Certified Rule Labeling

Julian Nagele    Harald Zankl

University of Innsbruck, Austria

26th RTA    1 July 2015
Overview

- Introduction
- Rule Labeling
- Relative Termination
- Certification
- Conclusion
Formalization & Certification

Introduction

Formalization & Certification

Literature

Isabelle/HOL

IsaFoR

Confluence Tool

TRS

XML Proof

CeTA

algorithms & techniques

theorems & proofs

code generation & Haskell compiler

accept/reject

The diagram illustrates the process of formalization and certification, with various tools and techniques involved. Isabelle/HOL and IsaFoR are used for formalizing theorems and proofs, which are then processed by the Confluence Tool, which in turn generates code for the Haskell compiler. The resulting code is verified by CeTA, which either accepts or rejects the rule labeling.
Theorem (van Oostrom 1994)

A *locally decreasing* ARS is confluent.
Decreasing Diagrams

**Definition**

An ARS $\{\xrightarrow{\alpha}\}_{\alpha \in \mathcal{I}}$ is **locally decreasing** if

- $\exists$ well-founded relation $<$ on $\mathcal{I}$ with

**Theorem (van Oostrom 1994)**

A locally decreasing ARS is confluent.
Decreasing Diagrams

Definition

An ARS \( \{ \rightarrow_\alpha \}_{\alpha \in I} \) is locally decreasing if

- \( \exists \) well-founded relation \(<\) on \( I \) with

\[ \forall \alpha, \beta \in I \quad \alpha < \alpha \vee \beta \quad \text{or} \quad \beta < 2 \beta \quad \text{or} \quad \alpha < \beta \]

Theorem (van Oostrom 1994)

A locally decreasing ARS is confluent.
Definition

An ARS \( \{ \to_\alpha \}_{\alpha \in \mathcal{I}} \) is locally decreasing if

- \( \exists \) well-founded relation \(<\) on \( \mathcal{I} \) with

labels \( \gamma \) with \( \gamma < \alpha \) or \( \gamma < \beta \)

Theorem (van Oostrom 1994)

A locally decreasing ARS is confluent.
An ARS $\{\to_{\alpha}\}_{\alpha \in I}$ is locally decreasing if

- $\exists$ well-founded relation $<$ on $I$ with

$$\alpha \lor \beta \lor \alpha \lor \beta \lor \alpha \lor \beta \lor \alpha \lor \beta$$

Theorem (van Oostrom 1994)

A locally decreasing ARS is confluent.

- formalized by Zankl, RTA 2013
Contribution: Formalization

Theorem (van Oostrom, 2008)

A linear TRS is confluent if it is locally decreasing for the rule labeling.
Contribution: Formalization

**Theorem (van Oostrom, 2008)**

A linear \textit{TRS} is confluent if it is locally decreasing for the rule labeling.

**Duties**

1. specialize decreasingness \textit{from ARSs to TRSs}
Contribution: Formalization

Theorem (van Oostrom, 2008)

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

Duties

1. specialize decreasingness from ARSs to TRSs
2. formalize rule labeling
**Introduction**

**Contribution: Formalization**

**Theorem (van Oostrom, 2008)**

*A linear TRS is confluent if it is locally decreasing for the rule labeling.*

**Theorem (Zankl, Felgenhauer, Middeldorp, 2011)**

*A left-linear TRS $\mathcal{R}$ is confluent if $\mathcal{R}_d/\mathcal{R}_{nd}$ is terminating and all its critical peaks are decreasing for the rule labeling.*

**Duties**

1. specialize decreasingness from ARSs to TRSs
2. formalize rule labeling
**Contribution: Formalization**

**Theorem (van Oostrom, 2008)**

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

**Theorem (Zankl, Felgenhauer, Middeldorp, 2011)**

A left-linear TRS $R$ is confluent if $R_d/R_{nd}$ is terminating and all its critical peaks are decreasing for the rule labeling.

**Duties**

1. specialize decreasingness from ARSs to TRSs
2. formalize rule labeling
3. formalize source labeling and interplay with rule labeling
Contribution: Formalization & Certification

Theorem (van Oostrom, 2008)
A linear TRS is confluent if it is locally decreasing for the rule labeling.

