CoCo Participant: CeTA 2.21*

Julian Nagele, Christian Sternagel, Thomas Sternagel,
René Thiemann, Sarah Winkler and Harald Zankl

Institute of Computer Science, University of Innsbruck, Austria

Automatic provers have become popular in several areas like first-order theorem proving, SMT, etc. Since these provers are complex pieces of software, they might contain errors which might lead to wrong answers, i.e., incorrect proofs. Therefore, certification of the generated proofs is of major importance.

The tool CeTA [6] is a certifier that can be used to certify confluence and non-confluence proofs of term rewrite systems (TRSs) and conditional term rewrite systems (CTRSs). Its soundness is proven as part of IsaFoR, the *Isabelle Formalization of Rewriting*. The following techniques are currently supported in CeTA—for further details we refer to the certification problem format (CPF) and to the sources of IsaFoR and CeTA (`http://cl-informatik.uibk.ac.at/software/ceta/`).

Term rewrite systems. Since CeTA was originally conceived for termination analysis, our first method is Newman's lemma in combination with the critical pair theorem. For possibly non-terminating TRSs, CeTA can ensure that weakly orthogonal and strongly closed TRSs are confluent, as well as check applications of the rule labeling heuristic [4] and addition and removal of redundant rules [3]. To disprove confluence one can provide a divergence $s \to^* t_1$, $s \to^* t_2$ and a certificate for non-joinability. Here CeTA supports: t_1 and t_2 are distinct normal forms, testing that $tcap(t_1\sigma)$ and $tcap(t_2\sigma)$ are not unifiable, usable rules, discrimination pairs, argument filters and interpretations [1], and reachability analysis using tree automata techniques [2].

Conditional term rewrite systems. This year a major novelty in CeTA's repertoire of confluence criteria is support for conditional rewriting. CeTA can now certify that almost orthogonal, properly oriented, right-stable 3-CTRSs are confluent [5], including support for infeasible critical pairs, where currently the supported justification is a certificate for non-reachability using *tcap*. The second supported technique for CTRSs is unraveling [7], transforming the system into a TRS where then the aforementioned techniques can be certified.

References

[1] T. Aoto. Disproving confluence of term rewriting systems by interpretation and ordering. In *FroCoS*, volume 8152 of *LNCS*, pages 311–326, 2013.

[2] B. Felgenhauer and R. Thiemann. Reachability analysis with state-compatible automata. In *LATA*, volume 8370 of *LNCS*, pages 347–359, 2014.

[3] J. Nagele, B. Felgenhauer, and A. Middeldorp. Improving automatic confluence analysis of rewrite systems by redundant rules. In *RTA*, volume 36 of *LIPIcs*, pages 257–268, 2015.

[4] J. Nagele and H. Zankl. Certified rule labeling. In *RTA*, volume 36 of *LIPIcs*, pages 269–284, 2015.

[5] C. Sternagel and T. Sternagel. Level-confluence of 3-CTRSs in Isabelle/HOL. In *IWC*, 2015. This volume.

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

[7] S. Winkler and R. Thiemann. Formalizing soundness and completeness of unravelings. In *FroCoS*, volume 9322 of *LNCS (LNAI)*, 2015. To appear.

*Supported by Austrian Science Fund (FWF), projects I963, P27502, P27528, and Y757.