RELATIVE TIMING BASED VERIFICATION OF CONCURRENT SYSTEMS

MARCO ANTONIO PEÑA BASURTO
Llicenciat en Informàtica, Technical University of Catalonia, Barcelona, Spain 1993
Llicenciat amb grau en Informàtica, Technical University of Catalonia, Barcelona, Spain 1995

Department of Computer Architecture
Technical University of Catalonia
Barcelona (Spain), February, 2003

A thesis submitted in partial fulfillment of the requirements for the degree of Doctor en Informàtica

To Nuria and Pau

Para mi no hay emoción comparable a la que produce la actividad creadora, tanto en ciencia como en arte, literatura u otras ocupaciones del intelecto humano. Mi mensaje, dirigido sobre todo a la juventud, es que si sienten inclinación por la ciencia, la sigan, pues no dejará de proporcionarles satisfacciones inigualables. Cierto es que abundan los momentos de desaliento y frustración, pero éstos se olvidan pronto, mientras que las satisfacciones no se olvidan jamás.

—Severo Ochoa

It has long been my personal view that the separation of practical and theoretical work is artificial and injurious. Much of the practical work done in computing, both in software and hardware design, is unsound and clumsy because the people who do it do not have any clear understanding of the fundamental principles underlying their work. Most of the abstract mathematics and theoretical work is sterile because it has no contact with the real computing.

—Christopher Strachey

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

The thesis presents a new theory and methodology for the formal verification of safety properties in timed systems. The correct operation of such systems not only depends on a set of functional properties but also on certain assumptions about the delays of the components of the system and the response times of the environment in which the system operates. The verification of this type of systems typically involves several computationally hard problems. In particular, the combinatorial state explosion problem becomes exacerbated by the time dimension.

The theory that supports the proposed verification approach extends the conventional BDD-based symbolic methods to the verification of timed systems, modeled by means of *timed transition systems*. The theory is based on the *relative timing* paradigm, which instead of considering exact time differences in the occurrence of events, considers the effect of delays in terms of relative orderings between events. For example, in order to guarantee that a *race* is not propagated in a digital circuit, it is often sufficient to check that certain signal switches before another, instead of identifying the exact instants of time in which both signals switch. Moreover, the timing information does not need to computed for the overall system, but only *locally* for the part of the system involved in the proof or disproof of a given property. This is possible thanks to a crucial observation, that the set of executions of a transition system can be covered by a set of partial orders. As a consequence, only a subset of the events of the system is involved in the proof of a property and the timing analysis can be carried out very efficiently.

Conventional methods for the verification of timed systems rely on the computation of the exact timed state space of the system as the first step of the analysis. Although efficient techniques have been devised to overcome the complexity issue (*e.g.* difference bound matrices), symbolic methods cannot be easily applied. Thus, the combinatorial time-state explosion problem often limits the applicability of such methods to moderate-size systems.

Instead, the approach proposed in the thesis relies on an incremental refinement of the untimed state space of the system, so that timing information is incorporated as soon as it is needed. The timing information is derived by an efficient *off-line* timing analysis over small sets of events. The refined state space is captured under the model of *lazy transition*

system, which allows an efficient representation of the timed domain using conventional symbolic methods. As a consequence, the approach can be potentially applied to bigger systems or to systems with more level of detail, than those that can be handled by similar methods for the verification of timed systems. Moreover, the incremental nature of the approach provides a good way to obtain at least partial results even on systems for which complete solutions could be too complex to compute.

A key feature of the proposed verification approach is that not only proves or disproves the correctness of a timed system. If the system is correct the set of relative timing relations used for the proof are provided. Such relations constitute a set of sufficient timing constraints that guarantee the correctness of the system. On the other hand, if the system is incorrect, a counterexample failure trace is provided. The most important aspect of all this feedback is that it can be used as valuable *back-annotation* information along the design process. This feature, which allows to bridge the gap between verification and design, constitutes another differential aspect of our verification approach when compared to other equivalent verification methods.

