Data Structures for Real-Time Verification

Description du projet

Context

This project is related to the *Action de recherche collaborative* (TP)I: (Timed / Probabilistic) Interfaces [13] and the *ADT* ETI: ECDAR for Timed Interfaces. It is conducted within the context of the *Action exploratoire* ESTASE and the INRIA team DISTRIBCOM [16].

Background

Model checking [6] comprises methods and tools for the analysis and verification of complex software systems. The goal of model checking is to provide a comprehensive analysis of a software system, with the intention of mathematically proving the system to behave as intended. Contrary to testing, model checking is thus capable of detecting *all* bugs of a system. To this end, the user provides a comprehensive formal model of the software system and a set of formal properties the system has to satisfy, and then the model checker can detect whether or not the system obeys the properties.

The subject of model checking within theoretical computer science is quite mature. Many powerful tools for model checking exist [22, 23, 25, 26] and are routinely used by industry.

Real-time model checking [2] is an extension of model-checking formalisms to also encompass properties related to *timing constraints*. In contrast, classical model checking as described above can only handle and infer *logical* properties, *ie* whether or not an action will occur, and in which order actions happen, but not precisely *when*.

Also the subject of real-time model checking within theoretical computer science is well-established, with several powerful tools in existence [17, 19, 24, 28]. The world leader in this domain is the tool UPPAAL [4] which has been developed jointly at Uppsala University, Sweden, and Aalborg University, Denmark, and is now actively maintained in Aalborg.

Interface theories [7] are an extension of the model checking formalism to allow for *incremental* verification and design. The central idea is that there is no fixed comprehensive model of the whole system, but rather parts of the system are modeled independently (even by independent teams) and incrementally verified and combined into bigger parts. The subject of the *ADT* ETI is *real-time interface theories* using the ECDAR toolset [18] which currently is based on an extension of UPPAAL. ECDAR is maintained jointly in Aalborg and at INRIA Rennes.

Data structures

Real-time model checking is implemented using symbolic states consisting of so-called *zones* [2]. Hence instead of having to keep track of precise timing information, this information is abstracted into zones, which geometrically are a very specific kind of convex polyhedra. Internally in tools like UPPAAL, zones are represented using so-called *difference-bound matrices* (DBMs) [10] and other data structures.

Data structures for real-time verification is a very active research area, as there are a number of problems with DBMs which hinder application of tools like UPPAAL and ECDAR. One such problem is that DBMs are not closed under union and complement: in symbolic real-time model checking, one generally wishes to lump symbolic states together to combat state-space explosion, but using DBMs, this is not possible.

As the current state-of-the-art, other data structures such as *clock difference diagrams* (CDDs) [5] are used for representing unions of zones, but these again have the problem that one cannot efficiently perform symbolic analysis using CDDs, hence costly conversion between CDDs and DBMs is necessary. Another problem, specific and central for the ECDAR tool, is that reuse of components is impossible using current data structures. New data structures for real-time model checking are thus called for.

One promising such data structure is the one of *convex max-plus polyhedra*, [1] which are the analogues of convex polyhedra in the algebra over the max-plus semiring (which consists of the real numbers together with maximum and addition as operations). Recent research [8, 11] shows that convex max-plus polyhedra can efficiently represent zones and also some unions of zones, and that real-time model checking using convex max-plus polyhedra is feasible.

There are other data structures for real-time model checking which have been proposed, [3, 9, 12] and through development of new tools (such as ECDAR) and formalisms (*e.g.* statistical model checking), new demands on these data structures continuously arise. Hence research on data structures for real-time model checking is a continuous interplay between the high-level needs of real-time verification and the low-level details of the tools.

Impact

The successful development and implementation of new data structures for real-time model checking can lead to a dramatic increase in the usefulness of tools such as UPPAAL or ECDAR. The current implementation of ECDAR suffers from state-space explosion and other fundamental problems which new data structures can solve.

Cooperation

For research in max-plus polyhedra, there is a strong group at INRIA Saclay and Ecole Polytechnique (the MAXPLUS joint team [20] headed by Stephane Gaubert) and at CEA Saclay (the MeASI team [21] at CEA LIST headed by Eric Goubault), with which we will cooperate. They have expertise which we will need to gain a geometric understanding of operations on zones and max-plus polyhedra which then can be translated into algorithms.

For research in data structures and algorithms for real-time verification in general, there is a strong group at VERIMAG (the DCS team [14] headed by Yassine Lakhnech and the TEMPO team [27] headed by Oded Maler) in Grenoble. They will be interested in cooperation on implementing our new data structures in their tools and in ECDAR.

