Automated Proofs of Confluence of Term Rewrite Systems

Bertram Felgenhauer

Computational Logic
Institute of Computer Science
University of Innsbruck

JAIST Spring School
Kanazawa 2012-03-08

Contents

Term Rewrite Systems

Definitions

- function symbols $\mathcal{F}$ with arity $\mathsf{ari} : \mathcal{F} \to \mathbb{N}$
- (infinite) set of variables $\mathcal{V}$ $(x, y, z, \ldots)$
- terms $\mathcal{T}(\mathcal{F}, \mathcal{V}) := \mathcal{V} \cup \{f(t_1, \ldots, t_{\mathsf{ari}(f)}) \mid t_i \in \mathcal{T}(\mathcal{F}, \mathcal{V})\}$
- positions $\mathcal{P}\mathsf{os}(v) = \{\epsilon\}$,
  $\mathcal{P}\mathsf{os}(f(t_1, \ldots, t_n)) = \{\epsilon\} \cup \{i \cdot p \mid i = 1 \ldots n, p \in \mathcal{P}\mathsf{os}(t_i)\}$
- subterm $t|_p$ $(p \in \mathcal{P}\mathsf{os}(t))$
- replacement $t[t']_p$
- substitution $\sigma : \mathcal{V} \to \mathcal{T}(\mathcal{F}, \mathcal{V})$ with $\{v \mid \sigma(v) \neq v\}$ finite
- TRS $\mathcal{R} \subseteq \mathcal{T}(\mathcal{F}, \mathcal{V})^2$ with $l \notin \mathcal{V}$ and $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(l)$ for $l \to r \in \mathcal{R}$
- rewrite step $t[l\sigma]_p \to_{\mathcal{R}} t[r\sigma]_p$, where $l \to r \in \mathcal{R}$

Example

Let $\mathcal{F} = \{^{-1}, \circ\}$, $\mathcal{V} = \{x, y, z, \dots\}$ and $\mathcal{R}$ consist of the rules

$$1 \circ x \to x \qquad x^{-1} \circ x \to 1 \qquad (x \circ y) \circ z \to x \circ (y \circ z)$$

Then we can rewrite

$$\underline{((x^{-1})^{-1} \circ x^{-1})} \circ x \to_{\mathcal{R}} \underline{1 \circ x} \to_{\mathcal{R}} x$$
$$\underline{((x^{-1})^{-1} \circ x^{-1}) \circ x} \to_{\mathcal{R}} (x^{-1})^{-1} \circ \underline{(x^{-1} \circ x)} \to_{\mathcal{R}} (x^{-1})^{-1} \circ 1$$

This proves $x = (x^{-1})^{-1} \circ 1$.

Example

Let $\mathcal{R}'$ consist of the rules

$$
\begin{array}{rrr}
1 \circ x \to x & x^{-1} \circ x \to 1 & (x \circ y) \circ z \to x \circ (y \circ z) \\
x \circ 1 \to x & x \circ x^{-1} \to 1 & x^{-1} \circ (x \circ y) \to y \\
(x^{-1})^{-1} \to x & 1^{-1} \to 1 & x \circ (x^{-1} \circ y) \to y \\
 & & (x \circ y)^{-1} \to y^{-1} \circ x^{-1}
\end{array}
$$

Then

$$\underline{(x^{-1})^{-1}} \circ 1 \to_{\mathcal{R}'} \underline{x \circ 1} \to_{\mathcal{R}'} x$$

This proves $x = (x^{-1})^{-1} \circ 1$.
In fact $\mathcal{R}'$ is complete: terminating and confluent.

Proofs and Confluence

Let $\to$ be a (rewrite) relation. Define

- $\leftarrow = \to^{-1}$ (inverse), $\leftrightarrow = \leftarrow \cup \to$ (symmetric closure)
- $\xrightarrow{=}$ (reflexive closure), $\xrightarrow{+}$ (transitive closure), $\xrightarrow{*}$ (reflexive, transitive closure)
- proof $t \xleftrightarrow{*} t'$ $(t = t_0 \leftrightarrow t_1 \cdots t_{n-1} \leftrightarrow t_n = t')$

If every peak proof $t \xleftarrow{*} \cdot \xrightarrow{*} t'$ has an equivalent valley proof $t \xrightarrow{*} \cdot \xleftarrow{*} t'$, then $\to$ is confluent.
If every proof $t \xleftrightarrow{*} t'$ has a valley proof $t \xrightarrow{*} \cdot \xleftarrow{*} t'$, then $\to$ has the Church-Rosser-property.