The verification approach has been fully implemented in an experimental CAV tool called TRANSYT. The tool can handle hierarchical and distributed modular systems which can inter-operate by a variety of communication mechanisms. TRANSYT has successfully proved its functionality as well as the validity of the overall verification approach, by verifying a number of timed asynchronous circuits with up to more than 10^6 untimed states. The experiments cover, for example, the verification of: complex-gate decompositions in quasi-speed-independent asynchronous circuits, delay-reset domino circuits, pulse-based systems, circuits optimized for speed using timing assumptions, etc. Additionally, compositional verification methods have been combined with the basic verification approach in order to tackle the size/complexity issues involved in the verification of complex timed systems. Thus, abstractions, assume-guarantee reasoning and mathematical induction have been used to prove the correctness the IPCMOS architecture. It is a scalable pipelined architecture which is aimed to the interconnection of different clock zones in a system.

Thanks to the rather theoretical nature of the proposed verification approach, its potential applicability covers a wider range of systems than those cited above, such as: custom transistor-level circuits that exploit the technology limits for performance, complex digital structures where synchronization is a crucial issue (*e.g.* dynamic MOS), asynchronous and GALS-type systems, real-time systems, etc.

ACKNOWLEDGMENTS

If I have seen further than others, it is because I was standing upon the shoulders of giants.

—Isaac Newton - Letter to a friend, 1676

The first person that deserves my acknowledgment is my supervisor Jordi Cortadella. He introduced me to the world of asynchronous circuits, Petri nets, formal verification, etc. back in 1993 when I was still an undergraduate student. His deep insight into the subject of this thesis provided me a lot of helpful suggestions. Without his guidance and kind encouragement this thesis would have never been possible.

I am specially indebted to my other supervisor, Enric Pastor. His continuous support and friendship have helped me to overcome the (technical and personal) difficulties during the critical phases of this work.

My gratitude also to Alex Kondratyev and Alexander Smirnov for their contributions to the theoretical soundness and the practical implementation of this work, respectively. And to Luciano Lavagno, Alex Yakovlev and Alexander Taubin, for their kindness hosting me in respective visits to the *Politecnico di Torino*, the University of Newcastle and the University of Aizu. The numerous insightful discussions with them about different research topics have contributed this thesis in a number of ways.

Thanks to the other members of the CAD/VLSI group at the Department of Computer Architecture of the Technical University of Catalonia —Rosa Badia, Fermín Sánchez and Josep Carmona— and former members —Oriol Roig and Enric Musoll. Along these years they have provided me with the kind of environment that makes work a much more pleasant experience.

Thanks also to the reviewers at Department of Computer Architecture —Rosa Badia, Antonio González and Antonio Juan Hormigo— and the external reviewers —Abelardo Pardo and Supratik Chakraborty. They read carefully the preliminary versions of this thesis giving me valuable suggestions on the contents and the presentation of this work. And the members of the thesis committee for the effort they put into judging this thesis.

On the institutional and industry side I would like to acknowledge: the Ministry of Science and Technology of Spain under contracts CICYT-TIC 95-0419, CICYT-TIC 98-0410-CO-01 and CICYT-TIC 2001-2476-CO-03; the ACiD Working Group under contracts ESPRIT-7225, ESPRIT-21949 and IST-1999-29119; and Intel Corporation. They all are gratefully acknowledged for funding this research.

On the personal side my family deserves infinite gratitude: my father Antonio, my mother Adoración and my brother Jose. Thanks a lot for your efforts on infusing me the values of a good education and supporting all my studies along the years.

And the most effusive thanks to Nuria. During all this time she has been my best friend, providing lots of emotional support and love, and patiently suffering the numerous moments of solitude she has been forced to because of my work. This thesis is dedicated to her and our beloved son Pau.

Finally I would like to express my thanks to everyone I have not cited above but has helped me, directly or not, in the long way until this thesis has been completed. Thanks a lot to you all.