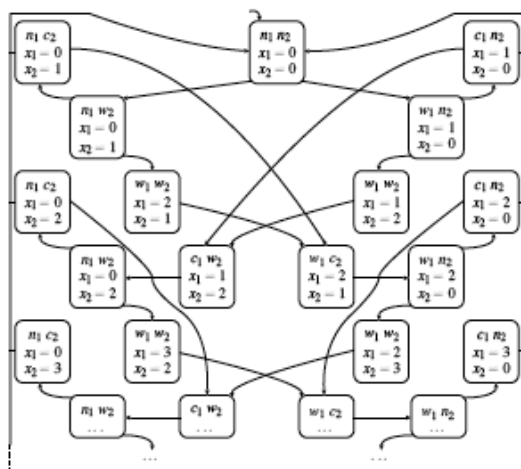


# What is Model Checking?

## Informal description

Model checking is an automated technique that, given a finite-state model of a system and a formal property, systematically checks whether this property holds for (a given state in) that model.

# What are Models?



# What are Models?

## Transition systems

- States labeled with basic propositions
- Transition relation between states
- Action-labeled transitions to facilitate composition

## Expressivity

- Programs are transition systems
- Multi-threading programs are transition systems
- Communicating processes are transition systems
- Hardware circuits are transition systems
- What else?



# What are Properties?

## Example properties

- Can the system reach a deadlock situation?
- Can two processes ever be simultaneously in a critical section?
- On termination, does a program provide the correct output?

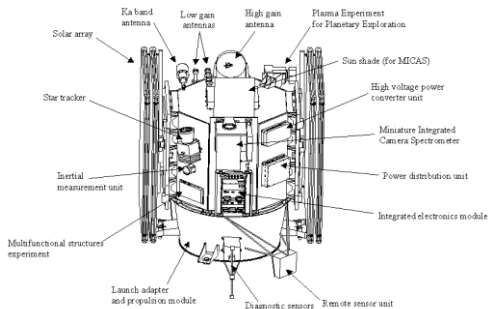
## Temporal logic

- Propositional logic
- Modal operators such as  $\Box$  “always” and  $\blacklozenge$  “eventually”
- Interpreted over state sequences (linear)
- Or over infinite trees of states (branching)

# NASA's Deep Space-1 Spacecraft

## Model checking

has been applied to several modules of this spacecraft



launched in October 1998

## A Small Program Fragment

```
process Inc = while true do if  $x < 200$  then  $x := x + 1$  od  
process Dec = while true do if  $x > 0$  then  $x := x - 1$  od  
process Reset = while true do if  $x = 200$  then  $x := 0$  od
```

*is  $x$  always between (and including) 0 and 200 if it starts in this range?*

# Modeling in NanoPromela

```
int x = 0;

proctype Inc() {
  do :: true -> if :: (x < 200) -> x = x + 1 fi od
}

proctype Dec() {
  do :: true -> if :: (x > 0) -> x = x - 1 fi od
}

proctype Reset() {
  do :: true -> if :: (x == 200) -> x = 0 fi od
}

init {
  atomic{ run Inc() ; run Dec() ; run Reset() }
}
```

## How to Check?

Extend the model with a “monitor” process that checks  $0 \leq x \leq 200$ :

```
proctype Check() {  
    assert (x >= 0 && x <= 200)  
}  
  
init {  
    atomic{ run Inc() ; run Dec() ; run Reset() ; run Check() }  
}
```

# A Counterexample

```
.....
605: proc  1 (Inc)   line   9 "pan_in" (state 2) [((x<200))]
606: proc  1 (Inc)   line   9 "pan_in" (state 3) [x = (x+1)]
607: proc  3 (Dec)  line   5 "pan_in" (state 2)  [((x > 0))]
608: proc  1 (Inc)   line   9 "pan_in" (state 1) [(1)]
609: proc  3 (Reset) line  13 "pan_in" (state 2) [((x==200))]
610: proc  3 (Reset) line  13 "pan_in" (state 3) [x = 0]
611: proc  3 (Reset) line  13 "pan_in" (state 1) [(1)]
612: proc  2 (Dec)   line   5 "pan_in" (state 3) [x = (x-1)]
613: proc  2 (Dec)   line   5 "pan_in" (state 1) [(1)]

spin: line  17 "pan_in", Error: assertion violated
spin: text of failed assertion: assert(((x>=0)&&(x<=200)))
```

