*The Department of Electrical & Computer Engineering*
*The University of Auckland*
*New Zealand*

# Automated Techniques for Formal Verification of SoCs

*Roopak Sinha*

*February 2009*

*Supervisors: Partha S Roop*

A thesis submitted in partial fulfillment of the requirements of Doctor of Philosophy in Engineering

# Abstract

System-on-a-chip (SoC) designs have gained immense popularity as they provide designers with the ability of integrating all components (called IPs) of an application-specific computer system onto a single chip. However, one of the main bottlenecks of the SoC design cycle is the validation of complex designs. As system size grows, validation time increases beyond manageable limits. It is desirable that design inconsistences are found and fixed early in the design process, as validation overheads are significantly higher after IPs are integrated. This thesis presents a range of techniques for the automatic verification and design of SoCs that aim to reduce post-integration validation costs.

Firstly, *local module checking* algorithm, a practical implementation of module checking, is presented. This technique allows for the comprehensive verification of IPs such that they guarantee the satisfaction of critical specifications regardless of the SoC they are used in. Local module checking is shown to be able to validate IPs in much lesser time on average than global module checking, and can help in handling many important validation tasks much before the integration stage.

Next, a number of *protocol conversion* techniques that assist in the composition of IPs with incompatible protocols is presented. The inconsistencies between IP protocols, called mismatches, are bridged by the automatic generation of some extra glue-logic, called a converter. Converters generated by the proposed techniques can handle control, data-width and clock mismatches between multiple IPs in a unified manner. These approaches ensure that the integration of IPs is *correct-by-construction*, such that the final system is guaranteed to satisfy key specifications without the need for further validation.

Finally, a technique for automatic IP reuse using *forced simulation* is presented, which involves automatically generating an *adaptor* that guides an IP such that it satisfies desired specifications. The proposed technique can generate adaptors in many cases where existing IP techniques fail. As it is guaranteed that reused IPs satisfy desired specifications, post-integration validation costs are significantly reduced.

For each proposed technique, a comprehensive set of results is presented that highlights the significance of the solution. It is noted that the proposed approaches can help automate SoC design and achieve significant savings in post-integration validation costs.

# List of Publications

The following is a list of research articles that are based on the techniques presented in this thesis:

1. Roopak Sinha, Partha S. Roop and Bakhadyr Khoussainov. Adaptive Verification using Forced Simulation. *Electrical Notes in Theoretical Computer Science*, 141(3):171-197, 2005. *(This article was originally presented at "Formal Foundations of Embedded Software and Component-Based Software Architectures (FESCA)", 2005.)*

2. Samik Basu, Partha S. Roop and Roopak Sinha. Local Module Checking for CTL Specifications. *Electrical Notes in Theoretical Computer Science*, 176(2):125-141, 2007. *(A shorter version of this article was presented at "Formal Foundations of Embedded Software and Component-Based Software Architectures (FESCA)", 2006.)* **Received the best paper award at FESCA 2006**.

3. Roopak Sinha, Partha S. Roop and Samik Basu. A Model Checking Approach to Protocol Conversion. *Electrical Notes in Theoretical Computer Science*. 203(4):81-94, 2008. *(A shorter version of this paper was presented at "Model-driven High-level Programming of Embedded Systems (SLA++P)", 2007.)*

4. Roopak Sinha, Partha S. Roop, Samik Basu and Zoran Salcic. A Module Checking Based Converter Synthesis Approach for SoCs. In *VLSID '08: Proceedings of the 21st International Conference on VLSI Design*, pages 492-501, Hyerabad, India, 2008. IEEE Computer Society

5. Roopak Sinha, Partha S. Roop, and Samik Basu. SoC Design Approach using Convertibility Verification. *EURASIP Journal on Embedded Systems, Special Issue on "Model-driven High-level Programming of Embedded Systems. Selected papers from Sla++p'07 and Sla++p'08"*. (accepted for publication)

6. Roopak Sinha, Partha S. Roop, Samik Basu and Zoran Salcic. Multi-Clock SoC Design using Protocol Conversion. Design, Automation and Test in Europe (DATE) 2009. (accepted for publication).

# Acknowledgements

I would like to acknowledge the following individuals with whom I have had the privilege of collaborating to develop the ideas presented in this thesis.

- **Dr. Partha S Roop**: Not only my supervisor, but also a great friend and guide. His contributions towards the completion of thesis, which were not only academic, are invaluable and deeply appreciated.
- **Prof. Samik Basu**: Our collaboration with him started with the module checking problem which has been instrumental in the subsequent formulation of the various protocol conversion techniques presented in this thesis.
- **Prof. Zoran Salcic**: His input has been essential in guiding the work presented in this thesis towards SoC design and verification.
- **Prof. Bakhadyr Khoussainov**: His help towards the development of forced simulation based IP reuse is much appreciated.
- **Li Hsien Yoong, Alif Wahid, Sidhartha Andalam and Simon Yuan**: My lab mates who provided a motivating environment for research and fun.

I would also like to thank my family, especially my wife **Arpita**, without whose help, support and understanding, this thesis would not have been completed.