Computational Logic

Certification of Confluence Proofs

via Decreasing Diagrams

Julian Nagele and Harald Zankl

Institute of Computer Science
University of Innsbruck
Austria

41st TRS meeting Sep 26–28, 2014

Overview

- Formalization and Certification
- Progress
- Experimentals
- Conclusion

Formalization & Certification

Formalization

- formalize notions in theorem prover (definitions, etc.)
- prove theorems in theorem prover

Certification

- proof checking by trustable program
- theorem prover – generated program

This work

- formalization and certification
- decreasing diagrams, rule labeling, etc.
- Isabelle/HOL

Formalization

Definition

An ARS $\mathcal{A} = (A, \to)$ is locally decreasing if

- $\exists \mathcal{I}$ and well-founded relation $<$ on $\mathcal{I}$ with $\to = \bigcup_{\alpha \in \mathcal{I}} \to_\alpha$ and $\leftarrow_\alpha \cdot \to_\beta \subseteq \ \to^*_{\vee\alpha} \cdot \to^=_\beta \cdot \to^*_{\vee\alpha\beta} \cdot \ \leftarrow^*_{\vee\alpha\beta} \cdot \leftarrow^=_\alpha \cdot \leftarrow^*_{\vee\beta}$

Theorem (van Oostrom 1997, 2008)

A locally decreasing ARS is confluent.

$\longrightarrow$ old work (RTA 2013)
approx. 2000 lines Isabelle

Formalization & Certification

Informal Statement (van Oostrom, 2008)

A linear TRS which is locally decreasing for the rule labeling is confluent.

Duties

1. lift local decreasingness from ARSs to TRSs
2. formalize rule labeling
3. check confluence proof (certificates) generated by automated tools

$\longrightarrow$ new work (CoCo 2014)
1700 lines of Isabelle

ARS to TRS

Lemma

A linear TRS which is locally decreasing for the rule labeling is confluent.

Definition (following RTA 2011 paper)

A labeling ℓ

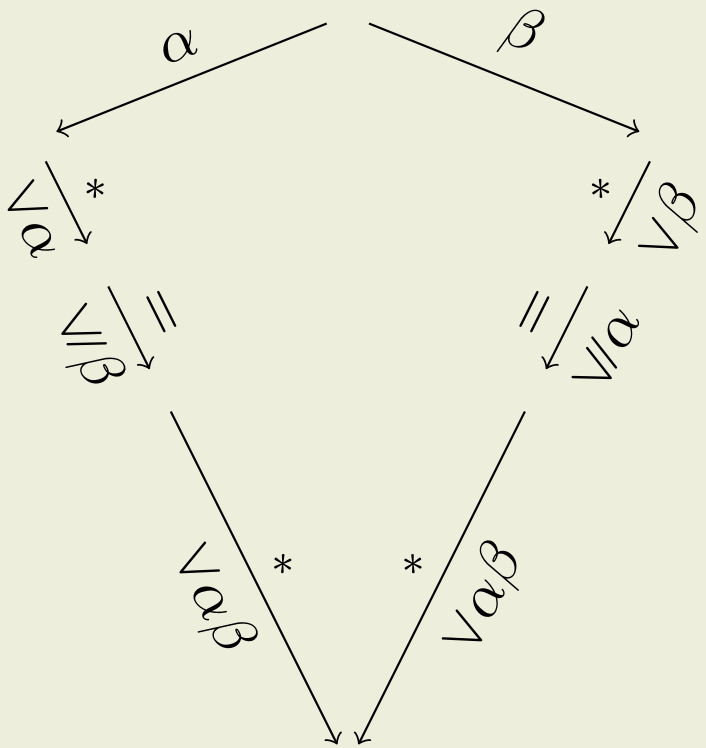
- maps rewrite steps to labels
  $\ell(s \to t) = \alpha$
- is closed under contexts and substitutions
  $\ell(s \to t) = \ell(u \to v) \longrightarrow \ell(C[s\sigma] \to C[t\sigma]) = \ell(C[u\sigma] \to C[v\sigma])$
  $\ell(s \to t) > \ell(u \to v) \longrightarrow \ell(C[s\sigma] \to C[t\sigma]) > \ell(C[u\sigma] \to C[v\sigma])$
- variable peaks and parallel peaks are locally decreasing
  ...

