Solver for Feature Tree Logic

Mihaela Sighireanu and Ralf Treinen

mihaela.sighireanu@lsv.fr,ralf.treinen@irif.fr

Location: Laboratoire Méthodes Formelles (LMF), ENS Paris-Saclay, 4 avenue des Sciences, Gif-sur-Yvette, France
or IRIF, Université de Paris, 8 place Aurelie Némours, 75013 Paris, France.

Context: The Feature Tree Logic (FTL) has been proposed in the research project Colis for the specification of POSIX primitives that transform the file system (e.g., `mv` or `mkdir`) [3]. The specifications obtained in FTL have been used for the verification of installation scripts in Debian [2]. A symbolic execution engine [1] constructs an encoding of the behavior of the script as an FTL formula. This is achieved by unrolling the constructions of the scripting language (for instance POSIX shell) and combining them with the known behavior of the UNIX primitives.

The properties verified are mainly correctness properties, that is no error state is reached starting from a correct configuration. An extension to more involved properties like idempotency (executing two times the same script is like executing once) would require an efficient solver for the complete first-order theory of FTL.

The complete first order theory of FTL is decidable, a decision procedure has been proposed in [4] and implemented in OCaml for the quantifier-free fragment in the solver COLIS-DP.

Objective: This internship aims at improving the COLIS-DP solver by adding the quantifier elimination procedure proposed in [4] and a procedure for computing the minimal model of a formula in FTL. These extensions of the solver are required to check the well-formedness of the specifications for POSIX primitives and for generating tests from these specifications. An ambitious consequence of this internship is to obtain a test suite for the POSIX implementations of primitives dealing with the file system.

Workplan: The intern will start by getting familiar with the logic, the decision proposed procedure and the present version of the solver COLIS-DP [5, colis-language/tree/master/src/constraints]. Then, s.he will implement the procedure proposed in [4] for quantifier elimination and will work on an algorithm to obtain a model from a quantifier-free formula in FTL. The intern will test her/his implementation on the formulas used for the specification of POSIX primitives.

Requirement: Basic knowledge of first order logic and mastering of OCaml programming.

References

[1] Becker, B., Marché, C.: Ghost Code in Action: Automated Verification of a Symbolic Interpreter. In: Chakraborty, S., A.Navas, J. (eds.) Verified Software: Tools, Techniques and Experiments. Lecture Notes in Computer Science (2019), https://hal.inria.fr/hal-02276257

[2] Becker, B.F.H., Jeannerod, N., Marché, C., Régis-Gianas, Y., Sighireanu, M., Treinen, R.: Analysing installation scenarios of debian packages. In: Biere, A., Parker, D. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 26th International Conference, TACAS 2020, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2020, Dublin, Ireland, April 25-30, 2020, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12079, pp. 235–253. Springer (2020). https://doi.org/10.1007/978-3-030-45237-7_14, https://doi.org/10.1007/978-3-030-45237-7_14

[3] Jeannerod, N., Régis-Gianas, Y., Marché, C., Sighireanu, M., Treinen, R.: Specification of UNIX utilities. Technical report, HAL Archives Ouvertes (Oct 2019), https://hal.inria.fr/hal-02321691

[4] Jeannerod, N., Treinen, R.: Deciding the first-order theory of an algebra of feature trees with updates. In: Galmiche, D., Schulz, S., Sebastiani, R. (eds.) 9th International Joint Conference on Automated Reasoning. Lecture Notes in Computer Science, vol. 10900, pp. 439–454. Springer, Oxford, UK (Jul 2018), https://hal.archives-ouvertes.fr/hal-01807474

[5] The CoLiS project: The CoLiS toolchain. https://github.com/colis-anr