Static Analysis for Hybrid Automata without Widening
Internship Proposal

Thao Dang[1] and Thomas Martin Gawlitza[1]

VERIMAG {Thao.Dang,Thomas.Gawlitza}@imag.fr ⋆

Location and Context. Laboratory VERIMAG in Grenoble (http://www-verimag.imag.fr/) or INRIA-Grenoble (http://www.inria.fr/centre-de-recherche-inria/grenoble-rhone-alpes).
The internship is connected to the ANR research project VEDECY (http://sites.google.com/site/vedecy/home).

1 Description of the topic

A *hybrid automaton* describes a *computer program* together with its analog environment and is a well-established mathematical model for describing cyber-physical systems. A hybrid automaton consists of a finite number of states, some transition rules which describe the transitions between states, and a bunch of differential equations describing the behavior of the analog environment. The goal of the proposed internship is to develop an *analyzer* for *affine* hybrid automata that aims at proving safety properties, i.e. proving that a given automaton cannot go into an *error state*. For that we will use novel approaches that are based on *strategy iteration*.

Strategy iteration (also called *policy iteration*) was introduced by Howard for solving *stochastic control problems* [16, 19] and is also applied to *two-players zero-sum games* [15, 18, 22] or min-max-plus systems [2]. Applied to static analysis problems, the goal of such a strategy iteration algorithm is to compute the *least solution* of a system of inequalities

$$\begin{array}{ccc} \mathbf{x}_1 \geq f_{1,1}(\mathbf{x}_1,\ldots,\mathbf{x}_n) & \cdots & \mathbf{x}_1 \geq f_{1,k_1}(\mathbf{x}_1,\ldots,\mathbf{x}_n) \\ \vdots & \vdots & \vdots \\ \mathbf{x}_n \geq f_{n,k_n}(\mathbf{x}_1,\ldots,\mathbf{x}_n) & \cdots & \mathbf{x}_1 \geq f_{1,k_1}(\mathbf{x}_1,\ldots,\mathbf{x}_n), \end{array}$$

where $\mathbf{x}_1,\ldots,\mathbf{x}_n$ are variables that take values in $\overline{\mathbb{R}} := \mathbb{R} \cup \{-\infty,\infty\}$ and the $f_{i,j}$'s are operators that are monotone and concave. The existence of the least solution is ensured by the fixpoint theorem of Knaster/Tarski [21]. An extremely simple example is given by the following system of inequalities:

$$\begin{array}{ll} \mathbf{x}_1 \geq 0 & \mathbf{x}_1 \geq \frac{1}{2}\mathbf{x}_1 + \mathbf{x}_2 \\ \mathbf{x}_2 \geq 3 & \mathbf{x}_2 \geq \min\{\mathbf{x}_2 + 1,\ 10\} \end{array}$$

Observe that the least solution of the above system of inequalities is $\mathbf{x}_1 = 20$, $\mathbf{x}_2 = 10$.

In order to solve such systems of inequalities using strategy iteration, one considers them as a game between two players. One player aims at maximizing the value and the other player aims at minimizing it. The behavior of the minimizer is described through a so-called *min-strategy*. Accordingly, the behavior of the maximizer is described through a so-called *max-strategy*.

Adjé et al. [1], Costan et al. [3], Gaubert et al. [5] developed algorithms that iterate over min-strategies, whereas Esparza et al. [4], Gawlitza and Seidl [6, 7, 8, 9], Gawlitza and Monniaux [10], Gawlitza and Seidl [11, 12, 13] developed algorithms that iterate over max-strategies.

Goals. Within this internship we will focus on the algorithms that iterate over max-strategies (see Esparza et al. [4], Gawlitza and Seidl [6, 7, 8, 9], Gawlitza and Monniaux [10], Gawlitza and Seidl [11, 12, 13]). We will implement and adapt them such that they can be used for the analysis of *hybrid automata* (cf. Sankaranarayanan et al. [20]). The implementation work is preferably carried out in OCaml or C/C++.

⋆ VERIMAG is a joint laboratory of CNRS, Université Joseph Fourier and Grenoble INP.

2 Requirements

- Experience in programming (in particular in OCaml or C/C++) and knowledge of linear algebra and Linear Programming are welcome.
- Open-mindedness and enthusiasm.