Lemma

A linear TRS which is locally decreasing for the rule labeling is confluent.

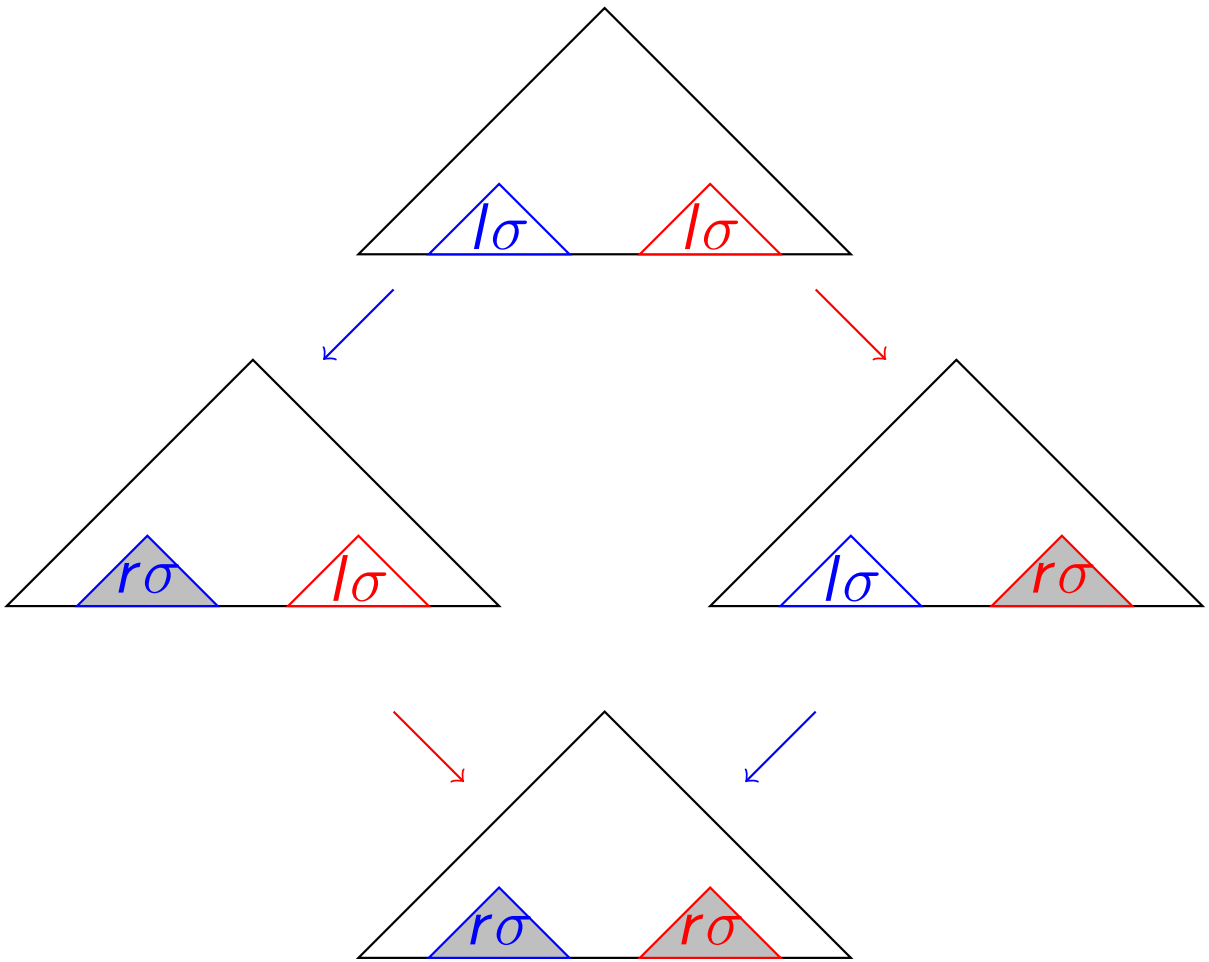
Definition

A TRS is locally decreasing if all local peaks are decreasing.



