

An Efficient Canonical Narrowing Implementation for Protocol Analysis

Raúl López-Rueda^{a,*}, Santiago Escobar^a, José Meseguer^b

^a*VRAIN, Universitat Politècnica de València, Valencia, Spain, Camino de vera, S/N, 46022 Valencia Spain*

^b*University of Illinois, Illinois, USA, 901, West Illinois Street, IL 61801 Urbana USA*

Abstract

This work improves the *canonical narrowing* previously implemented using Maude 2.7.1 by taking advantage of the new functionalities that Maude 3.1 offers. In order to perform more faithful comparisons between algorithms, we have also implemented the Maude's standard narrowing and, since the built-in narrowing implemented at the C++ level returns only one solution, we have implemented a function to collect all the solutions. Our experiments on these three narrowing algorithms show that canonical narrowing outperforms Maude's standard narrowing, both at the C++ level and at the meta-level. The results of these experiments are relevant for narrowing-based protocol analysis tools, as well as for improving the analysis of many other narrowing-based applications such as logical model checking, theorem proving or partial evaluation.

References

- [1] Raúl López-Rueda, Santiago Escobar, and José Meseguer. An efficient canonical narrowing implementation for protocol analysis. In Kyungmin Bae, editor, *Rewriting Logic and Its Applications - 14th International Workshop, WRLA 2022, Held as a Satellite Event of ETAPS, Munich, Germany, April 2-3, 2022, Proceedings*, Lecture Notes in Computer Science. Springer, 2022. To appear.

*Corresponding author

Email addresses: rloprue@upv.es (Raúl López-Rueda), sescobar@upv.es (Santiago Escobar), meseguer@illinois.edu (José Meseguer)