Dissertationen

Dirk Beyer: **Formale Verifikation von Realzeit-Systemen mittels Cottbus Timed Automata**

Promotion: Brandenburgische Technische Universität Cottbus
Erstgutachter: Prof. Dr. Claus Lewerentz, Brandenburgische TU Cottbus
Zweitgutachter: Prof. Dr.-Ing. Monika Heiner, Brandenburgische TU Cottbus
Drittgutachter: Prof. Dr. Werner Damm, Universität Oldenburg
Datum der Prüfung: 26. November 2002
Veröffentlichung: Berlin: Verlag Mensch & Buch, 2002. Zugl.: http://www.ub.tu-cottbus.de/hss/diss/fak1/beyer_d; Cottbus, Univ., Diss., 2002. ISBN: 3-89820-450-2

Kurzfassung:

Over the last decade the formalism of timed automata has become more and more important in the field of modeling and verification of real-time systems. However, its application leads to the following main problems which were solved in the thesis:

- Large systems can be modeled only in a complicated and unstructured manner. The model consists of a collection of automata which communicate only on one level. It is not possible to model recurrent parts of the system in a reusable way, they have to be defined as often as needed.
- The algorithmic verification is possible only for small models because of enormous consumption of time and memory (state-space explosion).

The modeling formalism **Cottbus Timed Automata** (CTA), which is introduced in the thesis, extends the existing concepts of timed automata by means of **modularity**. The behavior of a CTA model is defined by mapping it onto timed automata. Because of the ability of hierarchical structuring with modules and the mechanism of instantiation for recurrent use of previously defined modules even large systems can be modeled.

For the verification of CTA models an **efficient BDD-based reachability analysis** is introduced which outperforms the existing verification tools for timed automata. One key to this improvement is to use the modular structure of the model for the computation of good BDD variable orderings. Additionally, **refinement checking** is defined and implemented, which is also based on the efficient BDD representation. This makes it possible to verify large models which are intractable for pure model checking.

Timed automata are not sufficiently expressive to model all aspects of a **hybrid system**. Therefore the CTA formalism is extended from timed to hybrid automata. To integrate the verification of hybrid models into the tool, a representation of the model on the basis of the double description method, which is a matrix-based data structure for convex polyhedra, is implemented.

The theoretical concepts introduced in the first part of the thesis were implemented in the tool **Rabbit**. The architecture principle is flexibility: not only parts of the tool can be easily and flexibly extended or changed, but also the whole data structure for the representation of the model can be chosen at run-time. Therefore, the tool can serve as verification framework for various (future) data structures for representation, when new ideas about data structures and algorithms have to be empirically evaluated. For a lot of example models it has been shown that the tool Rabbit is more efficient than the existing tools.

Finally, the thesis reports results of a **case study for modeling and verification** of a large, realistic system: a production cell with 44 sensors and 28 motors. The procedure of modeling is explained and the hierarchical structure is sketched out. Properties of the system are specified and verified. With the help of modular proof principles, properties of the system were verified not only for small parts of the model, but also carried over to the whole system.

Conclusion: Contradicting the occasionally expressed opinion that the technology of model checking has reached its limitations, this thesis has shown that models of large size can be verified. The key idea is the use of **structure**: a modeling formalism is introduced to provide the expressiveness to reflect the explicit structure of components and its communication in the model in a quite natural way. The structural modeling allows the construction of models which are understandable, easy to use and easy to adopt. Furthermore, this structure is used to improve the performance of the verification task. The BDD implementation reduces the size complexity of the representation of configuration sets by using a structure-oriented variable ordering. This allows efficient reachability analysis of large models. The refinement analysis supports the application of compositional proof techniques. The modular structure of the model does lead to refinement structures which are not artificially created, but they are compatible to the natural structure of the system and therefore they can be used as abstractions in modular proofs.