

CMPE 58Q: Formal Verification of Hardware and Software Systems, Spring 2009

Instructor: Asst. Prof. Alper Sen **Email:** alper.sen@boun.edu.tr **Office Hours:** By appointment
Website: <http://www.cmpe.boun.edu.tr/courses/cmpe58Q/spring2009/>

Functional Verification consumes a big portion of the overall design cycle. This task is complicated with the increasing size and complexity of designs. In this class, we will read and discuss research papers on verification of concurrent systems. Students will gain an understanding of some core and state of the art solutions in verification of concurrent systems. These systems include hardware as well as software systems. SoCs, parallel programs.

Each student is expected to do an exhaustive research on the chosen topics. The presentations need to be discussed with the instructor before class presentation. The term projects will be written in a research paper format.

Grading will be done based on class presentations, class participation, term project and term paper.

Topics of interest are as follows:

- Formal verification techniques: model checking, temporal logic, Binary Decision Diagrams (BDD), SAT, assertion based verification, System Verilog Assertion (SVA), Partial Order Reduction, Bounded Model Checking (BMC).
- Dynamic verification techniques: simulation-based verification, predictive verification, Dynamic Partial Order Reduction (DPOR), test benches, slicing.
- System level verification techniques: SystemC, virtual prototyping/verification.
- Equivalence checking: combinational and sequential equivalence checking
- Debugging, Error Diagnosis
- Coverage techniques: simple, functional, mutation based coverage
- Automated deadlock and race detection
- Emulation, FPGA prototyping based verification
- Design validation techniques

Sample List of Papers:

BDD:

- F. Somenzi. Binary Decision Diagrams. In M. Broy and R. Steinbruggen, editors, *Calculational System Design*, Vol. 173, NATO Science Series F: Computer and Systems Sciences, IOS Press, 1999.
- Formal Hardware Verification with BDDs: An Introduction by Alan J. Hu
- Alan J. Hu, Formal Hardware Verification with BDDs: An Introduction, *IEEE Pacific Rim Conference on Communications, Computers, and Signal Processing (PACRIM)*, pp.677-682, 1997.
- Randal Bryant, "Graph-Based Algorithms for Boolean Function Manipulation", *IEEE Transactions on Computers*, August 1986.

CMPE58Q

- Randal Bryant, "Symbolic Boolean Manipulation with Ordered Binary Decision Diagrams", CMU CS Tech Report CMU-CS-92-160, 1992.
- Randal Bryant, "Binary Decision Diagrams and Beyond: Enabling Technologies for Formal Verification", International Conference on Computer-Aided Design, 1995.
- R. E. Bryant's 1992 Computing Surveys paper, BDDs
- K.L. McMillan, Symbolic Model Checking. Kluwer Academic, 1993.

SAT:

- Symbolic model checking without BDDs, A. Biere, A. Cimatti, E. Clarke, and Y. Zhu.. Proc. TACAS'99.
- "Searching for Truth: Techniques for Satisfiability of Boolean Formulas", L. Zhang thesis (Ch. 2, 3, 4)
- A Survey of Recent Advances in SAT-Based Formal Verification
- Lintao Zhang and Sharad Malik, "The Quest for Efficient Boolean Satisfiability Solvers
- Chaff: Engineering an Efficient SAT Solver " M.W. Moskewicz, C.F. Madigan, Y. Zhao, L. Zhang, S. Malik, DAC 2001.
- Safety Property Verification Using Sequential SAT and BM, G. Parthasarthy, M. Iyer
- Using SAT for Combinational Equivalence Checking, E. Goldberg et al.