Theorem (Zankl, Felgenhauer, Middeldorp, 2011)
A left-linear TRS $\mathcal{R}$ is confluent if $\mathcal{R}_d/\mathcal{R}_{nd}$ is terminating and all its critical peaks are decreasing for the rule labeling.

Duties
1. specialize decreasingness from ARSs to TRSs
2. formalize rule labeling
3. formalize source labeling and interplay with rule labeling
4. check confluence proof certificates generated by automated tools
From ARSs to TRSs

Lemma

A linear TRS is confluent if it is locally decreasing for the rule labeling.
From ARSs to TRSs

**Lemma**

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

**Definition**

A TRS is locally decreasing if all local peaks are decreasing.
From ARSs to TRSs

**Lemma**

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

**Definition**

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

\[ \alpha \lor \beta \lor \alpha \lor \beta = \lor \alpha \lor \beta \lor \alpha \lor \beta \]

 infinitely many!

JN & HZ (UIBK)
**Lemma**

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

**Definition**

A TRS is locally decreasing if all local peaks are decreasing.
From ARSs to TRSs

Lemma

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

Definition

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

Local Peaks

\[ s[r_1\sigma_1]_p \leftarrow s[l_1\sigma_1]_p = s = s[l_2\sigma_2]_q \rightarrow s[r_2\sigma_2]_q \]
From ARSs to TRSs

Lemma

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

Definition

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

Local Peaks

\[ s[r_1\sigma_1]_p \leftarrow s[l_1\sigma_1]_p = s = s[l_2\sigma_2]_q \rightarrow s[r_2\sigma_2]_q \]

three possibilities (modulo symmetry):

(parallel peak) \( p \parallel q \)

(function peak) \( q \leq p \) and \( p \backslash q \in Pos_F(l_2) \)

(variable peak) \( q \leq p \) and \( p \backslash q \notin Pos_F(l_2) \)
Local Peaks: Parallel Peak
Local Peaks: Parallel Peak

\[ l_\sigma \quad l_\sigma \quad l_\sigma \]

\[ r_\sigma \quad l_\sigma \quad r_\sigma \]

\[ r_\sigma \quad r_\sigma \quad r_\sigma \]

infinitely many
Local Peaks: Variable Peak \((l \rightarrow r \text{ linear})\)
Local Peaks: Variable Peak ($l \rightarrow r$ linear)

\[ l \sigma \]

\[ r \sigma \]

infinitely many
Local Peaks: Function Peak

\[ l \sigma \]

\[ ? \]

infinitely many!
Local Peaks: (Instance of) Critical Peak

\[ I \]

\[ I_\sigma \]

finitely representable!
Lemma

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

A linear TRS which is locally decreasing for the rule \textit{labeling} is confluent.

Definition

A labeling $\ell$

- maps rewrite steps to labels
- is closed under contexts and substitutions
A linear TRS which is locally decreasing for the rule labeling is confluent.

**Definition**

A labeling $\ell$

- maps rewrite steps to labels
  \[ \ell(s \to t) = \alpha \]
- is closed under contexts and substitutions
  If $\ell(s \to t) = \ell(u \to v)$ then $\ell(C[s\sigma] \to C[t\sigma]) = \ell(C[u\sigma] \to C[v\sigma])$
  If $\ell(s \to t) > \ell(u \to v)$ then $\ell(C[s\sigma] \to C[t\sigma]) > \ell(C[u\sigma] \to C[v\sigma])$
A linear TRS which is locally decreasing for the rule labeling is confluent.

**Definition**

A labeling $\ell$

- maps rewrite steps to labels
  \[ \ell(s \rightarrow t) = \alpha \]
- is closed under contexts and substitutions
  If $\ell(s \rightarrow t) = \ell(u \rightarrow v)$ then $
  \ell(C[s\sigma] \rightarrow C[t\sigma]) = \ell(C[u\sigma] \rightarrow C[v\sigma])$
  If $\ell(s \rightarrow t) > \ell(u \rightarrow v)$ then
  $\ell(C[s\sigma] \rightarrow C[t\sigma]) > \ell(C[u\sigma] \rightarrow C[v\sigma])$
- is compatible with $\mathcal{R}$ if parallel and variables peaks of $\mathcal{R}$ are locally decreasing for $\ell$
A TRS $\mathcal{R}$ is locally decreasing if its critical peaks are locally decreasing for a compatible labeling $\ell$. 

