

Verification of Embedded Systems using a Petri Net based Representation

Luis Alejandro Cortés, Petru Eles, and Zebo Peng
Dept. of Computer and Information Science
Linköping University, Linköping, Sweden
{luico,petel,zebpe}@ida.liu.se
<http://www.ida.liu.se/~luico/>

Embedded systems are typically constituted of application-specific hardware components and software running on programmable platforms. The inherent heterogeneity of this kind of systems makes them very complex and consequently difficult to verify. Moreover, the increasing demand on high-performance products has boosted the levels of sophistication of such systems. For the levels of complexity typical to modern electronic systems, traditional validation techniques like simulation and testing are neither sufficient nor viable to verify their correctness. Formal methods are becoming a practical alternative to ensure the correctness of designs. They might overcome some of the limitations of traditional validation methods. At the same time, formal verification can give a better understanding of the system behavior, contributes to uncover ambiguities, and reveals new insights of the system.

The contributions of this work are two fold: first, we formally define the semantics of PRES+, a Petri net based computational model aimed to represent embedded systems; second, we introduce an approach to formal verification of embedded systems by using model checking and we propose a systematic procedure to translate PRES+ models into timed automata in order to make use of existing model checking tools.

PRES+ (Petri net based Representation for Embedded Systems) is a computational model based on Petri nets that allows to capture important features of embedded systems. When used to model embedded systems, the representation we introduce has several interesting characteristics: non-determinism may be naturally represented by PRES+; parallel or concurrent activities may be easily expressed in terms of Petri nets; in our model tokens carry information, thus PRES+ overcomes the lack of expressiveness of classical Petri nets where tokens are considered as “black dots”; our model captures timing aspects by associating lower and upper limits to the duration of activities related to transitions and keeping time information in token stamps.

Formal methods have been extensively used in software development and hardware verification. However, they are not commonplace in embedded systems design. In this work we present an approach to verification using model checking for embedded systems represented in PRES+. Model checking is an approach to formal verification that lets the designer prove whether certain design properties hold in a given model of the system. Our approach allows to determine the truth of CTL (Computation Tree Logic) and TCTL (Timed CTL) formulas with respect to a PRES+ model. In order to use existing model checking tools, we introduce a systematic procedure to translate PRES+ models into timed automata. This method can be automated in a relatively simple manner.

We study an ATM server modeled in PRES+ in order to illustrate the feasibility of our approach on practical applications. This example shows that our work is not only appropriate to verify the correctness of embedded systems, but may also be a useful tool for design space exploration.