Embedded Software Laboratory

RWTH AACHEN UNIVERSITY

Seminar: Applying Formal Verification Methods to Emebdded Systems

Jörg Brauer, Joost-Pieter Katoen, Stefan Kowalewski, Thomas Noll, Bastian Schlich

First Meeting – 05.02.2009

People

- Software Modeling and Verification Group (I2)
  - Professor Dr. Ir. Joost-Pieter Katoen
  - AOR Priv.-Doz. Dr. Thomas Noll
    noll@cs.rwth-aachen.de
  - N. n.
- Embedded Software Laboratory (I11)
  - Professor Dr.-Ing. Stefan Kowalewski
  - Dr. Bastian Schlich (BS)
    schlich@embedded.rwth-aachen.de
  - Dipl.-Inform. Jörg Brauer (JB)
    brauer@embedded.rwth-aachen.de

Procedure

- Weekly seminar
- Tuesday 15:00 - 17:00 (21.04.2009)
- Deadlines (relative)
  - 6 weeks before talk: literature + structure
  - 2 weeks before talk: final version of paper
  - 1 week before talk: final version of slides

Rules - Disqualification

- Unsatisfactory submission
- Not correcting borderline submission
- Missing more than one deadline
- Missing a deadline by more than three days
- Missing a meeting/talk

Literature + Structure

- Course in library (mandatory for Bachelors)
- Search for additional literature
- Structure of the paper
- PDF file

Paper

- 15 pages in given style
- PDF + Latex
- Bound into a single document
- No direct translation
- Own contribution
  - Combining several articles/papers
  - Evaluation

Talk

- 35 minutes
- 10 minutes discussion
- Slides
  - Power Point or PDF
  - Readability
  - No overfull slides
  - No fancy colors
  - Slide numbers

Topics

- 10 theoretical topics supervised by I2
- 10 practical topics supervised by I11
- Pairs of theoretical and practical topics
- Exchange information in these pairs

Topic 1: Data Flow and Control-Flow Analysis (I2)

- Flemming Nielson, Hanne R. Nielson, Chris Hankin: *Principles of Program Analysis*, 2nd ed., Springer, 2005 (Sct. 1.3 and 2)
- Student: Hu

Topic 2: Worst Case Execution Time Analysis (JB)

- Christian Ferdinand, Reinhold Heckmann, Marc Langenbach, Florian Martin, Michael Schmidt, Henrik Theiling, Stephan Thesing, Reinhard Wilhelm: *Reliable and Precise WCET Determination for a Real-Life Processor*, EMSOFT 2001, LNCS 2211, 2001, 469-485
- Student: Angel

Topic 3: Abstract Interpretation (I2)

- Flemming Nielson, Hanne R. Nielson, Chris Hankin: *Principles of Program Analysis*, 2nd ed., Springer, 2005 (Sct. 1.5 and 4)
- Student: Holger

Topic 4: Abstract Interpretation of Reactive Systems (JB)

- D. Dams, R. Gerth, O. Grumberg: *Abstract Interpretation of Reactive Systems*, ACM Transactions on Programming Languages and Systems 19(2), 1997, 253-291
- Student: Julia

Topic 5: Slicing (I2)

- F. Tip: *A Survey of Program Slicing Techniques*, Journal of Programming Languages 3(3), 1995, 121-189
- Student: Falak

Topic 6: Application of Slicing to Model Checking (JB)

- J.Hatcliff, M.B.Dwyer, H.Zheng: *Slicing Software for Model Construction*. J. Higher Order Symbol. Comput. 13(4):315-353, 2000
- Student: Gao

Topic 7: Separation Logic (I2)

- John C. Reynolds: *Separation Logic: A Logic for Shared Mutable Data Structures*. LICS 2002: 55-74
- Student: Philipp

Topic 8: Shape Analysis (JB)