**Proof**

- $\mathcal{R} \cup \alpha \{ (s, t) \mid s \rightarrow t \text{ and } \ell(s \rightarrow t) = \alpha \}$ is locally decreasing
- Conclude by main result of decreasing diagrams
Lemma

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

Proof

by case analysis on peaks using compatibility, closure under context/substitution and mirroring diagrams
Labeling

Lemma

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

Proof

by case analysis on peaks using compatibility, closure under context/substitution and mirroring diagrams

Corollary

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

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

Proof

by case analysis on peaks using compatibility, closure under context/substitution and mirroring diagrams

Corollary

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

Proof

- $\text{ARS} \cup_{\alpha} \{(s, t) \mid s \rightarrow t \text{ and } \ell(s \rightarrow t) = \alpha\}$ is locally decreasing
- conclude by main result of decreasing diagrams
Lemma

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

**Definition (Rule labeling)**

$$\ell^i(s \rightarrow_{l,r,p,\sigma} t) = i(l \rightarrow r) \quad i: \mathcal{R} \rightarrow \mathbb{N}$$
Rule Labeling

Lemma

A TRS \( \mathcal{R} \) is confluent if its critical peaks are locally decreasing for a compatible labeling \( \ell \).

Definition (Rule labeling)

\[ \ell^i(s \rightarrow_{l ightarrow r, p, \sigma} t) = i(l \rightarrow r) \quad i: \mathcal{R} \rightarrow \mathbb{N} \]

Lemma

If \( \mathcal{R} \) is linear then rule labeling is compatible labeling.
Rule Labeling

Definition (Rule labeling)

\[ \ell^i(s \rightarrow_{l \rightarrow r, p, \sigma} t) = i(l \rightarrow r) \quad i : \mathcal{R} \rightarrow \mathbb{N} \]

Lemma

If \( \mathcal{R} \) is linear then rule labeling is compatible labeling.

Proof

Parallel Peak

Variable Peak
Rule Labeling

Lemma

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

Definition (Rule labeling)

\[
\ell^i(s \rightarrow_{l,p,\sigma} t) = i(l \rightarrow r) \quad i: \mathcal{R} \rightarrow \mathbb{N}
\]

Lemma

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

Corollary

A linear TRS is confluent if its critical peaks are locally decreasing for the rule labeling.
Definition (Source labeling)

\[ \ell^{\text{src}}(s \rightarrow_l r, p, \sigma \ t) = s \]
Source labeling

Definition (Source labeling)

\[ \ell^{\text{src}}(s \rightarrow^l r, p, \sigma t) = s \]

Theorem

A left-linear TRS \( R \) is confluent if \( R_d/R_{nd} \) is terminating and all its critical peaks are decreasing for the rule labeling.
Local Peaks: Variable Peak ($l \rightarrow r$ left-linear)
Local Peaks: Variable Peak ($l \rightarrow r$ left-linear)
Source Labeling

Definition (Source labeling)

- \( \ell_{src}(s \rightarrow l \rightarrow r, p, \sigma \ t) = s \)
- labels are compared with \( \rightarrow^{+} \mathcal{R}_{d}/\mathcal{R}_{nd} \)

\[ s \rightarrow s \rightarrow t \rightarrow u \rightarrow u_1 \rightarrow v \rightarrow u_1 \rightarrow u \]
Source Labeling

Definition (Source labeling)
- $\ell_{\text{src}}(s \rightarrow_{l \rightarrow r, p, \sigma} t) = s$
- labels are compared with $\rightarrow_{\mathcal{R}_d/\mathcal{R}_{nd}}$

