**Multi-University Research Initiative on**

**High-Confidence Design for Distributed Embedded Systems**

Frameworks and Tools for High-Confidence Design of

Adaptive, Distributed Embedded Control Systems

**Progress Report 2010**

Team Member: Edmund M. Clarke, Computer Science Department, CMU

# Accomplishments and New Findings

The work reported has been jointly carried out by Prof. Edmund M. Clarke and Prof. André Platzer.

## Statistical Model Checking

Statistical Model Checking is an efficient technique for solving the Probabilistic Model Checking problem that is, finding out whether a system satisfies a specification with at least (or at most) a fixed probability. For example: “does the system fulfill a request within 1ms with probability at least 0.99?”

Our Statistical Model Checking approach encompasses both hypothesis testing and estimation, and it is based on Bayes’ theorem and sequential sampling. Bayes’ theorem enables us to incorporate prior information about the model being verified, where available. Sequential sampling means that the number of sampled traces is not fixed a priori, but it is instead determined at “run-time”, depending on the evidence gathered by the samples seen so far. This often leads to significantly smaller number of sampled traces (simulations). Our estimation method follows directly from our Bayesian approach. In fact, Bayes’ theorem enable us to obtain the posterior distribution of the true probability *p* with which the model satisfies the formula (i.e., the distribution of *p* according to the data sampled and chosen prior). By integrating the posterior over a suitably chosen interval, we can compute a Bayes interval estimate with any given confidence coefficient.

We have continued investigating the applicability of Bayesian Statistical Model Checking to the verification of Probabilistic Bounded Linear Temporal Logic (PBLTL) properties of Simulink/Stateflow (SL/SF) models. The technique combines model checking of system simulation traces and statistical techniques to infer whether a property is true or not. In particular, it uses Bayesian hypothesis testing and estimation. We have proved error bounds for both statistical techniques. We have applied the approach to a SL/SF model implementing a fault-tolerant fuel control system for a gasoline engine, with very good performance results. In particular, our estimation method can be orders of magnitude faster than other estimation-based model checking techniques. This work was presented at the HSCC 2010 conference.

First-year student Anvesh Komuravelli (CMU) has devised and implemented a model checker for BLTL formulas. The algorithm analyzes system traces “on the fly”, i.e., element by element, without requiring access to the full trace. This feature is highly desirable for Statistical Model Checking, because we wish to stop system simulation as soon as we can decide whether a BLTL property is true or false on the current trace. Also, the algorithm does not store any information about the trace being analyzed, so its memory requirements are minimal. A technical report is forthcoming.

On 17-19 May 2010, Paolo Zuliani (CMU) visited Vanderbilt, in order to start integrating CMU’s statistical model checking techniques with Vanderbilt’s tool chain. Work focused in particular on the verification of a Stateflow/Simulink model for the STARMAC Quadrotor controller. Faults were injected into the model as missing sensors’ readings. Fault occurrence and duration were modeled by a Poisson process and by an exponential distribution, respectively. We verified PBLTL properties of the Quadrotor, e.g. “with probability at least 0.99, over the next 200 seconds it is never the case that the Quadrotor strays from the target path more than *threshold* for more than 10 seconds”, where *threshold* can be chosen to test different levels of design strength. Our initial findings confirm that statistical model checking can be effectively applied for the verification of real-world embedded systems.

## Verification of Hybrid Systems via Differential Invariants

André Platzer has written a book about hybrid systems verification that will appear with Springer as "Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics." This book describes basic and advanced verification techniques for hybrid systems, including applications to air traffic control analysis. It will be a good introduction for graduate students working in the area.

# Publications

1. Paolo Zuliani, André Platzer, Edmund M. Clarke: Bayesian Statistical Model Checking with Application to Stateflow/Simulink Verification . HSCC 2010: 243-252.
2. Himanshu Jain, Edmund M. Clarke: Efficient SAT solving for non-clausal formulas using DPLL, graphs, and watched cuts. DAC 2009: 563-568.
3. Edmund M. Clarke, E. Allen Emerson, Joseph Sifakis: Model checking: algorithmic verification and debugging. Commun. ACM 52(11): 74-84 (2009).
4. Himanshu Jain, Edmund M. Clarke, Orna Grumberg: Efficient Craig interpolation for linear Diophantine (dis)equations and linear modular equations. Formal Methods in System Design 35(1): 6-39 (2009).
5. André Platzer, Edmund M. Clarke: Computing Differential Invariants of Hybrid Systems as Fixedpoints. Formal Methods in System Design, 35(1): 98-120 (2009).
6. Edmund M. Clarke, Alexandre Donzé, Axel Legay: On simulation-based probabilistic model checking of mixed-analog circuits. Formal Methods in System Design, *to appear*.
7. Yu-Fang Chen, Azadeh Farzan, Edmund M. Clarke, Yih-Kuen Tsay, Bow-Yaw Wang: Learning Minimal Separating DFA's for Compositional Verification. TACAS 2009: 31-45.
8. André Platzer, Edmund M. Clarke: Computing Differential Invariants of Hybrid Systems as Fixedpoints. CAV 2008: 176-189.
9. Himanshu Jain, Daniel Kroening, Natasha Sharygina, Edmund M. Clarke: Word-Level Predicate-Abstraction and Refinement Techniques for Verifying RTL Verilog. IEEE Trans. on CAD of Integrated Circuits and Systems 27(2): 366-379 (2008).

# Honors and Awards

1. 2010 LICS Test-of-time Award – Edmund M. Clarke. July 2010, Edinburgh, UK.
2. Best Paper Award - André Platzer and Edmund M. Clarke: Formal Verification of Curved Flight Collision Avoidance Maneuvers: A Case Study. FM 2009, 547-562.
3. Best Paper Award – Edmund M. Clarke, Alexandre Donzé, Axel Legay: Statistical Model Checking of Mixed-Analog Circuits with an Application to a Third Order Delta-Sigma Modulator. Haifa Verification Conference, October 27-30, 2008, Haifa, Israel.
4. Strachey Lecture – Edmund M. Clarke. My 27-year Quest to Overcome the State Explosion Problem. Oxford University Computing Laboratory, May 12,2009, Oxford, UK.
5. Technion CS Distinguished Lectures – Edmund M. Clarke. Technion - Israel Institute of Technology, May 17-26, 2009, Haifa, Israel.
6. Keynote Speaker – Edmund M. Clarke.
   1. Model Checking – My 27-year Quest to Overcome the State Explosion Problem. NASA Formal Methods Symposium, April 6-8, 2009, Moffett Field, CA.
   2. Model Checking - My 27-Year Quest to Overcome the State Explosion Problem. LPAR 2008, November 22-27, 2008, Doha, Qatar.
   3. BMC: Before Model Checking. CAV 2008, July 7-14, 2008, Princeton, NJ.
   4. Model Checking. DAC 2008, June 8-13, 2008, Anaheim, CA.
   5. U.S. Department of Defense Workshop on Satisfiability, March 3-5, 2009, Baltimore, MD.

# Personnel

Supported:

1. Edmund M. Clarke, Professor, Computer Science Dept., CMU
2. Alexandre Donzé, Post Doc, Computer Science Dept., CMU

Associated but not supported:

1. Anvesh Komuravelli, PhD student, Computer Science Dept., CMU
2. André Platzer, Professor, Computer Science Dept., CMU
3. Axel Legay, Post Doc, Computer Science Dept., CMU
4. Azadeh Farzan, Post Doc, Computer Science Dept., CMU
5. Himanshu Jain, PhD candidate, Computer Science Dept., CMU
6. Paolo Zuliani, Post Doc, Computer Science Dept., CMU