Performance Analysis of Systems and Software using a Theorem Prover

Osman Hasan and Sofiène Tahar

Department of Electrical and Computer Engineering, Concordia University
1455 de Maisonneuve W., Montreal, Quebec, H3G 1M8 Canada
Email: {o_hasan, tahar}@ece.concordia.ca
Web: http://hvg.ece.concordia.ca

Abstract

Nowadays, computer simulation is one of the most widely used performance analysis technique. However, simulation based analysis usually provides approximate results due to its inherent nature and it cannot handle large-scale problems due to its enormous CPU time requirements. The unreliability of the results poses a serious problem in safety critical applications, such as those in space travel, military, and medicine, where a mismatch between the predicted and the actual system performance may result in either inefficient usage of the available resources or by unnecessarily paying higher costs to meet some performance or reliability criteria. A possible solution for overcoming these limitations is to conduct performance analysis within the environment of a higher-order-logic theorem prover. Higher-order logic is a system of deduction with a precise semantics and can be used for the development of almost all classical mathematical theories. Whereas, interactive theorem proving is the field of computer science and mathematical logic concerned with computer based formal proof tools that require some sort of human assistance. Due to the high expressiveness of the higher-order-logic and the inherent soundness of interactive theorem proving, this approach can be used to conduct error free performance analysis at the cost of significant user interaction.

There has been some fruitful developments in this emerging area and a preliminary infrastructure has been proposed that allows the formalization of random variables in higher-order-logic and the formal verification their useful probabilistic and statistical properties within the theorem prover. The main focus of the tutorial is to introduce this new area of research and present its practical effectiveness for conducting precise performance analysis of real world system and software examples.

The tutorial begins by presenting a comprehensive introduction to formal methods and their usefulness in the system design process. It is followed by an overview of the HOL theorem prover, which is the higher-order-logic theorem prover that we have used in this project. Next, we present the process of formalizing (or modeling) random variables and verifying their correctness by proving the corresponding probabilistic and statistical properties, such as mean and variance, in HOL. These formalized random variables can be used to model the uncertainties and random elements found in a system and thus allow us to reason about its performance issues in HOL. For illustration purposes, we present the performance analysis of two examples. Firstly, we verify the average number of trials required for the Coupon Collector's problem, which is a well known commercially used algorithm. Next, we verify the average delay relations for three commonly used Automated Repeat Request (ARQ) protocols, i.e., Stop-and-Wait, Go-Back-N and Selective-Repeat using the HOL theorem prover.

Tutorial Duration: Half Day

Outline

- Introduction to Formal Methods [9]
- HOL Theorem Prover [1]
- Formalization and Verification of Random Variables in HOL [8, 3, 2]
- Verification of Probabilistic and Statistical Properties in HOL [5, 4, 6, 7]
- Performance Analysis of Coupon Collector's Problem
- Performance Analysis of ARQ Protocols

References

[1] J. Harrison, K. Slind, and R. Arthan. HOL. In *The Seventeen Provers of the World*, volume 3600 of *LNCS*, pages 11–19. Springer, 2006.

[2] O. Hasan and S. Tahar. Formalization of the Continuous Probability Distributions. In *Conference on Automated Deduction*, volume 4603 of *LNAI*, pages 3–18. Springer, 2007.

[3] O. Hasan and S. Tahar. Formalization of the Standard Uniform Random Variable. *Theoretical Computer Science*, 382(1):71–83, 2007.

[4] O. Hasan and S. Tahar. Verification of Expectation Properties for Discrete Random Variables in HOL. In *Theorem Proving in Higher-Order Logics*, volume 4732 of *LNCS*, pages 119–134. Springer, 2007.

[5] O. Hasan and S. Tahar. Verification of Probabilistic Properties in HOL using the Cumulative Distribution Function. In *Integrated Formal Methods*, volume 4591 of *LNCS*, pages 333–352. Springer, 2007.

[6] O. Hasan and S. Tahar. Verification of Tail Distribution Bounds in a Theorem Prover. In *Numerical Analysis and Applied Mathematics*, volume 936, pages 259–262. American Institute of Physics, 2007.

[7] O. Hasan and S. Tahar. Formal Verification of Expectation and Variance for Discrete Random Variables. Technical Report, Concordia University, Montreal, Canada, June 2007; http://hvg.ece.concordia.ca/Publications/TECH_REP/FVEVDR_TR07.

[8] J. Hurd. *Formal Verification of Probabilistic Algorithms*. PhD Thesis, University of Cambridge, Cambridge, UK, 2002.

[9] M.Huth and M.Ryan. *Logic in Computer Science. Modelling and Reasoning about Systems*. Cambridge University Press, 2004.