Designing a SAT modulo ODE solver

Postdoc

——————————————

Keywords: SAT/SMT solvers, Interval analysis, Constraint programming

Lab: U2IS, ENSTA ParisTech, 828 boulevard des maréchaux 91762 Palaiseau Cedex

Advisors: Julien Alexandre dit Sandretto, Alexandre Chapoutot, and Sylvain Conchon (Université Paris-Sud)

Duration: 12 months. An extension for a second year is possible.

Expected start time Immediately.

Salary: The indicative net monthly salary is between 2200€ and 2400€, depending on experience.

——————————————

Scientific context and job description. Control-command systems are made of software part and continuous-time dynamics which closely related in order to produce an automatic behavior. They are member of the important class of *cyber-physical systems* (CPS). In order to provide guarantee on this behavior, formal verification methods can be applied to produce a mathematical proof that the system designed fulfill some (functional) requirements. Nevertheless, the challenge in applying formal verification methods on CPS is the need to take into account its continuous-time part (usually described by ordinary differential equations) and its discrete-time part, *i.e.*, the software part, (generally described by a transition system).

In previous work, on formal verification of CPS, *SAT module ODE* solvers [5, 7, 6] have been defined to tackle this challenge. These solvers embed theory solver to deal with QF_NRA logic and specialized solver to take care of ODEs. We want to take a fresh look at this approach so the aim of this postdoc project is to

- define the logic fragment suitable to verify CPS ;

- develop a new SAT modulo ODE solver taking advantage of the latest development of SMT Solver [4]; and ODE solver [3, 2, 1]

Application. The candidate

- must have obtained a PhD degree in Computer Science or related area, with excellent grades.

- is required to have a very strong background in theoretical Computer Science, logic and formal methods.

- must be capable of programming in the most popular programming languages, including C, C++, Ocaml, Bash.

- should demonstrate commitment, team working and a critical mind.

- must have a good knowledge of the English language is necessary.

Note that previous experience in formal verification by model checking and/or numerical methods for ODE, is a plus but not essential.

Candidate should send by <u>email</u>, the following documents <u>in PDF</u>,

- Academic CV with an established research record

- Covering letter stating why you consider yourself suitable for the post (maximum 2 pages A4)

- References do not need to be included with the application, but shortlisted applicants will need to send 2 reference letters before interview.

with a title "Application to Postdoc SAT modulo ODE", to

- Julien Alexandre dit Sandretto – `alexandre@ensta.fr`

- Alexandre Chapoutot – `chapoutot@ensta.fr`

- Sylvain Conchon – `sylvain.conchon@lri.fr`

Closing date for application: the 15th of February 2019

References

[1] J. Alexandre dit Sandretto and A. Chapoutot. DynBEX: a Differential Constraint Library for Studying Dynamical Systems (Poster). In *Conference on Hybrid Systems: Computation and Control*, 2016.

[2] J. Alexandre dit Sandretto and A. Chapoutot. Validated Explicit and Implicit Runge-Kutta Methods. *Reliable Computing electronic edition*, 22, 2016.

[3] O. Bouissou, A. Chapoutot, and A. Djoudi. Enclosing temporal evolution of dynamical systems using numerical methods. In *NASA Formal Methods*, number 7871 in LNCS, pages 108–123. Springer, 2013.

[4] L. M. de Moura and D. Jovanovic. A model-constructing satisfiability calculus. In *Verification, Model Checking, and Abstract Interpretation, 14th International Conference, VMCAI 2013, Rome, Italy, January 20-22, 2013. Proceedings*, pages 1–12, 2013.

[5] A. Eggers, N. Ramdani, N. Nedialkov, and M. Fränzle. Improving the sat modulo ode approach to hybrid systems analysis by combining different enclosure methods. *Software and Systems Modeling*, pages 1–28, 2012.

[6] S. Gao, S. Kong, and E. M. Clarke. dreal: An smt solver for nonlinear theories over the reals. In *International Conference on Automated Deduction*, volume 7898 of *LNCS*, pages 208–214. Springer, 2013.

[7] D. Ishii, K. Ueda, and H. Hosobe. An interval-based sat modulo ode solver for model checking nonlinear hybrid systems. *International Journal on Software Tools for Technology Transfer*, 13(5):449–461, 2011.