Formal Verification
Project Proposal

Zhendong Ang, Louis Vialar, Arthur Jacot, Simon Guilloud

October 26, 2020

We plan to work on decision procedures for weak second-order monadic logic of one successor (WS1S) and Regular expressions, both of which are provably equivalent to finite state automatas. We will present the paper *Combining WS1S and HOL* by David Basin and Stefan Friedrich [1]. This paper explains how MONA, a tool to solve instances of WS1S, can be combined with HOL (Higher Order Logic) as it is implemented in Isabelle/HOL.

Our project will consist of the following parts:

1. Study and read the theory of WS1S, regular expressions and automatas, MONA, etc.

2. Write in scala a small program that let the user enter WS1S formulas or RE, with some usable internal encoding and basic operations on these expressions.

3. Implement the morphism from RE to automatas, and similarly for WS1S.

4. Implement the path search algorithm on automatas and the lifting of the solution to RE and WS1S.

5. (Possible, depending on time). The decision procedure for WS1S (points 3 and 4) is semantic-based. When embeding WS1S in HOL, the solution returned by MONA does not provide a proof that the corresponding HOL term is true. Indeed, Basin and Friedrich explain that proof reconstruction implies to formalize the whole theory of automatas in HOL, which is not practical. It may be interesting to be able to extract an HOL proof from the decision procedure, possibly by modifying this procedure. We're not really sure of how ambitious this is however.

References

[1] D. Basin and S. Friedrich, "Combining WS1s and HOL,"