From Model Checking to Model Learning

Two Basic Techniques in Model-Based Development of Embedded Systems

Frits Vaandrager
fvaan@cs.ru.nl
Model-Based System Development

Vision: Models as primary artifacts throughout engineering lifecycle of computer-based systems

Models used for:
- Communication between stakeholders
- Simulation, verification and validation
- Design space exploration
- Code generation
- Testing
- Reuse
Model-Based Development at Océ

Happy flow model of paper path

Co-simulation of paper path with VDM++ and bond graphs

Use of Uppaal for data path scheduling

Adaptive control of printer behaviour using Bayesian networks

“The modelling approach from Boderc has enabled Océ to skip a complete physical machine-building iteration cycle, saving many man-years of effort”
Two Fundamental Research Questions

- How can we prove interesting behavioral properties of complex models?
  - model checking

- How can we obtain valid models of existing (legacy, black box, ..) components?
  - model learning
Overview Talk

- Model Checking
- Model Learning
- Research Funding
Part 1: Model Checking
Model Checking

M: Traffic Light Controller

P: No Collisions

Does M satisfy P?

Yes!

No, and here’s an example of why not.
Example: Gossip Girl Problem

Five girls all have a gossip of their own.

They call each other over the phone. Whenever two girls talk they exchange all gossips they know.

How many calls are needed before every girl knows every gossip?
State Machine
Solution Model Checker
Real Time Systems

**Control Theory**

Plant

*Continuous*

**Computer Science**

Controller Program

*Discrete*

Eg.: Pump Control
Air Bags
Robots
Cruise Control
ABS
CD Players
Production Lines

Real Time System
A system where correctness not only depends on the logical order of events but also on their *timing*
WANT: if press is issued twice quickly then the light will get brighter; otherwise the light is turned off.
Timed Automata

Solution: Add real-valued clock $x$
UPPAAL 4.0
Impact

Company Downloads
Mecel
Jet
Symantec
SRI
Relogic
Realwork
NASA
Verified Systems
Microsoft
ABB
Airbus
PSA
Saab
Siemens
Volvo
Lucent Technologies
Etc etc
Observation

(EU VHS project)

Many scheduling problems can be phrased in a natural way as reachability problems for timed automata.
Challenge Océ: Design of printer data path

Use cases:

- Printing
- Scanning

Mapping constraints

Typical requirements:
1. Throughput must be X pages per minute
2. Scanning should not disrupt printing

Hardware platform: board template

Dimensioning constraints:
1. FPGA buffer memory size
2. CPU/GPU count & speed
3. Bus bandwidth

DESIGN OBJECTIVE
- good mapping and scheduling
- satisfy requirements
- right sizes
From Printer Models to Uppaal
From Uppaal to Gantt Charts

Challenges

- Dynamic resources
- Timing uncertainty
- Repetitive behavior
Why Timed Games?

- **Controller synthesis:**
  - Model the environment + what a controller *can* do.
  - Generate controller that meets control objective
  - Generate the *right* code automatically.
  - 2-player timed game: environment moves vs controller moves
    ⇒ Timed Game Automata
Timed Game Automata

- Timed automata with controllable and uncontrollable transitions
- Reachability & safety games
  - control: A<> TGA.goal
  - control: A[] not TGA.L4
- Memoryless strategy:
  - state $\rightarrow$ action
Using Timed Games for Printers
Outcomes ESI project Octopus

- Toolset for Model-Driven Design-Space Exploration
- Addresses Océ challenges

- Analysis plugins
- DSEIR (design-space exploration intermediate representation)
- Domain-Specific Modeling
- Search plugins
- Diagnostics plugins
Part 2: Model Learning
Children Learn How to Use Computers

Can computers learn state diagrams as well?
Angluin’s L* Algorithm (1987)

Learning Finite Automata:

Teacher

Membership Queries

Yes / No

Equivalence Queries

Yes / No + Counterexample

Learner
Learning Models of Reactive Systems

Learner: Formulate hypothesis
Model-Based Testing: Test hypothesis
LearnLib Tool

- Tool for active learning of Mealy machine models
- Developed by group Bernhard Steffen (University Dortmund)
- Able to learn models with up to 10,000 states
Case Study: Biometric Passport
Case Study: Banking Cards

- Reverse engineering of EMV protocol applications for collection of banking and credit cards

- Simple models with up to 7 states (NB EMV standard has over 700 pages)

- At most 1500 membership queries, less than 30 minutes

- Models provide unique fingerprints of different cards

- Useful as part of security evaluation
Case Study: Philips Bounded Retransmission Protocol

Use learning to test whether BRP protocol implementations are correct relative to reference implementation.
Experimental Setting

- All correct/incorrect implementations of BRP identified via both routes
- Correct models learned for 5 out of 6 mutant implementations of BRP
Case Study: Engine Status Manager of Océ Printer

Goal: learn models of realistic printer controllers

Possible use: regression testing, generation of new implementations,..
Visualisation of Learned Model

1314 states, 64.136.029 member queries
Use of Mappers to Handle Data
**Theory**

- Mapper induces two transformations:
  - An abstraction operator $\alpha_A$ that transforms concrete models into abstract models
  - A concretization operator $\gamma_A$ that transforms abstract models into concrete models

- **Theorem 1.** *Suppose* $\alpha_A(M) \leq H$. *Then* $M \leq \gamma_A(H)$. 
Tomte Tool

Compute abstractions automatically

SUT 

Concrete Input → Concrete Output

Mapper

Abstract Input → Abstract Output

Learner 

LearnLib
Learned model is extended finite state machine with 29 states, 3741 transitions, and 17 state variables with various types
Research Challenges

- Learn models with structure (data,..)
- Cope with state space explosion
- Visualisation of learned models
- Cope with nondeterminism SUTs
- ...

