

Higher-Order Confluence: Automation and Certification

Julian Nagele* 

Institute of Computer Science, University of Innsbruck

Towards Certification of Confluence Proofs for Higher-Order Rewrite Systems

- automate higher-order confluence criteria on top of CSI (first-order confluence prover): currently supported are Knuth and Bendix' criterion, (weak) orthogonality, and development closed systems
- certify confluence proofs by formalizing confluence results in Isabelle/HOL as part of IsaFoR (Isabelle Formalization of Rewriting): focus on first-order criteria that extend to higher-order setting

Automation

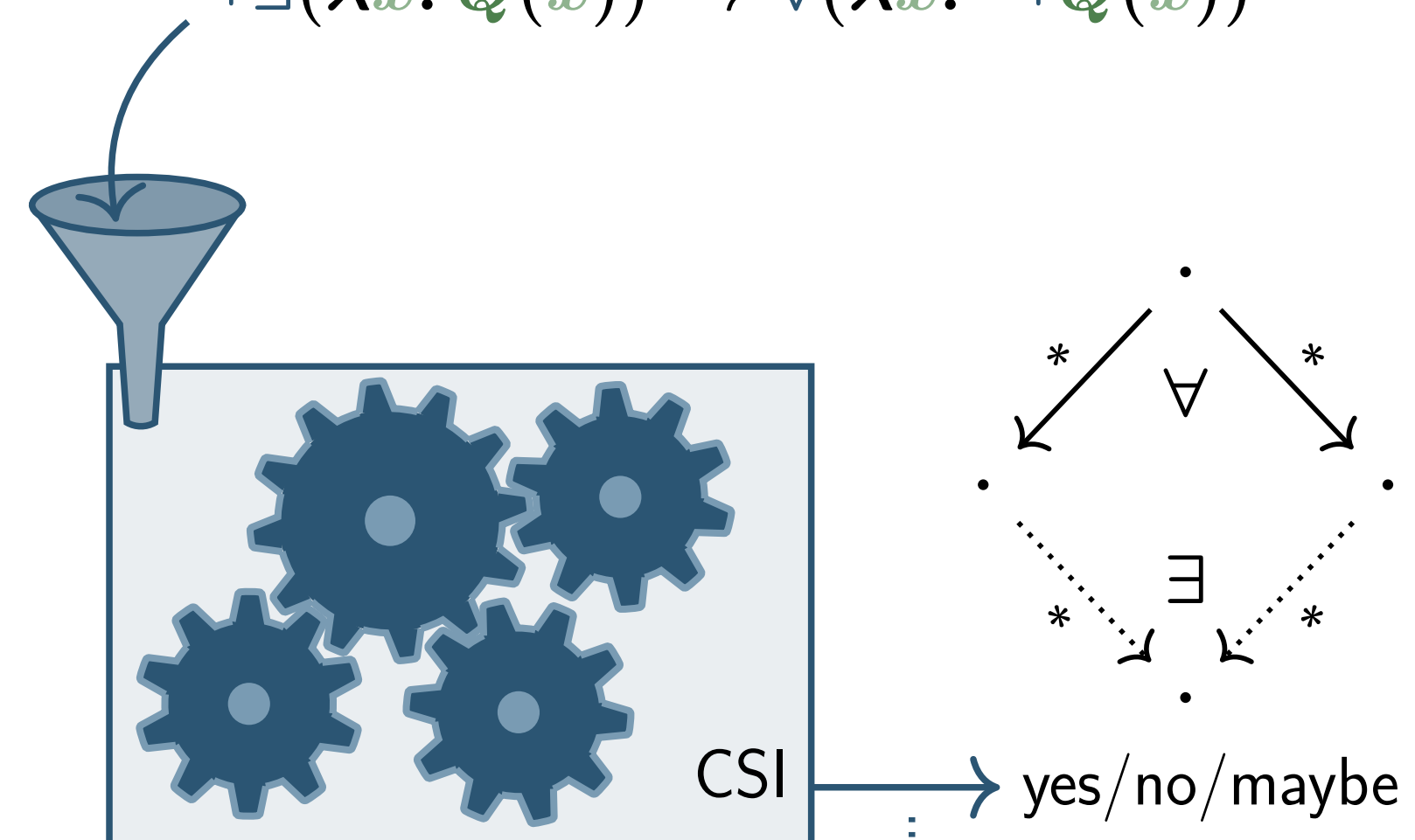
Higher-Order Rewrite Systems

- variable binding
- functional variables
- quantifiers, λ -calculi, process calculi, etc.

