CeTA – Certifying Termination and Complexity Proofs in 2016*

Sebastiaan J.C. Joosten, René Thiemann, and Akihisa Yamada

University of Innsbruck, Austria

CeTA is a certifier for automatically generated proofs. Its soundness – if CeTA accepts a proof of a certain property, then the property holds – is proven in the Isabelle/HOL [4] formalization IsaFoR [5]. A complete list of supported proof techniques as well as IsaFoR and CeTA itself are available at `http://cl-informatik.uibk.ac.at/software/ceta/`. We highlight some recent extensions of CeTA for validating complexity and termination proofs.

AC termination Previous versions of CeTA would model term rewrite systems modulo AC as relative rewrite systems and then apply techniques for relative rewriting. The new version now has support for AC dependency pairs [1], including refinements such as AC usable rules and AC dependency graphs [8].

Complexity of matrix interpretation CeTA can now precisely determine the asymptotic growth rate of A^n where A is the maximum-matrix determined by some matrix-interpretation [3]. To this end, algebraic numbers and Jordan-normal forms have been formalized [6, 7].

Integer transition systems Tools that prove termination or safety of imperative programs often abstract the program into an Integer Transition System (ITS).

Current CeTA can certify proofs of safety properties for ITSs. To show safety, a proof contains inductive invariants such that the error states have the inductive invariant False [2]. Together with Marc Brockschmidt, we work towards certifying termination proofs. These show that no transition can be taken infinitely often, using previously certified invariants.

References

1 K. Kusakari and Y. Toyama. On proving AC-termination by AC-dependency pairs. *IEICE T. Inf. Syst.*, E84-D(5):439–447, 2001.

2 K. McMillan. Lazy abstraction with interpolants. In *CAV'06*, volume 4144 of *LNCS*, pages 123–136, 2006.

3 G. Moser, A. Schnabl, and J. Waldmann. Complexity analysis of term rewriting based on matrix and context dependent interpretations. In *FSTTCS'08*, LIPIcs 2:304–315, 2008.

4 T. Nipkow, L. Paulson, and M. Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer, 2002.

5 R. Thiemann and C. Sternagel. Certification of termination proofs using CeTA. In *TPHOLs'09*, volume 5674 of *LNCS*, pages 452–468, 2009.

6 R. Thiemann and A. Yamada. Algebraic numbers in Isabelle/HOL. In *ITP'16*, LNCS, 2016. To appear.

7 R. Thiemann and A. Yamada. Formalizing Jordan normal forms in Isabelle/HOL. In *CPP'16*, pages 88–99. ACM, 2016.

8 A. Yamada, C. Sternagel, R. Thiemann, and K. Kusakari. AC dependency pairs revisited. In *CSL'16*, LIPIcs, 2016. To appear.

* This work was partially supported by FWF project Y757. The authors are listed in alphabetical order regardless of individual contributions or seniority.