Definition
An ARS $\{\rightarrow_\alpha\}_{\alpha \in \mathcal{I}}$ is extended locally decreasing if
- $\exists$ well-founded relation $<$ on $\mathcal{I}$ and preorder $\leq$ with $\leq \cdot < \cdot \leq \subseteq <$ and
- $\alpha \leftarrow \cdot \rightarrow \beta \subseteq \rightarrow^* \cdot \rightarrow^* \vee \beta \cdot \rightarrow^* \vee \alpha \beta \cdot \vee \alpha \beta \leftarrow \cdot \vee \beta \leftarrow$
Relative Termination

Source Labeling

Definition (Source labeling)

- $\ell^{\text{src}}(s \rightarrow_{l \rightarrow r, p, \sigma} t) = s$
- labels are compared with $\rightarrow^{+}_{R_d/R_{nd}}$

Definition

An ARS $\{\rightarrow_{\alpha}\}_{\alpha \in \mathcal{I}}$ is extended locally decreasing if

- $\exists$ well-founded relation $<$ on $\mathcal{I}$ and preorder $\leq$ with $\leq \cdot < \cdot \leq \subseteq <$ and

  $\alpha \leftarrow \cdot \rightarrow \beta \subseteq \rightarrow^{*}_{\vee \alpha} \cdot \rightarrow^{*}_{\vee / \beta} \cdot \rightarrow^{*}_{\vee \alpha \beta} \cdot \vee / \alpha \leftarrow \cdot \vee \beta \leftarrow$

Lemma (Hirokawa, Middeldorp 2010)

Every extended locally decreasing ARS is locally decreasing.
Source Labeling

Definition (Source labeling)
- \( \ell^{\text{src}}(s \rightarrow I \rightarrow r, p, \sigma \ t) = s \)
- labels are compared with \( \rightarrow^{+}_{Rd/Rnd} \) and \( \rightarrow^{*}_{R} \)

Definition
An ARS \( \{ \rightarrow_{\alpha} \}_{\alpha \in I} \) is extended locally decreasing if
- \( \exists \) well-founded relation \( < \) on \( I \) and preorder \( \leq \) with \( \leq \cdot < \cdot \leq \subseteq < \) and
\[
\alpha \leftarrow \cdot \rightarrow_{\beta} \subseteq \rightarrow_{\wedge \alpha}^{*} \cdot \rightarrow_{\vee \beta}^{*} \cdot \vee_{\alpha \beta}^{*} \cdot \leftarrow_{\wedge \alpha}^{*} \cdot \leftarrow_{\vee \beta}^{*}
\]

Lemma (Hirokawa, Middeldorp 2010)
Every extended locally decreasing ARS is locally decreasing.
Lemma

If $R_d/R_{nd}$ is terminating for a left-linear TRS $R$ then lexicographic combination $\ell^{src} \times \ell^i$ is a compatible labeling.
Lexicographic Combination

Lemma

If $R_d/R_{nd}$ is terminating for a left-linear TRS $R$ then lexicographic combination $\ell^{src} \times \ell^i$ is a compatible labeling.

\[
\ell_1 \times \ell_2(s \rightarrow t) = (\ell_1(s \rightarrow t), \ell_2(s \rightarrow t)) \\
(\alpha_1, \alpha_2) \geq (\beta_1, \beta_2) \text{ iff } \alpha_1 > \beta_1 \text{ or } \alpha_1 \geq \beta_1 \text{ and } \alpha_2 \geq \beta_2 \\
(\alpha_1, \alpha_2) > (\beta_1, \beta_2) \text{ iff } \alpha_1 > \beta_1 \text{ or } \alpha_1 \geq \beta_1 \text{ and } \alpha_2 > \beta_2
\]
Lemma

If $R_d/R_{nd}$ is terminating for a left-linear TRS $R$ then lexicographic combination $\ell^{src} \times \ell^i$ is a compatible labeling.

Theorem

A left-linear TRS $R$ is confluent if $R_d/R_{nd}$ is terminating and all its critical peaks are decreasing for the rule labeling.
Relative Termination

Lexicographic Combination

Lemma

If $\mathcal{R}_d/\mathcal{R}_{nd}$ is terminating for a left-linear TRS $\mathcal{R}$ then lexicographic combination $\ell^{src} \times \ell^i$ is a compatible labeling.

