Witness Extraction for MSO on Infinite Words
Master Internship

The goal of this internship is to propose a constructive variant of MSO on infinite words, with witness extraction abilities.

Advisor: Colin Riba and Henryk Michalewski.

Location: Plume team of the Lip Laboratory, Ens de Lyon, France, or
Faculty of Mathematics, Informatics and Mechanics, University of Warsaw, Warsaw, Poland.

Contact: colin.riba@ens-lyon.fr and H.Michalewski@mimuw.edu.pl.

1 Scientific Context

MSO on Infinite Words and Automata. Monadic Second-Order Logic (MSO) on infinite words is known to be decidable since the celebrated work of Büchi [Büc62]. Decidability typically follows from an effective equivalence between MSO-formulas and finite state automata running on infinite words. Such automata, and most notably *Büchi automata*, provide an established framework for the specification and verification of non-terminating programs (in particular *via* the *model checking* technique, see e.g. [BK08]), while MSO is a yardstick language for expressing properties about them (see e.g. [PP04] for a comprehensive presentation of the subject).

Axiomatizations and Proof Theoretical Analysis of MSO. It is known since D. Siefkes's work [Sie70] that MSO on infinite words can be axiomatized as a subsystem of second-order arithmetic. This axiomatization yields a classical, non-constructive system.

On the other hand, intuitionistic variants of classical arithmetic enjoy witnessing properties, in the sense that from a constructive formal proof of a formula $\forall x.\exists y.\phi(x,y)$ one can extract a computable witnessing function f, *i.e.* a computable function f such that $\phi(n,f(n))$ holds for all n (recall that intuitionistic logic is classical logic without the excluded middle, see e.g. [SU06] for a presentation of the subject). However, this is not directly possible in the case of MSO, since in this logic there are provable statments $\forall x.\exists y.\phi(x,y)$ which can not be witnessed by any computable function.

2 Description of the Internship

The goal of this internship is to devise an intuitionistic variant of MSO, as close as possible to classical logic, but with usual intuitionistic witness extraction.

We target a system based on a restriction of MSO to particular infinite words known as *ultimately periodic words*. The ultimately periodic words are exactly the infinite words which can be generated by finite state deterministic automata; they are finitely representable and computable, and an MSO-formula is statisfiable on infinite words if and only if it is satisfiable on ultimately periodic words. Moreover, one can decide wether a given MSO-formula is satisfied by a given ultimately periodic word. We expect this decidability property to allow, in an intuitionistic system equiped with a concrete representation of ultimately periodic words, to have strong (if not all) instances of the excluded middle.

Prerequisites. There is no formal prerequisite other than undergraduate logic and automata. Basic knowledge of Büchi automata and intuitionistic logic is a plus, but not a requirement.

3 Possible Extensions

The starting question above has different extensions, including:

- Comparing intuitionistic MSO on ultimately periodic words with a known synthesis mechanism for MSO known as *Church's synthesis problem* (see e.g. [Tho08]).
- Extending the computational analysis of MSO on ultimately periodic words to MSO on infinite words generated by higher-order recursion scheme, following Ong's theorem [Ong06].

These questions (as well as others) may lead to a PhD thesis. They are part of the ANR project *RAPIDO* (lead by A. Saurin from PPS) aiming at applying proof-theoretical methods to infinite objects.

References

[BK08] C. Baier and J.-P. Katoen. *Principles of Model Checking.* MIT Press, 2008.

[Büc62] J. R. Büchi. On a Decision Methond in Restricted Second-Order Arithmetic. In E. Nagel et al., editor, *Logic, Methodology and Philosophy of Science (Proc. 1960 Intern. Congr.)*, pages 1–11. Stanford Univ. Press, 1962.

[Ong06] C.-H. L. Ong. On Model-Checking Trees Generated by Higher-Order Recursion Schemes. In *Proceedings of LICS 2006*, pages 81–90. IEEE Computer Society, 2006.

[PP04] D. Perrin and J.-É. Pin. *Infinite Words: Automata, Semigroups, Logic and Games.* Pure and Applied Mathematics. Elsevier, 2004.

[Sie70] D. Siefkes. *Decidable Theories I : Büchi's Monadic Second Order Successor Arithmetic*, volume 120 of *LNM.* Springer, 1970.

[SU06] M. H. Sørensen and P. Urzyczyn. *Lectures on the Curry-Howard Isomorphism*, volume 149 of *Studies in Logic and the Foundations of Mathematics.* Elsevier Science Inc., 2006.

[Tho08] W. Thomas. Solution of Church's problem: A tutorial. In K. Apt and R. van Rooij, editors, *New Perspectives on Games and Interaction*, volume 4. Amsterdam University Press, 2008.