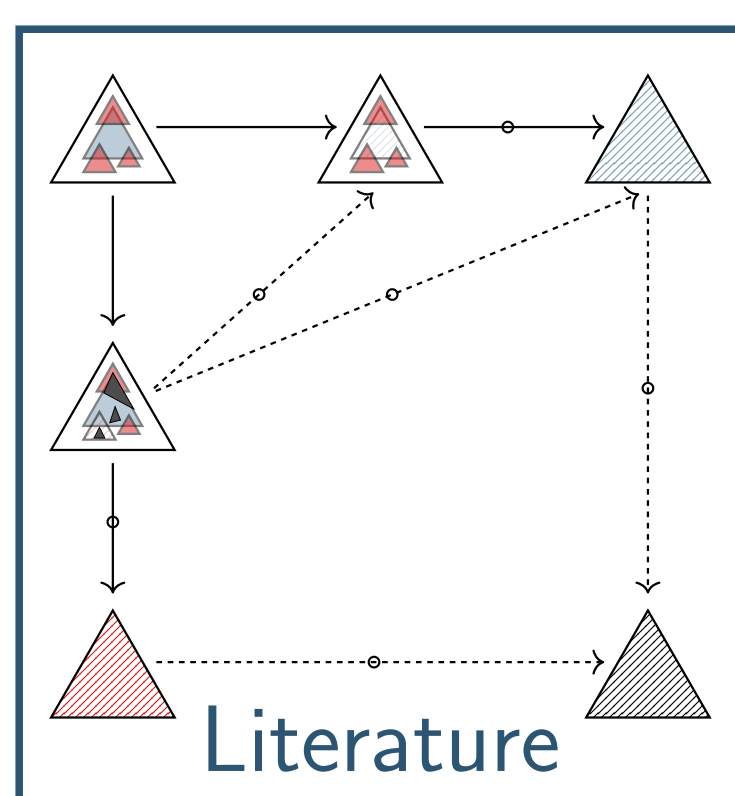
$$\begin{aligned} & \neg \neg P \rightarrow P \\ & \neg(P \wedge P') \rightarrow (\neg P) \vee (\neg P') \\ & \neg(P \vee P') \rightarrow (\neg P) \wedge (\neg P') \\ & \neg \forall(\lambda x. Q(x)) \rightarrow \exists(\lambda x. \neg Q(x)) \\ & \neg \exists(\lambda x. Q(x)) \rightarrow \forall(\lambda x. \neg Q(x)) \end{aligned}$$



- 4th Confluence Competition during IWC 2015
- new higher-order category
- certification category

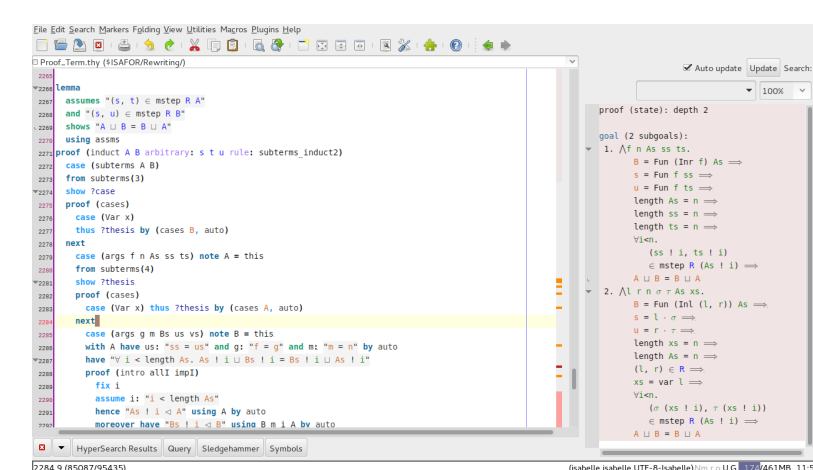
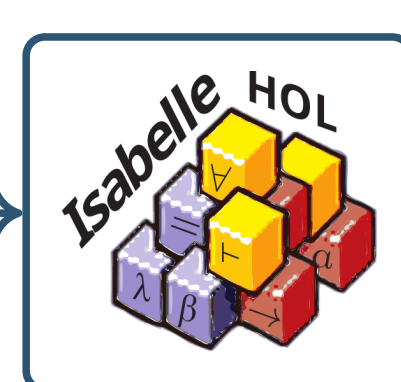


Certification



How to Trust Output of Tools?

- formalize results and techniques in proof assistant
- implement check functions with soundness proof
- generate trusted certifier from formalization



IsaFoR

code generation
& Haskell compiler

Proof

```
<certificationProblem>
<input>
...
</input>
<proof>
<crProof>
  <decreasingDiagrams>
    <relativeTerminationProof>
      <ruleRemoval>
        ...
      </ruleRemoval>
    </relativeTerminationProof>
    <ruleLabeling>
      <ruleLabelingFunction>
        ...
      </ruleLabelingFunction>
    </ruleLabeling>
    <joinableCriticalPairs>
      ...
    </joinableCriticalPairs>
  </decreasingDiagrams>
</crProof>
</proof>
</certificationProblem>
```

accept/reject/unsupported

Selected Literature



V. van Oostrom
Developing Developments
Theoretical Computer Science, 175(1):159–181, 1997



R. Mayr and T. Nipkow
Higher-Order Rewrite Systems and their Confluence
Theoretical Computer Science, 192(1):3–29, 1998



H. Zankl, B. Felgenhauer, and A. Middeldorp
CSI – A Confluence Tool
In *Proc. 23rd CADE*, volume 6803 of *LNAI*, pages 499–505, 2011



J. Nagele and R. Thiemann
Certification of Confluence Proofs using CeTA
In *Proc. 3rd IWC*, pages 19–23, 2014

* Supported by FWF (Austrian Science Fund) project P27528.