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. Similar 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