Proposition

Confluence and the Church-Rosser-property are equivalent.

Newman's Lemma

- $\to$ is terminating if it allows no infinite reduction $t_0 \to t_1 \to \cdots$
- $\to$ is locally confluent if $\leftarrow \cdot \to \subseteq \xrightarrow{*} \cdot \xleftarrow{*}$

Lemma

If $\to$ is terminating and locally confluent, then $\to$ is confluent.

Proof. $\succ = \xrightarrow{+}$ is well-founded. We measure proofs

$$t_0 \leftrightarrow t_1 \leftrightarrow \cdots \leftrightarrow t_n \quad (*)$$

by the multiset $\{t_i \mid i = 0 \ldots n\}$. If $t_{i-1} \leftarrow t_i \to t_{i+1}$ then by local confluence $t_{i-1} \to u_1 \to \cdots \leftarrow u_{m-1} \leftarrow t_{i+1}$, where $t_i \succ u_j$.

$$t_0 \xleftrightarrow{*} t_{i-1} \xrightarrow{*} u_? \xleftarrow{*} t_{i+1} \xleftrightarrow{*} t_n$$

has smaller measure than $(*)$. Hence this process will terminate. ∎

Knuth-Bendix Criterion

Let $\mathcal{R}$ be a TRS.

- $l_1 \to r_1, l_2 \to r_2 \in \mathcal{R}$. W.l.o.g. $\mathcal{V}\mathrm{ar}(l_1) \cap \mathcal{V}\mathrm{ar}(l_2) = \varnothing$
- $p \in \mathcal{P}\mathrm{os}(l_2)$ and $l_2|_p \notin \mathcal{V}$
- σ be a most general unifier of l_1 and $l_2|_p$ ($l_1\sigma = l_2|_p\sigma$)

Then $\langle l_2[r_1]_p\sigma, r_2\sigma\rangle$ is a critical pair of $\mathcal{R}$.

Note. $l_2[r_1]_p\sigma \leftarrow l_2[l_1]_p\sigma = l_2\sigma \to r_2\sigma$

Example. $\mathcal{R} = \{1 \circ x \to x, x^{-1} \circ x \to 1, (x \circ y) \circ z \to x \circ (y \circ z)\}$ has a critical pair $\langle 1 \circ z, x^{-1} \circ (x \circ z)\rangle$ originating from $(x^{-1} \circ x) \circ z$.

Lemma

If all critical pairs of $\mathcal{R}$ have a valley proof then $\to_{\mathcal{R}}$ is locally confluent.

Theorem (Knuth, Bendix 1970)

If $\mathcal{R}$ is terminating and all critical pairs are joinable, then $\mathcal{R}$ is confluent.

Orthogonality

A TRS $\mathcal{R}$ is called orthogonal if it is left-linear (no duplicate variables in left-hand sides of rules) and has no critical pairs.
We write $t \mathrel{+\!\!\!\!\!\!\to}_{\mathcal{R}} t'$ if $t \to_{\mathcal{R}} t_1 \cdots t_{n-1} \to_{\mathcal{R}} t'$ such that all rewrite steps are at parallel positions.

Lemma (Parallel Moves)

If $\mathcal{R}$ is orthogonal then ${}_{\mathcal{R}}\!\leftarrow\!\!\!\!\!\!\!+\!\!\!+ \cdot \mathrel{+\!\!\!+\!\!\!\!\!\!\to}_{\mathcal{R}} \subseteq \mathrel{+\!\!\!+\!\!\!\!\!\!\to}_{\mathcal{R}} \cdot {}_{\mathcal{R}}\!\leftarrow\!\!\!\!\!\!\!+\!\!\!+$

Lemma

If $\leftarrow \cdot \to \subseteq \to \cdot \leftarrow$ then $\to$ is confluent.