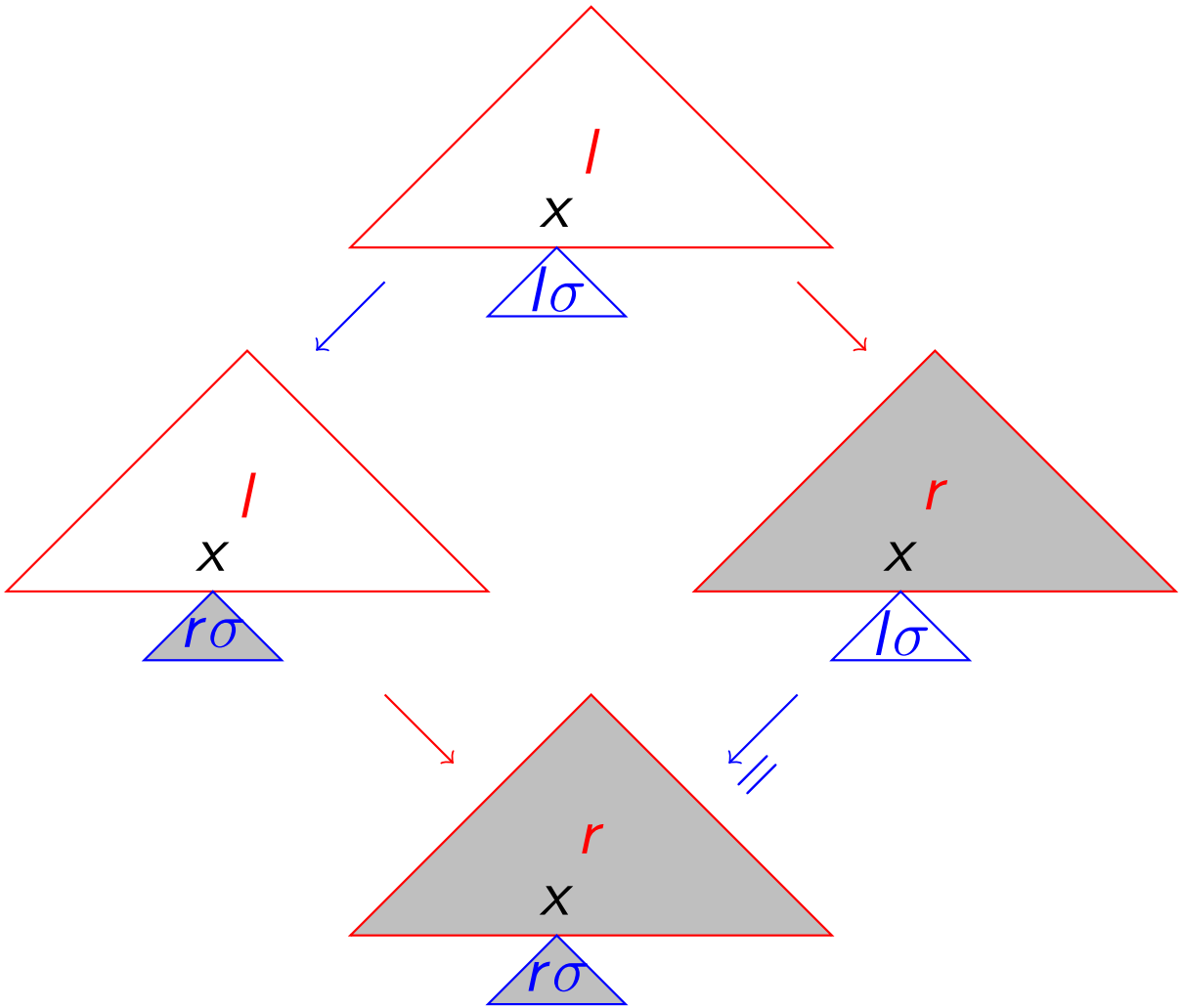
infinitely many!

Local peaks (parallel case)



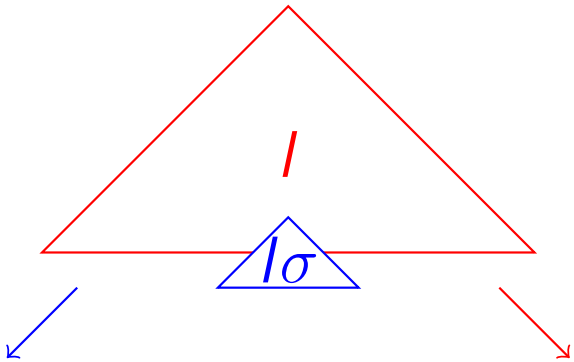
infinitely many!

