Derivatives of WS1S Formulas

Dmitriy Traytel (traytel@in.tum.de)

Fakultät für Informatik, Technische Universität München, Germany

In his seminal work [5], Büchi envisioned weak monadic second-order logic of one successor (WS1S) to become a "more conventional formalism [that] can be used in place of regular expressions [...] for formalizing conditions on the behaviour of automata". This vision became truth—WS1S has been used to encode decision problems in hardware verification [1], network verification [2], synthesis [6], as well as many others.

Equivalence of WS1S formulas is decidable, although the decision procedure's complexity is non-elementary [9]. Nevertheless, the MONA tool [7] shows that the daunting theoretical complexity can often be overcome in practice by employing a multitude of smart optimizations. Similarly to Büchi, MONA's user manual [8] calls WS1S a "simple and natural notation" for regular languages.

Traditionally, decision procedures for WS1S do not try to benefit themselves from the conventional, simple, and natural logical notation. Instead, by exploiting the logic-automaton connection, formulas are translated into finite automata which are then minimized. During the translation all the rich algebraic formula structure including binders and high-level constructs is lost. On the other hand, the subsequent minimization might have benefited from some simplifications on the formula level.

Concerning the algebraic structure, regular expressions are situated somewhere in between of WS1S formulas and finite automata. In earlier work [15], we propose a semantics-preserving translation of WS1S formulas into regular expressions. Thereby, equivalence of WS1S formulas is reduced to equivalence of regular expressions. To decide equivalence of regular expressions, we employ a coalgebraic decision procedure based on a finality test and Brzozowski derivatives [4]—the coalgebra structure on regular expressions [12].

In recent work [13], we go one step further by defining a coalgebra structure directly on WS1S formulas. The main contributions are:

- We define a symbolic *derivative* operation for a WS1S formula.
- We define a *finality test* determining if a formula holds in the empty interpretation.
- Taking the two above notions together, we obtain a decision procedure for WS1S that operates only on formulas.
- We formalize the newly defined notions in Isabelle/HOL [10] and formally verify that the obtained algorithm indeed decides equivalence of WS1S formulas.

The obtained decision procedure can be considered an elegant toy—implementable only with a few hundreds lines of Standard ML [14] and teachable in class. By no means it should be evaluated against MONA's thousands of lines of tricky performance optimizations. On the other hand, we are confident that symbolic decision procedures must not hide behind automata-based ones in terms of performance in general as witnessed by several successful examples [3, 11].

References

[1] Basin, D., Klarlund, N.: Automata based symbolic reasoning in hardware verification. Formal Methods In System Design 13, 255–288 (1998), extended version of: "Hardware verification using monadic second-order logic," *CAV '95*, LNCS 939

[2] Baukus, K., Bensalem, S., Lakhnech, Y., Stahl, K.: Abstracting WS1S systems to verify parameterized networks. In: Graf, S., Schwartzbach, M.I. (eds.) TACAS 2000. LNCS, vol. 1785, pp. 188–203. Springer (2000)

[3] Bonchi, F., Pous, D.: Checking NFA equivalence with bisimulations up to congruence. In: Giacobazzi, R., Cousot, R. (eds.) POPL 2013. pp. 457–468. ACM (2013)

[4] Brzozowski, J.A.: Derivatives of regular expressions. J. ACM 11(4), 481–494 (Oct 1964)

[5] Büchi, J.R.: Weak second-order arithmetic and finite automata. Z. Math. Logik und Grundl. Math. 6, 66–92 (1960)

[6] Hamza, J., Jobstmann, B., Kuncak, V.: Synthesis for regular specifications over unbounded domains. In: Bloem, R., Sharygina, N. (eds.) FMCAD 2010. pp. 101–109. IEEE (2010)

[7] Henriksen, J.G., Jensen, J.L., Jørgensen, M.E., Klarlund, N., Paige, R., Rauhe, T., Sandholm, A.: MONA: Monadic second-order logic in practice. In: Brinksma, E., Cleaveland, R., Larsen, K., Margaria, T., Steffen, B. (eds.) TACAS 1995. LNCS, vol. 1019, pp. 89–110. Springer (1995)

[8] Klarlund, N., Møller, A.: MONA Version 1.4 User Manual. BRICS, Department of Computer Science, Aarhus University (January 2001), notes Series NS-01-1. Available from `http://www.brics.dk/mona/`. Revision of BRICS NS-98-3

[9] Meyer, A.R.: Weak monadic second order theory of succesor is not elementary-recursive. In: Parikh, R. (ed.) Logic Colloquium. Lecture Notes in Mathematics, vol. 453, pp. 132–154. Springer (1975)

[10] Nipkow, T., Paulson, L., Wenzel, M.: Isabelle/HOL — A Proof Assistant for Higher-Order Logic, LNCS, vol. 2283. Springer (2002)

[11] Pous, D.: Symbolic algorithms for language equivalence and kleene algebra with test. In: Walker, D. (ed.) POPL 2015. pp. 357–368. ACM (2015)

[12] Rutten, J.J.M.M.: Automata and coinduction (an exercise in coalgebra). In: Sangiorgi, D., de Simone, R. (eds.) CONCUR 1998. LNCS, vol. 1466, pp. 194–218. Springer (1998)

[13] Traytel, D.: A coalgebraic decision procedure for WS1S, `http://www21.in.tum.de/~traytel/papers/ws1s_derivatives/ws1s_derivatives.pdf`

[14] Traytel, D.: Supplementary material associated with [13]. `https://github.com/dtraytel/WS1S` (2015)

[15] Traytel, D., Nipkow, T.: Verified decision procedures for MSO on words based on derivatives of regular expressions. In: Morrisett, G., Uustalu, T. (eds.) ICFP 2013. pp. 3–12. ACM (2013)