Proof. Like Newman's Lemma, but count number of inversions (area).

Theorem (Rosen 1973)

If $\mathcal{R}$ is orthogonal then $\mathcal{R}$ is confluent.

Proof. Note that $\to \subseteq \mathrel{+\!\!\!+\!\!\!\!\!\!\to} \subseteq \xrightarrow{*}$, so $\xrightarrow{*} = \mathrel{+\!\!\!+\!\!\!\!\!\!\to}^*$. ∎

Non-left-linearity Trouble

Let $\mathcal{R}$ be given by

$$\mathsf{F}(x,x) \to \mathsf{A} \qquad \mathsf{F}(x,\mathsf{G}(x)) \to \mathsf{B} \qquad \mathsf{C} \to \mathsf{G}(\mathsf{C})$$

Then $\mathcal{R}$ has no critical pairs but is not confluent.

A related example is

$$\mathsf{F}(x,x) \to A \qquad \mathsf{G}(x) \to \mathsf{F}(x,\mathsf{G}(x)) \qquad \mathsf{C} \to \mathsf{G}(\mathsf{C})$$

Decreasing Diagrams

Definition. Given

- a set of labels $\mathcal{L}$ equipped with a well-founded order $\succ$
- a collection of rewrite relations $(\underset{\alpha}{\rightarrow})_{\alpha \in \mathcal{L}}$
- $\underset{\curlyvee\alpha}{\longrightarrow} = \bigcup_{\alpha \succ \beta} \underset{\beta}{\rightarrow}$ and $\underset{\curlyvee\alpha,\beta}{\longrightarrow} = \underset{\curlyvee\alpha}{\longrightarrow} \cup \underset{\curlyvee\beta}{\longrightarrow}$.

$(\underset{\alpha}{\rightarrow})$ is locally decreasing if for all $\alpha, \beta \in \mathcal{L}$,

$$\underset{\alpha}{\leftarrow} \cdot \underset{\beta}{\rightarrow} \subseteq \overset{*}{\underset{\curlyvee\alpha}{\longleftrightarrow}} \cdot \overset{=}{\underset{\beta}{\rightarrow}} \cdot \overset{*}{\underset{\curlyvee\alpha,\beta}{\longleftrightarrow}} \cdot \overset{=}{\underset{\alpha}{\leftarrow}} \cdot \overset{*}{\underset{\curlyvee\beta}{\longleftrightarrow}}$$

Theorem (van Oostrom 1994, 2008)

If $(\underset{\alpha}{\rightarrow})$ is locally decreasing then $\bigcup_{\alpha \in \mathcal{L}} \underset{\alpha}{\rightarrow}$ is confluent.

Proof. By some suitable measure on proofs.

Applying Decreasing Diagrams

Questions

- How to label rewrite steps?
- What kind of rewrite steps?
- How to obtain an effectively checkable criterion?

Examples

- Newman's lemma: Label $s \to t$ by s, ordered by $\xrightarrow{+}$.
- Orthogonality: Use $\mathrel{+\!\!\!\!\!\!\;+\!\!\!\!\!\rightarrow}$, but only a single label.
- Rule labeling: Label $s \to_{\mathcal{R}} t$ by the used rewrite step.
- ...

To check local decreasingness, analyze critical pairs.

Applying Decreasing Diagrams

Theorem (van Oostrom 2008)

Let $\mathcal{R}$ be a linear TRS, and $\succ$ be a well-founded order on $\mathcal{L} = \mathcal{R}$. If all critical peaks can be joined decreasingly, then $\mathcal{R}$ is confluent.

Proof. Measure rewrite steps by the applied rule. ∎

Theorem (Hirokawa, Middeldorp 2010)

Let $\mathcal{R}$ be a left-linear TRS such that the critical pair steps $\mathsf{CPS}(\mathcal{R})$ are terminating relative to $\mathcal{R}$, and critical pairs are joinable. Then $\mathcal{R}$ is confluent.