BMC:

- "Bounded Model Checking," A. Biere, A. Cimatti, E. M. Clarke, O. Strichman and Y. Zhu. Vol. 58 of Advances in Computers, 2003. Academic Press
- BMC Using Satisfiability Checking, E. Clarke et al.
- Verifying Safety Properties of a PowerPC Microprocessor Using Symbolic Model Checking without BDDs

POR, DPOR:

- Dynamic partial-order reduction for model checking software. Cormac Flanagan, Patrice Godefroid: Pages 110-121, POPL 2005
- E.M. Clarke, O. Grumberg, M. Minea, D. Peled: State space reduction using partial order techniques International Journal on Software Tools for Technology Transfer 2 (1999) 3, 279-287
- Model Checking Book Ch. 2
- State Space Reduction using Partial Order Techniques, E. M. Clarke, O. Grumberg, M. Minea, and D. Peled
- P. Godefroid and P. Wolper, "A Partial Approach to Model Checking," Proc. Sixth IEEE Symp. Logic in Computer Science, pp. 406-415, 1991

Temporal Logic:

- Model Checking Book Ch. 3, temporal logic
- E. M. Clarke, E. A. Emerson & A. P. Sistla, Automatic Verification of Finite-State Concurrent Systems using Temporal Logic Specifications,
- System Verilog Assertions, IEEE standard
<http://www.doulos.com/knowhow/sysverilog/tutorial/assertions/>,
- http://www.sutherland-hdl.com/papers/2006-DesignCon_Getting_Started_with_SVA_presentation.pdf

SystemC:

- Alper Sen, Vinit Ogale and Magdy S. Abadir, Predictive Runtime Verification of Multi-Processor SoCs in SystemC, Design Automation Conference (DAC), June 2008
- W. Ecker, V. Esen, T. Steininger, M. Velten, and M. Hull. Implementation of a Transaction Level Assertion Framework in SystemC. In Proceedings of the Conference on Design Automation and Test in Europe (DATE), 2007.
- Formal Verification of LTL formulas for SystemC designs, D. Grose, R. Drechsler
- CheckSyC: An Efficient Property Checker for RTL SystemC designs, D. Grose,
- Design and Verification of SystemC Transaction level Models, A. Habibi, S. Tahar
- Test Coverage for Loose Timing Annotations, S. Helmstetter et al.
- Automatic generation of schedulings for improving the test coverage of SoC, C. Helmstetter, Proceedings of the International Conference on Formal Methods in Computer Aided Design (FMCAD), 2006.
- SoC Modeling Methodology for Architectural Exploration and Software Development, M. Silbermintz, A. Shar
- PINAPA: An extraction tool for systemc descriptions of soc, M. Moy,
- A Systemc/TLM semantics in Promela and its possible applications, C. Traulsen, J. Cornet, M. Moy
- Formal techniques for SystemC verification, M. Vardi, DAC 2007
- The simulation semantics of SystemC, W. Mueller et al.
- System level validation using formal techniques, R. Drechsler, D. Grose
- A. Kasuya and T. Tesfaye. Verification methodologies in a TLM-to-RTL design flow. In Proceedings of the Design Automation Conference (DAC), 2007.
- Empirical Study of SystemC, A. Ki
- System-level validation using formal techniques, Rolf Drechsler et al.
- Open SystemC Initiative, <http://www.systemc.org/>.

Runtime Verification:

- Runtime Model Checking of Multithreaded C/C+ Programs, Y. Yang, X. Chen, G. Gopalakrishnan
- Alper Sen and Vijay K. Garg, Formal Verification of Simulation Traces Using Computation Slicing, In IEEE Transactions on Computers, April 2007
- Alper Sen and Vijay K. Garg, Partial Order Trace Analyzer (POTA) for Distributed Programs, In Proceedings of the Third International Workshop on Runtime Verification (RV), July 2003.
- Runtime Safety Analysis of Multithreaded Programs,” Koushik Sen, Grigore Rosu, and Gul Agha, FSE/ESEC'03
- DART: Directed Automated Random Testing,” Patrice Godefroid, Nils Klarlund, and Koushik Sen, PLDI'05.
- CUTE: A Concolic Unit Testing Engine for C,” Koushik Sen, Darko Marinov, and Gul Agha, ESEC/FSE'05.
- jCUTE (CUTE for concurrent programs): Gul Agha
- Hybrid Concolic Testing and LATEST: Rupak Majumdar
- Model-Checking multi-threaded distributed Java programs, S. Stoller

CMPE58Q

- K. Havelund and G. Rosu, "Monitoring Java Programs with Java PathExplorer," Proc. First Int'l Workshop Runtime Verification (RV), 2001.