# Breaking the Error

```
int x = 0;

proctype Inc() {
  do :: true -> atomic{ if :: x < 200 -> x = x + 1 fi } od
}

proctype Dec() {
  do :: true -> atomic{ if :: x > 0 -> x = x - 1 fi } od
}

proctype Reset() {
  do :: true -> atomic{ if :: x == 200 -> x = 0 fi } od
}

init {
  atomic{ run Inc() ; run Dec() ; run Reset() }
}
```

# The Model Checking Process

- **Modeling phase**
  - model the system under consideration
  - as a first sanity check, perform some simulations
  - formalize the property to be checked
- **Running phase**
  - run the model checker to check the validity of the property in the model
- **Analysis phase**
  - property satisfied? → check next property (if any)
  - property violated? →
    - 1 analyze generated counterexample by simulation
    - 2 refine the model, design, or property . . . and repeat the entire procedure
  - out of memory? → try to reduce the model and try again



# The Pros of Model Checking

- widely applicable (hardware, software, protocol systems, ...)
- allows for partial verification (only most relevant properties)
- potential “push-button” technology (software-tools)
- rapidly increasing industrial interest
- in case of property violation, a counterexample is provided
- sound and interesting mathematical foundations
- not biased to the most possible scenarios (such as testing)

## The Cons of Model Checking

- main focus on **control-intensive** applications (less data-oriented)
- model checking is only as “good” as the system model
- no guarantee about **completeness** of results
- impossible to check **generalizations** (in general)

Nevertheless:

*Model checking is a effective technique  
to expose potential design errors*

# Striking Model-Checking Examples

- **Security: Needham-Schroeder encryption protocol**
  - error that remained undiscovered for 17 years unrevealed
- **Transportation systems**
  - train model containing  $10^{476}$  states
- **Model checkers for C, Java and C++**
  - used (and developed) by Microsoft, Digital, NASA
  - successful application area: device drivers
- **Dutch storm surge barrier in Nieuwe Waterweg**
- **Software in the current/next generation of space missiles**
  - NASA's Mars Pathfinder, Deep Space-1, JPL LARS group

## Course Topics

### What are appropriate **models**?

- transition systems
- from programs to transition systems
- from circuits to transition systems
- multi-threading, communication, . . .
- nanoPromela: an example modeling language

### What are **properties**?

- safety: “something bad never happen”
- liveness: “something good eventually happens”
- fairness: “if something may happen frequently, it will happen”

## Course Topics

### How to check **regular** properties?

- finite-state automata and regular safety properties
- Büchi automata and  $\omega$ -regular properties
- model checking: nested depth-first search

### How to express properties **succinctly**?

- Linear-time Temporal Logic (LTL): syntax and semantics
- What can be expressed in LTL?
- LTL model checking: algorithms, complexity
- How to treat fairness in LTL

## Course Topics

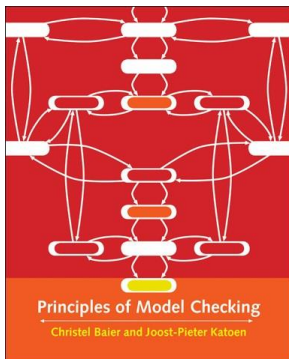
### How to express properties **succinctly**?

- Computation Tree Logic (CTL): syntax and semantics
- What can be expressed in CTL?
- CTL model checking: algorithms, complexity
- How to treat fairness in CTL

### How to make models smaller?

- Equivalences and pre-orders on transition systems
- Which properties are preserved?
- Minimization algorithms

# Course Material



## Principles of Model Checking

**Christel Baier**

TU Dresden, Germany

**Joost-Pieter Katoen**

RWTH Aachen University, Germany

Gerard J. Holzmann, NASA JPL, Pasadena:

*“This book offers one of the most comprehensive introductions to logic model checking techniques available today. The authors have found a way to explain both basic concepts and foundational theory thoroughly and in crystal clear prose.”*