Proof idea. Measure rewrite steps $s \dashrightarrow\!\!\!\!\!\!\dashv\ t$ by s, ordered by the relative rewriting relation. ∎

Decomposition Methods

Theorem (Toyama 1987)

Let $\mathcal{R}_0$ and $\mathcal{R}_1$ be TRSs over disjoint signatures. Then $\mathcal{R}_0 \cup \mathcal{R}_1$ is confluent if and only if both $\mathcal{R}_0$ and $\mathcal{R}_1$ are confluent.

Theorem (Aoto, Toyama 1997)

Let $\mathcal{R}$ be a many-sorted TRS such that rules preserve well-sorted terms. Then $\mathcal{R}$ is confluent as a many-sorted TRS if and only if $\mathcal{R}$ is confluent as an unsorted TRS.

Theorem (F., Zankl, Middeldorp 2011)

Let $\mathcal{R}$ be an order-sorted TRS such that rules preserve well-sorted terms. If $\mathcal{R}$ is left-linear or non-duplicating then $\mathcal{R}$ is confluent if and only if $\mathcal{R}$ is confluent as an unsorted TRS. Otherwise, if $\mathcal{R}$ also reflects well-sorted terms, then again $\mathcal{R}$ is confluent iff $\mathcal{R}$ is confluent as an unsorted TRS.

Demo

CSI

Confluence Sill Inn

Past / Related

Refinements of orthogonality

- parallel closed TRSs, development closed TRSs
- special cases for overlay critical pairs

Reduction-Preserving Completion

- Idea: If $s \to_{\mathcal{R}} t \to_{\mathcal{R}} u$ then we can add $s \to r$ as a rule to $\mathcal{R}$ without affecting confluence.

Decidable Cases

- ground TRSs
- shallow, right-linear TRSs

Non-Confluence

- stable root symbols
- tree automata techniques

Other tools

- ACP
- Saigawa

Present

Proving confluence by rewriting proofs

- eliminate local peaks
- show termination

From abstract criteria to concrete

- analyze parallel, nested and critical overlap cases
- termination analysis is useful!

Decomposition

- smaller TRSs are often easier to deal with
- parts may have nice properties like left-linearity

Future

Open problems

- powerful criteria for non-terminating, non-left-linear TRSs
- more applications of decreasing diagrams
- convincing applications for confluence in absence of termination

Confluence Competition

- `http://coco.nue.riec.tohoku.ac.jp/`
- still easy to write competitive tools

Future

Open problems

- powerful criteria for non-terminating, non-left-linear TRSs
- more applications of decreasing diagrams
- convincing applications for confluence in absence of termination

Confluence Competition

- `http://coco.nue.riec.tohoku.ac.jp/`
- still easy to write competitive tools

Thank you!

Literature I

- Aoto, T., Toyama, Y.:
  Persistency of confluence.
  JUCS 3(11), 1134–1147 (1997)
- Felgenhauer, B., Zankl, H., Middeldorp, A.:
  Proving confluence with layer systems.
  In: Proc. 31st FSTTCS. . LIPIcs, vol. 13, pp. 288–299 (2011)
- Hirokawa, N., Middeldorp, A.:
  Decreasing diagrams and relative termination.
  In: Proc. 5th IJCAR. . LNCS (LNAI), vol. 6173, pp. 487–501 (2010)
- Huet, G.:
  Confluent reductions: Abstract properties and applications to term rewriting systems.
  JACM 27(4), 797–821 (1980)

Literature II

Klop, J., Middeldorp, A., Toyama, Y., de Vrijer, R.:
Modularity of confluence: A simplified proof.
IPL 49, 101–109 (1994)

Knuth, D., Bendix, P.:
Simple word problems in universal algebras.
In: Leech, J. (ed.) Computational Problems in Abstract Algebra, 263–297.
Pergamon Press (1970)

van Oostrom, V.:
Confluence by decreasing diagrams – converted.
In: Proc. 19th RTA. . LNCS, vol. 5117, pp. 306–320 (2008)