Formalizing Almost Development Closed Critical Pairs

Christina Kohl
Universität Innsbruck, Austria

Aart Middeldorp
Universität Innsbruck, Austria

Abstract

We report on the first formalization of the almost-development closedness criterion for confluence of left-linear term rewrite systems and illustrate a problem we encountered while trying to formalize the original paper proof by van Oostrom.

2012 ACM Subject Classification Theory of computation → Rewrite systems; Theory of computation → Logic and verification

Keywords and phrases Term rewriting, confluence, certification

Digital Object Identifier 10.4230/LIPIcs.ITP.2023.38

Category Short Paper

Supplementary Material *InteractiveResource (Isabelle Code)*: http://informatik-protem.uibk.ac.at/ITP2023/

Funding *Aart Middeldorp*: Austrian Science Fund (FWF) project I5943.

1 Introduction

Recently we formalized the well-known confluence criterion by van Oostrom based on development closed critical pairs of left-linear term rewrite systems in the proof assistant Isabelle/HOL [6]. Here we present an extension of this result which goes back to an observation by Toyama, namely that the condition on critical pairs can be weakened in case of overlays. This so-called *almost* development-closed criterion and its commutation version have now been integrated into the library IsaFoR[1] which enables the tool CeTA [5] to certify confluence and commutation proofs based on this criterion.

In Section 2 we recap some important definitions and basic results about term rewriting and proof terms. The latter are used to represent multi-steps as first-order terms in the formalized proof. In Section 3 we present a slightly adapted version of our recent formalization of the development-closed criterion presented in [3]. In Section 4 we first illustrate why we could not simply follow van Oostrom's paper proof for almost development-closedness in [9, 10]. Then we show how the proof in Section 3 can easily be extended to the more general version. Finally, we briefly describe the adaptations necessary for the commutation version of almost development-closed critical pairs.

HTML versions of the relevant Isabelle theory files can be found at

`http://informatik-protem.uibk.ac.at/ITP2023/`

and the main results in this paper are annotated by a ☑-symbol which directly links to the HTML presentation.

[1] http://cl-informatik.uibk.ac.at/isafor

14th International Conference on Interactive Theorem Proving (ITP 2023).
Editors: Adam Naumowicz and René Thiemann; Article No. 38; pp. 38:1–38:8
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2 Preliminaries

We assume familiarity with the basics of term rewriting, as can be found in [1], and only recap some important definitions here. The *multi-step* relation $\mathrel{\ominus\!\!\!\rightarrow}_{\mathcal{R}}$ is inductively defined on terms as follows:

- $x \mathrel{\ominus\!\!\!\rightarrow}_{\mathcal{R}} x$ for all variables x,
- $f(s_1,\ldots,s_n) \mathrel{\ominus\!\!\!\rightarrow}_{\mathcal{R}} f(t_1,\ldots,t_n)$ if $s_i \mathrel{\ominus\!\!\!\rightarrow}_{\mathcal{R}} t_i$ for all $1 \leqslant i \leqslant n$, and
- $\ell\sigma \mathrel{\ominus\!\!\!\rightarrow}_{\mathcal{R}} r\tau$ if $\ell \rightarrow r \in \mathcal{R}$ and $\sigma(x) \mathrel{\ominus\!\!\!\rightarrow}_{\mathcal{R}} \tau(x)$ for all $x \in \mathcal{V}\mathsf{ar}(\ell)$.

A critical *overlap* $(\ell_1 \rightarrow r_1, p, \ell_2 \rightarrow r_2)_\sigma$ of two TRSs $\mathcal{R}_1$ and $\mathcal{R}_2$ consists of variants $\ell_1 \rightarrow r_1$ and $\ell_2 \rightarrow r_2$ of rewrite rules in $\mathcal{R}_1$ and $\mathcal{R}_2$ without common variables, a position $p \in \mathcal{P}\mathsf{os}_{\mathcal{F}}(\ell_2)$, and a most general unifier σ of ℓ_1 and $\ell_2|_p$. From a critical overlap $(\ell_1 \rightarrow r_1, p, \ell_2 \rightarrow r_2)_\sigma$ we obtain a critical peak $\ell_2\sigma[r_1\sigma]_p\ {}_{\mathcal{R}_1}\!\leftarrow \ell_2\sigma[\ell_1\sigma]_p = \ell_2\sigma \rightarrow_{\mathcal{R}_2} r_2\sigma$ and the corresponding *critical pair* $\ell_2\sigma[r_1\sigma]_p\ {}_{\mathcal{R}_1}\!\leftarrow \rtimes \rightarrow_{\mathcal{R}_2} r_2\sigma$. Whenever $p = \epsilon$ we say $r_1\sigma\ {}_{\mathcal{R}_1}\!\leftarrow \rtimes \rightarrow_{\mathcal{R}_2} r_2\sigma$ is an *overlay*. A relation $\rightarrow$ is confluent if ${}^*\!\leftarrow \cdot \rightarrow^* \subseteq \rightarrow^* \cdot {}^*\!\leftarrow$. Two relations $\rightarrow_1$ and $\rightarrow_2$ commute if ${}_1^*\!\leftarrow \cdot \rightarrow_2^* \subseteq \rightarrow_2^* \cdot {}_1^*\!\leftarrow$. A relation $\rightarrow$ has the *diamond property* if $\leftarrow \cdot \rightarrow \subseteq \rightarrow \cdot \leftarrow$ and it is *strongly confluent* if $\leftarrow \cdot \rightarrow \subseteq \rightarrow^= \cdot {}^*\!\leftarrow$. We say that $\rightarrow_1$ and $\rightarrow_2$ *strongly commute* if ${}_1\!\leftarrow \cdot \rightarrow_2 \subseteq \rightarrow_2^= \cdot {}_1^*\!\leftarrow$. The following well-known results [1, Chapter 2] connect the diamond property and strong confluence (strong commutation) with confluence (commutation).