Conclusions/Perspective

- Promissing technique, many potential applications

- Useful for control intensive systems, such as network protocols and control software

- More research needed before routine use in commercial setting is feasible

- Wanted: challenging case studies!
Part 3: Research Funding
Lampson’s Tire Tracks

Interplay of university research, industrial research, and development for IT in the US (A)

- 1965
  - Timesharing
  - Client/server computing

- 1970
  - Graphics

- 1975
  - Entertainment

- 1980
  - LANs

- 1985
  - Workstations
  - Graphical User Interfaces
  - VLSI design

- 1990

- 1995

- 2000

CTSS, Multics / BSD
Unix
SDS 940, 36067, VMS
Berkeley, CMU, CERN
Pac, DEC, IBM
Novell, EMC, Sun, Oracle
Sketchpad, Utah
GM/IBM, Xerox, Microsoft
EoS, SGI, AT&T, Adobe

Spacewar (MIT), Tek (Rochester)
Atari, Nintendo, SGI, Pixar
Arpanet, Apollo, Internet
Pup
DECnet, TCP/IP

Rings, Hubnet
Ethernet, Datalink, Autonet
LANs, switched Ethernet

Lisp machine, Stanford
Xerox Alto
Xerox Star, Apollo, Sun
Engelbart / Rochester
Alto, Smalltalk
Star, Mac, Microsoft
Berkeley, Caltech, Mosaic

many
Final Report for Period: 09/1994 - 08/1999
Principal Investigator: Garcia-Molina, Hector
Organization: Stanford University
Title: The Stanford Integrated Digital Library Project

Senior Personnel
Name: Garcia-Molina, Hector
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Paepcke, Andreas
Worked for more than 160 Hours: Yes
Contribution to Project:
Project Director

Post-doc

Graduate Student
Name: Page, Larry
Worked for more than 160 Hours: Yes
Contribution to Project:
Name: Chang, Ed
Worked for more than 160 Hours: Yes
Contribution to Project:
Name: Chang, Kevin
Worked for more than 160 Hours: Yes
The Google search engine was developed as part of the project. It is now a company (www.google.com)
How About Us (NL)?

- Read Martin Rem’s book “Tegen de Stroom” : ASML, TomTom, WiFi, Bluetooth, Python, AMS-IX,..

- 21 Spin Offs CWI: Data Distilleries, MonetDB, Spinque, SIG, VectorWise,..

- ..

But we can do better!
Research Funding within NWO

- Other disciplines tend to view CS as less fundamental

- Applied/multidisciplinary research less favored

- CS researchers hypercritical

Need separate budget for CS research
Grades for CS Proposals in US
Representation different areas in Dutch CS unbalanced

- Intelligent systems and Formal methods overrepresented

- Minimal presence Computer systems, Database systems, Algorithms, Graphics

- Need more experimental systems research
ICT Research Funding

- Dutch government / NWO does not recognize importance ICT research
- Dutch government should invest more in education/research anyway
- Help/stimulate spin off companies

- Societal relevance should play larger role in allocation research money
  (Idea to let NWO support “Top sectors” good -up to a point; idea to stop FES bad)
US industry support voor Dutch CS research/education

2010 Google Europe Doctoral Fellowship Recipients

- Roland Angst, Google Europe Fellowship in Computer Vision (Swiss Federal Institute of Technology Zurich, Switzerland)
- Arnar Birgisson, Google Europe Fellowship in Computer Security (Chalmers University of Technology, Sweden)
- Omar Choudary, Google Europe Fellowship in Mobile Security (University of Cambridge, U.K.)
- Michele Coscia, Google Europe Fellowship in Computer Vision (University of Cambridge, U.K.)
- Moran Feldman, Google Europe Fellowship in Computer Security (University of Cambridge, U.K.)
- Neil Houlsby, Google Europe Fellowship in Machine Learning (University of Cambridge, U.K.)
- Kasper Dalgaard Larsen, Google Europe Fellowship in Computer Vision (University of Cambridge, U.K.)
- Florian Laws, Google Europe Fellowship in Computer Security (University of Cambridge, U.K.)
- Cynthia Liem, Google Europe Fellowship in Computer Vision (University of Cambridge, U.K.)

The project Dome is the unique research collaboration between IBM Netherlands and ASTRON. In this project fundamental research is performed in the field of Radio Astronomy and will concentrate on three domains:

1. Green supercomputing (extreme performance at minor energy costs)
2. Extreme Streaming (real time processing on a permanent basis of massive data amounts)

De Amerikaanse softwaregigant Microsoft is bereid een miljoen euro te steken in een onderzoek van de TU Delft naar zogenaamde quantumcomputers. De laatste handtekening van de deal is op de post gegaan, zo stelde Spinozaprijswinnaar Leo Kouwenhoven van de universiteit en onderzoeksleider vrijdag naar aanleiding van een bericht daarover in de Volkskrant.
What Should ICT Industry Do?

- Help improve image ICT profession and ICT studies
- Better lobby for more/better investments in ICT studies/research
What Should Academic Researchers Do?

- Work on fundamental problems
- Be inspired by practice
- Theory – tools – applications cycle
- Practice as laboratory
Thank You!

Questions?