For international cooperation, there is a strong group at Aalborg University, Denmark (the DES team [15] headed by Kim G. Larsen) which conducts research into data structures and algorithms for real-time model checking, and which maintains the tool UPPAAL.

References

[1] Xavier Allamigeon, Stephane Gaubert, and Eric Goubault. Inferring min and max invariants using max-plus polyhedra. In María Alpuente and Germán Vidal, editors,

SAS, volume 5079 of *Lecture Notes in Computer Science*, pages 189–204. Springer, 2008.

[2] Rajeev Alur and David L. Dill. A theory of timed automata. *Theor. Comput. Sci.*, 126(2):183–235, 1994.

[3] Eugene Asarin, Marius Bozga, Alain Kerbrat, Oded Maler, Amir Pnueli, and Anne Rasse. Data-structures for the verification of timed automata. In Oded Maler, editor, *HART*, volume 1201 of *Lecture Notes in Computer Science*, pages 346–360. Springer, 1997.

[4] Gerd Behrmann, Alexandre David, Kim Guldstrand Larsen, John Håkansson, Paul Pettersson, Wang Yi, and Martijn Hendriks. UPPAAL 4.0. In *QEST*, pages 125–126. IEEE Computer Society, 2006.

[5] Gerd Behrmann, Kim Guldstrand Larsen, Justin Pearson, Carsten Weise, and Wang Yi. Efficient timed reachability analysis using clock difference diagrams. In Nicolas Halbwachs and Doron Peled, editors, *CAV*, volume 1633 of *Lecture Notes in Computer Science*, pages 341–353. Springer, 1999.

[6] Edmund M. Clarke, E. Allen Emerson, and Joseph Sifakis. Model checking: algorithmic verification and debugging. *Commun. ACM*, 52(11):74–84, 2009.

[7] Luca de Alfaro and Thomas A. Henzinger. Interface theories for component-based design. In Thomas A. Henzinger and Christoph M. Kirsch, editors, *EMSOFT*, volume 2211 of *Lecture Notes in Computer Science*, pages 148–165. Springer, 2001.

[8] Jesper Dyhrberg, Qi Lu, Michael Madsen, Søren Ravn, and Uli Fahrenberg. Computations on zones using max-plus algebra. In *Proc. 22nd Nordic Workshop in Programming Theory (NWPT'10)*, 2010.

[9] Rüdiger Ehlers, Daniel Fass, Michael Gerke, and Hans-Jörg Peter. Fully symbolic timed model checking using constraint matrix diagrams. *Real-Time Systems Symposium, IEEE International*, pages 360–371, 2010.

[10] Thomas A. Henzinger, Xavier Nicollin, Joseph Sifakis, and Sergio Yovine. Symbolic model checking for real-time systems. *Inf. Comput.*, 111(2):193–244, 1994.

[11] Qi Lu, Michael Madsen, Martin Milata, Søren Ravn, Uli Fahrenberg, and Kim G. Larsen. Reachability analysis for timed automata using max-plus algebra. 2011. Submitted.

[12] Jesper B. Møller, Jakob Lichtenberg, Henrik Reif Andersen, and Henrik Hulgaard. Difference decision diagrams. In Jörg Flum and Mario Rodríguez-Artalejo, editors, *CSL*, volume 1683 of *Lecture Notes in Computer Science*, pages 111–125. Springer, 1999.

[13] ARC (TP)I. `http://arctpi.inria.fr/`.

[14] DCS. `http://www-verimag.imag.fr/DCS,31.html`.

[15] DES. `http://www.cs.aau.dk/en/research/des/`.

[16] DISTRIBCOM. `http://www.irisa.fr/distribcom/`.

[17] DREAM. `http://dre.sourceforge.net/`.

[18] ECDAR. `http://ecdar.cs.aau.dk`.

[19] IF. http://www-verimag.imag.fr/~async/IF/.

[20] MAXPLUS. http://www.cmap.polytechnique.fr/spip.php?rubrique103.

[21] MeASI LIST. http://www-list.cea.fr/.

[22] NuSMV. http://nusmv.fbk.eu/.

[23] PAT. http://www.comp.nus.edu.sg/~pat/.

[24] Roméo. http://romeo.rts-software.org/.

[25] SPIN. http://spinroot.com/.

[26] TAPAs. http://rap.dsi.unifi.it/tapas/.

[27] Tempo. http://www-verimag.imag.fr/Tempo,32.html.

[28] UPPAAL. http://www.uppaal.org/.