Local peaks (ancestor case: $l \to r$ linear)



infinitely many!

Local peaks (critical case)



?

finitely representable!

Lemma

A TRS $\mathcal{R}$ is locally decreasing if its critical peaks are locally decreasing for a labeling ℓ.

Proof

local peak is
- parallel peak ✓
- ancestor peak ? (or instance of it) ✓
- critical peak ✗ (or instance of it) ✓

Lemma

A TRS $\mathcal{R}$ is confluent if its critical peaks are locally decreasing for a labeling ℓ.

Proof

- (labeled) ARS $\{(s, a, t) \mid s \to t, \ell(s \to t) = a\}$ locally decreasing
- conclude by main result of decreasing diagrams

Rule labeling

Lemma

A TRS $\mathcal{R}$ is confluent if its critical peaks are locally decreasing for a labeling ℓ.

Definition (Rule labeling)

$\ell_i(s \to_{l\to r,p,\sigma} t) = i\ (l \to r) \qquad i : \mathcal{R} \to \mathbb{N}$

Lemma

If $\mathcal{R}$ is linear then rule labeling is labeling.

Corollary

A linear TRS which is locally decreasing for the rule labeling is confluent.

Source labeling

Lemma

A TRS $\mathcal{R}$ is confluent if its critical peaks are locally decreasing for a labeling ℓ.

Definition (Source labeling)

$\ell(s \to t) = s$

Lemma

If $\mathcal{R}$ is linear and terminating then source labeling is labeling.

Corollary

A linear terminating TRS which is locally decreasing for the source labeling is confluent.

Certificates (for rule labeling)

Required contents

- function $i : \mathcal{R} \to \mathbb{N}$ ✓
- critical pairs ✗
- joining sequences ✓

Observations

- CeTA has to compute critical pairs
- CeTA might compute variants of critical pairs

Experimental results

method	success	contributors
(weak) orthogonality	4	René
Knuth-Bendix	26	René
strongly closedness	28	Julian
rule labeling	41	Julian/Harald
$\sum$	56	

Table: Experimental results on 148 TRSs from CoCo 2014

Future Work

Definition

An ARS $\mathcal{A} = (A, \to)$ is extended locally decreasing if

- $\exists \mathcal{I}$ and well-founded relation $<$ on $\mathcal{I}$ with $\to = \bigcup_{\alpha \in \mathcal{I}} \to_\alpha$ and $\leftarrow_\alpha \cdot \to_\beta \subseteq \to^*_{\vee\alpha} \cdot \to^=_{\not\vee\beta} \cdot \to^*_{\vee\alpha\beta} \cdot \leftarrow^*_{\vee\alpha\beta} \cdot \leftarrow^=_{\not\vee\alpha} \cdot \leftarrow^*_{\vee\beta}$ with $\leqslant \cdot < \cdot \leqslant \subseteq <$

Lemma (Hirokawa, Middeldorp 2010)

Every extended locally decreasing ARS is locally decreasing.

Motivation

1. good for source labeling + relative termination
2. not needed for predecessor labeling + relative termination

Conclusion

Future^2 Work

1. parallel reduction $\longrightarrow$ beyond linearity
2. development steps $\longrightarrow$ beyond first-order

Summary

- formalization of rule labeling ✓
- relative termination labelings ✗
- ...

The bloody guts

```
lemma ancestor_steps_lin:
 assumes "(s,t) ∈ rstep_r_p_s R (l1, r1) p1 σ1"
  and "(s,u) ∈ rstep_r_p_s R (l2, r2) p2 σ2"
  and "p1 <#> q = p2"
  and "(v1 <#> v2) = q" and "v1 ∈ poss l1" and "l1 |_v1 = Var w"
  and lin: "linear_trs R"
  defines "τ ≡ (λt. if t = w then replace_at (σ1 t) v2 (r2 · σ2) else σ1 t)"
  defines "v ≡ (ctxt_of_pos_term p1 s)⟨r1 · τ⟩"
 shows
  "(u,v) ∈ (rstep_r_p_s R (l1, r1) p1 τ)"
  "(t = v)  ∨
   (∃ q. (q ∈ poss r1 ∧ (r1 |_ q = Var w)
         ∧ (t, v) ∈ (rstep_r_p_s R (l2,r2) (p1<#>q<#>v2) σ2)))"
```

▸ back