Deadlock and Race Detection:

- R. Agarwal and S. D. Stoller. Run-Time Detection of Potential Deadlocks for Programs with Locks, Semaphores, and Condition Variables. In Proceedings of the Workshop on Parallel and Distributed Systems: Testing and Debugging (PADTAD), 2006.
- E. Cheung, P. Satapathy, V. Pham, H. Hsieh, and X. Chen. Runtime Deadlock Analysis of SystemC Designs. In Proceedings of the IEEE International High-Level Design Validation and Test Workshop (HLDVT), 2006.
- - O. Shacham, M. Sagiv, and A. Schuster, "Scaling Model Checking of Dataraces Using Dynamic Information," Proc. 10th ACM Symp. Principles and Practice of Parallel Programming (PPOPP), pp. 107-118, 2005.

Equivalence Checking:

- M. N. Mneimneh and K. A. Sakallah. Principles of sequential-equivalence verification. IEEE D&T Comp. Vol. 22(3), pp. 248-257, 2005.
- Jawahar Jain, Amit Narayan, Masahiro Fujita, and Alberto Sangiovanni-Vincentelli, "Formal Verification of Combinational Circuits", VLSI Design, 1997.
- A theory and Implementation of Sequential Hardware Equivalence, C. Pixley
- Behavioral Consistency of C and Verilog programs using bounded model checking, E. Clarke, D. Kroening, K. Yorav

Symbolic Trajectory Evaluation:

- Validation of PowerPC Custom Memories using Symbolic Simulation, N. Krishnamurthy et al.
- Formal Verification of PowerPC arrays using STE, M. Pandey et al.
- An Introduction to STE, K. Claessen, J. Roorda

Coverage:

- "OCCOM-efficient computation of observability-based code coverage metrics for functional verification," Fallah, F.; Devadas, S.; Keutzer, K., IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, Volume: 20 Issue: 8, Aug. 2001
- Coverage Metrics for Functional Validation of Hardware designs, S. Tasiran, K. Keutzer

Mutation Analysis:

- Leveraging a Commercial Mutation Analysis tool for Research, M. Hampton, S. Petithomme
- Impact of HW mutation on the Verification Quality Improvement, Y. Serrestou, V. Beroulle
- Mutation of Model Checker Specifications for Test Generation and Evaluation, P. Black, V. Okun
- A Mutation Model for the SystemC TLM 2.0 Communication Interfaces, N. Bombieri F. Fummi, G. Pravadelli, DATE 2008

CMPE58Q

- A Methodology for Validating Digital Circuits with Mutation Testing, P. Vado, Y. Savaria, Y. Zoccarato
- Y. Serrestou papers
- Models and Coverage Metrics for Effective System Level Validation, Tim Cheng

Error Diagnosis:

- Error Localization and System Repair, Groce et al. 2005; Griesmayer et al. 2006
- "ErrorTracer: design error diagnosis based on fault simulation techniques," Shi-Yu Huang; Kwang-Ting Cheng, IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, Volume: 18 Issue: 9, Sept. 1999
- Error Diagnosis for Transistor Level Verification, A. Kuehlmann et al.
- Design Error Diagnosis and Correction via test Vector Simulation, A. Veneris et al.
- Equivalence Checking and Design error Diagnosis for Large Circuits, T. Cheng
- On the relation between simulation-based and sat-based diagnosis, G. Roy, S. Safarpour
- Fast error diagnosis for Combinational Verification, A. Gupta et al.
- Automating Post Silicon Debugging and Repair, K. Chang, I. Markov, V. Bertacco
- Error Diagnosis in Equivalence Checking of High Performance Microprocessors, Alper Sen, Workshop on Verification and Debugging (V&D), August 2006

Vector Clocks:

- F. Mattern, "Virtual Time and Global States of Distributed Systems," Parallel and Distributed Algorithms: Proc. Workshop Distributed Algorithms (WDAG), pp. 215-226, 1989.
- L. Lamport, "Time, Clocks, and the Ordering of Events in a Distributed System," Comm. ACM, vol. 21, no. 7, pp. 558-565, July 1978.
-

Survey Papers:

- Aarti Gupta, "Formal Hardware Verification Methods: A Survey", Formal Methods in System Design, Vol. 1, pp. 151-238, 1992.
- Formal Verification in Hardware Design: A Survey C. Kern and M. Greenstreet,
- "Formal Verification in a Commercial Setting", R. P. Kurshan, Proc. Design Automation Conference, Anaheim, California, June 9-13, 1997
- Model Checking a hardware design perspective, C. Pixley, V. Singhal
- On the Effective Deployment of Functional Formal Verification, IBM paper
- Verification of Cell Broadband Engine Processor, DAC 2006
- A Survey of Automated Techniques for Formal Software Verification, Daniel Kroening et al.

Tools:

- Partial Order Trace Analyzer (POTA), SPIN model checker, Java Multithreaded Path Analyzer (JMPAX), ABC equivalence checker, VIS, SMV, CUTE, Inspect, Java Pathfinder, Eraser, Cadence IFV, Synopsys FEV

Sample Project Topics:

- SystemC verification and instrumentation with POTA tool

CMPE58Q

- Coverage metrics for SystemC
- Multicore Communication API Verification
- GPU/CUDA/Multicore programming of verification algorithms
- Mutation analysis for Verilog/SystemC
- Build a virtual prototype of a complex system using SystemC and verify

Related Conferences:

- Design Automation Conference (DAC),
- Design Automation and Test in Europe (DATE) ,
- Computer Aided Verification (CAV),
- Formal Methods in Computer Aided Verification (FMCAD),
- International Conference on CAD (ICCAD),
- Microprocessor Test and Verification Workshop (MTV),
- Automated software Engineering (ASE),
- International Parallel and Distributed Processing Symposium (IPDPS),
- International Workshop on Formal Approaches to Testing of Software (FATES),
- SPIN International Workshop,
- International Workshop on Runtime Verification (RV),
- International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS),
- IEEE International High-Level Design Validation and Test Workshop (HLDVT)

Books:

Edmund M. Clarke, Orna Grumberg, and Doron Peled	Model Checking
Michael R A Huth and Mark D Ryan	Logic in Computer Science: Modeling and reasoning about systems
Janick Bergeron	Writing Testbenches Using SystemVerilog
Rolf Drechsler	Advanced Formal Verification
Doron A. Peled.	Software Reliability Methods
B. Berard et al.	Systems and Software Verification
Malay Ganai	SAT-Based Scalable Formal Verification Solutions
Leena Singh et al.	Advanced Verification Techniques: A SystemC Based Approach for Successful Tapeout,
Grant Martin, Brian Bailey, and Andrew Piziali	ESL Design and Verification: A Prescription for Electronic System Level Methodology
Masahiro Fujita, Indradeep Ghosh, Mukul Prasad	Verification Techniques for System-Level Design
Bruce Wile, John Goss, Wolfgang Roesner	Comprehensive Functional Verification: The Complete Industry Cycle
Douglas L. Perry , Harry Foster	Applied Formal Verification
Christel Baier, Joost-Pieter Katoen,	Principles of Model Checking

CMPE58Q

Kim Guldstrand Larsen	
Gerard J. Holzmann	The Spin Model Checker
Hiren D. Patel, Sandeep K. Shukla	Ingredients for Successful System Level Design Methodology
Thomas Kropf	Introduction to Formal Hardware Verification
James Reinders	Intel Threading Building Blocks: Outfitting C++ for Multi-core Processor Parallelism

Links on presentations:

<http://research.microsoft.com/en-us/um/people/simonpj/papers/giving-a-talk/giving-a-talk.htm>

<http://www.dac.com/45th/visual/prepkeep.html>