Bibliography

[1] A. Adjé, S. Gaubert, and E. Goubault. Coupling policy iteration with semi-definite relaxation to compute accurate numerical invariants in static analysis. In A. D. Gordon, editor, *ESOP*, volume 6012 of *LNCS*. Springer, 2010.

[2] J. Cochet-Terrasson, S. Gaubert, and J. Gunawardena. A Constructive Fixed Point Theorem for Min-Max Functions. *Dynamics and Stability of Systems*, 14(4):407–433, 1999.

[3] A. Costan, S. Gaubert, E. Goubault, M. Martel, and S. Putot. A Policy Iteration Algorithm for Computing Fixed Points in Static Analysis of Programs. In *Computer Aided Verification, 17th Int. Conf. (CAV)*. LNCS 3576, Springer Verlag, 2005.

[4] J. Esparza, T. Gawlitza, S. Kiefer, and H. Seidl. Approximative methods for monotone systems of min-max-polynomial equations. In L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz, editors, *ICALP (1)*, volume 5125 of *LNCS*. Springer, 2008.

[5] S. Gaubert, E. Goubault, A. Taly, and S. Zennou. Static analysis by policy iteration on relational domains. In Nicola [17].

[6] T. Gawlitza and H. Seidl. Computing game values for crash games. In K. S. Namjoshi, T. Yoneda, T. Higashino, and Y. Okamura, editors, *ATVA*, volume 4762 of *LNCS*. Springer, 2007.

[7] T. Gawlitza and H. Seidl. Precise relational invariants through strategy iteration. In J. Duparc and T. A. Henzinger, editors, *CSL*, volume 4646 of *LNCS*. Springer, 2007.

[8] T. Gawlitza and H. Seidl. Precise fixpoint computation through strategy iteration. In Nicola [17].

[9] T. Gawlitza and H. Seidl. Precise interval analysis vs. parity games. In J. Cuéllar, T. S. E. Maibaum, and K. Sere, editors, *FM*, volume 5014 of *LNCS*. Springer, 2008.

[10] T. M. Gawlitza and D. Monniaux. Improving strategies via smt solving. In *European Symposium on Programming (ESOP)*. Springer Verlag, 2011 (to appear).

[11] T. M. Gawlitza and H. Seidl. Games through nested fixpoints. In *CAV*, 2009 (to appear).

[12] T. M. Gawlitza and H. Seidl. Computing relaxed abstract semantics w.r.t. quadratic zones precisely. In R. Cousot and M. Martel, editors, *SAS*, volume 6337 of *Lecture Notes in Computer Science*. Springer, 2010.

[13] T. M. Gawlitza and H. Seidl. Solving systems of rational equations through strategy iteration. *TOPLAS*, (accepted, to appear).

[14] R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors. *Hybrid Systems*, volume 736 of *Lecture Notes in Computer Science*, 1993. Springer.

[15] A. Hoffman and R. Karp. On Nonterminating Stochastic Games. *Management Sci.*, 12:359–370, 1966.

[16] R. Howard. *Dynamic Programming and Markov Processes*. Wiley, New York, 1960.

[17] R. D. Nicola, editor. *Programming Languages and Systems, 16th European Symposium on Programming, ESOP 2007, Held as Part of the Joint European Conferences on Theory and Practics of Software, ETAPS 2007, Braga, Portugal, March 24 - April 1, 2007, Proceedings*, volume 4421 of *LNCS*, 2007. Springer.

[18] A. Puri. *Theory of Hybrid and Discrete Systems*. PhD thesis, University of California, Berkeley, 1995.

[19] M. L. Puterman. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. Wiley, New York, 1994.

[20] S. Sankaranarayanan, T. Dang, and F. Ivancic. A policy iteration technique for time elapse over template polyhedra. In M. Egerstedt and B. Mishra, editors, *HSCC*, volume 4981 of *Lecture Notes in Computer Science*. Springer, 2008.

[21] A. Tarski. A lattice-theoretical fixpoint theorem and its appications. *Pac. J. Math.*, 5:285–309, 1955.

[22] J. Vöge and M. Jurdziński. A Discrete Strategy Improvement Algorithm for Solving Parity Games. In *Computer Aided Verification, 12th Int. Conf. (CAV)*. LNCS 1855, Springer, 2000.