- Dino Distefano, Peter W. O'Hearn, Hongseok Yang: *A local shape analysis based on separation logic*, In Proc. of the 12th TACAS, vol. 3920, pp. 287-302, 2006
- Alexey Gotsman, Josh Berdine, Byron Cook: *Interprocedural Shape Analysis with Separated Heap Abstractions*, In Proc. of the 13th SAS, vol. 4134, pp. 240-260, 2006
- Student: Christian

Topic 9: CTL Model Checking (I2)

- C. Baier, J.-P. Katoen: *Principles of Model Checking*, MIT Press, 2008 (Sct. 6)
- Student: Stefan

Topic 10: [mc]square (BS)

- Bastian Schlich and Stefan Kowalewski: *[mc]square: A model checker for microcontroller code*, In Proc. of ISoLA 2006, pp. 466-473, IEEE Computer Society
- Bastian Schlich: *Model Checking of Software for Microcontrollers*, Dissertation Thesis. AIB-2008-14, RWTH Aachen University, 2008
- Student: Sebastian

Topic 11: Runtime Verification Using LTL (I2 – Practical Topic)

- V. Stolz, F. Huch: *Runtime verification of Concurrent Haskell programs*. Proceedings of the Fourth Workshop on Runtime Verification (RV 2004), ENTCS 113, Elsevier, 2004, 201-216
- V. Stolz, E. Bodden: *Temporal Assertions using AspectJ*, Proceedings of the Fifth Workshop on Runtime Verification (RV 2005), ENTCS 144(4), 2006,109-124
- Student: Fehmi

Topic 12: Java Path Finder (BS)

- K. Havelund and J. Skakkebaek: *Applying Model Checking in Java Verification*, In Proc. of the 7th Workshop on the SPIN Verification System, 1999, 216-231, LNCS
- Student: Norbert

Topic 13: Model Checking Timed Automata (I2)

- François Laroussinie, Nicolas Markey, Ph. Schnoebelen: *Model Checking Timed Automata with One or Two Clocks*. CONCUR 2004: 387-401. LNCS, Springer Verlag.
- Student: Daniel

Topic 14: Uppaal (BS)

- Ansgar Fehnker, Lodewijk van Hoesel and Angelika Mader*: Modelling and Verification of the LMAC Protocol for Wireless Sensor Networks*, Integrated Formal Methods, pages 253-272, LNCS, 2007
- Student: Rajeevan

Topic 15: Model Checking Hybrid Automata/Systems (I2)

- Rajeev Alur, Costas Courcoubetis, Nicolas Halbwachs, Thomas A. Henzinger, Pei-Hsin Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis, Sergio Yovine: *The Algorithmic Analysis of Hybrid Systems*. Theor. Comput. Sci. (TCS) 138(1):3-34 (1995)
- Student: Ivan

Topic 16: PHAVer (BS)

- Goran Frehse: *PHAVer: algorithmic verification of hybrid systems past HyTech*, International Journal on Software Tools for Technology Transfer (STTT), pages 263-279, 2008
- Student: Mustafa

Topic 17: Probabilistic Model Checking (I2)

- C. Baier, J.-P. Katoen: *Principles of Model Checking*, MIT Press, 2008 (Sct. 10)
- Student: Mike

Topic 18: Validating Wireless Sensor Network Protocols (BS)

- A. Boulis, A. Fehnker, M. Fruth, A. McIver. *CaVi -- Simulation and Model Checking for Wireless Sensor Networks.* QEST 2008
- Student: Andreas W.

Topic 19: Equivalences: Simulation and Bisimulation (I2)

- C. Baier, J.-P. Katoen: *Principles of Model Checking*, MIT Press, 2008 (Sct. 7)
- Student: Andreas H.

Topic 20: Dead Variable Reduction and Path Reduction (JB)

- Bastian Schlich, Jann Löll, Stefan Kowalewski: *Application of Static Analyses for State Space Reduction to Microcontroller Assembly Code*, FMICS, pages 21-37, 2008, LNCS
- Karen Yorav and Orna Grumberg: *Static Analysis for State-Space Reductions Preserving Temporal Logics*, Formal Methods in System Design, pages 67-96, 2004
- Student: Aamer

Further Questions?