Theorem

A left-linear TRS $\mathcal{R}$ is confluent if $\mathcal{R}_d/\mathcal{R}_{nd}$ is terminating and all its critical peaks are decreasing for the rule labeling.

Proof Sketch

- choose $\ell^{src} \times \ell^i$ as labeling
- for critical peaks: along a rewrite sequence labels never increase with respect to $\ell^{src}$
Certificates

Required Contents

- function $i: \mathcal{R} \rightarrow \mathbb{N}$
- certificate for termination of $\mathcal{R}_d/\mathcal{R}_{nd}$
- joining sequences for critical peaks
Certificates

Required Contents

- function $i : \mathcal{R} \rightarrow \mathbb{N}$
- certificate for termination of $\mathcal{R}_d/\mathcal{R}_{nd}$
- joining sequences for critical peaks

Observations

- CeTA has to compute critical peaks
- CeTA computes variants of critical peaks
- checking relative termination condition is completely independent of checking decreasingness for rule labeling
## Experimental results

<table>
<thead>
<tr>
<th>method</th>
<th>success</th>
</tr>
</thead>
<tbody>
<tr>
<td>(weak) orthogonality</td>
<td></td>
</tr>
<tr>
<td>Knuth-Bendix</td>
<td></td>
</tr>
<tr>
<td>strong closedness</td>
<td></td>
</tr>
<tr>
<td>$\ell^i$</td>
<td></td>
</tr>
<tr>
<td>$\ell^i + \text{SN}(R_d/R_{nd})$</td>
<td></td>
</tr>
<tr>
<td>$\sum$</td>
<td></td>
</tr>
</tbody>
</table>

**Table:** Experimental results for 148 TRSs from CoCo 2014.
## Experimental results

<table>
<thead>
<tr>
<th>method</th>
<th>success</th>
<th>CoCo 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>(weak) orthogonality</td>
<td>4</td>
<td>✓</td>
</tr>
<tr>
<td>Knuth-Bendix</td>
<td>26</td>
<td>✓</td>
</tr>
<tr>
<td>strong closedness</td>
<td>28</td>
<td>✓</td>
</tr>
<tr>
<td>$\ell^i$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\ell^i + \text{SN}(\mathcal{R}<em>d/\mathcal{R}</em>{nd})$</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>$\sum$</td>
<td>45</td>
<td></td>
</tr>
</tbody>
</table>

Table: Experimental results for 148 TRSs from CoCo 2014.
# Experimental results

<table>
<thead>
<tr>
<th>method</th>
<th>success</th>
<th>CoCo 2013</th>
<th>CoCo 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>(weak) orthogonality</td>
<td>4</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Knuth-Bendix</td>
<td>26</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>strong closedness</td>
<td>28</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$\ell^i$</td>
<td>41</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>$\ell^i + \text{SN}(\mathcal{R}<em>d/\mathcal{R}</em>{nd})$</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>$\sum$</td>
<td>45</td>
<td>56</td>
<td></td>
</tr>
</tbody>
</table>

**Table:** Experimental results for 148 TRSs from CoCo 2014.
## Experimental results

<table>
<thead>
<tr>
<th>method</th>
<th>success</th>
<th>CoCo 2013</th>
<th>CoCo 2014</th>
<th>CeTA 2.19</th>
</tr>
</thead>
<tbody>
<tr>
<td>(weak) orthogonality</td>
<td>4</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Knuth-Bendix</td>
<td>26</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>strong closedness</td>
<td>28</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ℓᵢ</td>
<td>41</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ℓᵢ + SN(ℛᵣ/ℛₘᵣ)</td>
<td>46</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>∑</td>
<td>45</td>
<td>56</td>
<td>58</td>
<td></td>
</tr>
</tbody>
</table>

**Table:** Experimental results for 148 TRSs from CoCo 2014.
Conclusion

Summary

- formalization of rule labeling
- in combination with relative termination using source labeling
- checking confluence certificates based on decreasing diagrams for the first time
Summary

- formalization of rule labeling
- in combination with relative termination using source labeling
- checking confluence certificates based on decreasing diagrams for the first time

Future Work

- lexicographic combination of labelings in certificate
- support more labelings
- label parallel/development steps