▶ **Lemma 1.** *Let $\rightarrow$, $\rightarrow_1$ and $\rightarrow_2$ be binary relations.*

1. *If $\rightarrow$ has the diamond property then $\rightarrow$ is confluent.*
2. *If $\rightarrow$ is strongly confluent then $\rightarrow$ is confluent.*
3. *If $\rightarrow_1 \subseteq \rightarrow_2 \subseteq \rightarrow_1^*$ and $\rightarrow_2$ is confluent then $\rightarrow_1$ is confluent.*
4. *Two strongly commuting relations commute.*
5. *Suppose $\rightarrow_1 \subseteq \rightarrow_{1'} \subseteq \rightarrow_1^*$ and $\rightarrow_2 \subseteq \rightarrow_{2'} \subseteq \rightarrow_2^*$. If $\rightarrow_{1'}$ and $\rightarrow_{2'}$ commute then $\rightarrow_1$ and $\rightarrow_2$ commute.* ◀

When applying this lemma to prove that (almost) development closed critical pairs imply confluence for left-linear TRSs, we instantiate $\rightarrow$ in the first (second) item with $\mathrel{\ominus\!\!\!\rightarrow}$ to obtain confluence of $\mathrel{\ominus\!\!\!\rightarrow}$. Then we can use the third item with the property $\rightarrow \subseteq \mathrel{\ominus\!\!\!\rightarrow} \subseteq \rightarrow^*$ to establish confluence of $\rightarrow$. The fourth and fifth items are used for the commutation version.

We used proof terms ([7, Chapter 8]) to represent multi-steps for both the formalization in [3] and the extension presented here. We only recap some concepts here. For a more basic introduction including examples see [2, 3]. Proof terms are built from function symbols, variables, and rule symbols. We use Greek letters for rule symbols. If α is a rule symbol then $\mathsf{lhs}(\alpha)$ ($\mathsf{rhs}(\alpha)$) denotes the left-hand (right-hand) side of the rewrite rule denoted by α. Furthermore $\mathsf{var}(\alpha)$ denotes the list $(x_1,\ldots,x_n)$ of variables appearing in α in some fixed order. The length of this list is the arity of α. The list $\mathsf{vpos}(\alpha) = (p_1,\ldots,p_n)$ denotes the corresponding variable positions in $\mathsf{lhs}(\alpha)$ such that $\mathsf{lhs}(\alpha)|_{p_i} = x_i$. Given a rule symbol α with $\mathsf{var}(\alpha) = (x_1,\ldots,x_n)$ and terms $t_1,\ldots,t_n$, we write $\langle t_1,\ldots,t_n\rangle_\alpha$ for the substitution $\{x_i \mapsto t_i \mid 1 \leqslant i \leqslant n\}$. Given a proof term A, its source $\mathsf{src}(A)$ and target $\mathsf{tgt}(A)$ are computed by the following equations for $\mathsf{st} \in \{\mathsf{src},\mathsf{tgt}\}$:

$$\mathsf{st}(x) = x \qquad \mathsf{st}(f(A_1,\ldots,A_n)) = f(\mathsf{st}(A_1),\ldots,\mathsf{st}(A_n))$$
$$\mathsf{src}(\alpha(A_1,\ldots,A_n)) = \mathsf{lhs}(\alpha)\langle \mathsf{src}(A_1),\ldots,\mathsf{src}(A_n)\rangle_\alpha$$
$$\mathsf{tgt}(\alpha(A_1,\ldots,A_n)) = \mathsf{rhs}(\alpha)\langle \mathsf{tgt}(A_1),\ldots,\mathsf{tgt}(A_n)\rangle_\alpha$$

Proof terms A and B are said to be *co-initial* if they have the same source. A proof term A over a TRS $\mathcal{R}$ is a witness of the multi-step $\mathsf{src}(A) \mathrel{\ominus\!\!\!\rightarrow}_{\mathcal{R}} \mathsf{tgt}(A)$. Every multi-step is witnessed by a proof term.

▶ **Lemma 2.** *For any substitution σ, proof term context C, and proof term A we have*

$$\begin{aligned} \mathsf{src}(A\sigma) &= \mathsf{src}(\mathsf{src}(A)\sigma) & \mathsf{tgt}(A\sigma) &= \mathsf{tgt}(\mathsf{tgt}(A)\sigma) \\ \mathsf{src}(C[A]) &= \mathsf{src}(C[\mathsf{src}(A)]) = \mathsf{src}(C)[\mathsf{src}(A)] & \mathsf{tgt}(C[A]) &= \mathsf{tgt}(C[\mathsf{tgt}(A)]) \end{aligned}$$ ◀

The following lemma will be used to complete the proof of strong confluence of almost development closed TRSs.

▶ **Lemma 3.** *If $s \to^* t$ then $\mathsf{tgt}(C[s\sigma]) \to^* \mathsf{tgt}(C[t\sigma])$ for arbitrary proof term contexts C and arbitrary substitutions over proof terms σ.* ☑

Proof. Straightforward induction on proof term contexts and using the fact that the rewrite relation is closed under contexts and substitutions. ◀

The following labeling is used to measure the amount of overlap between co-initial proof terms:

$$\mathsf{src}^\sharp(A) = \begin{cases} A & \text{if } A \in \mathcal{V} \\ f(\mathsf{src}^\sharp(A_1), \ldots, \mathsf{src}^\sharp(A_n)) & \text{if } A = f(A_1, \ldots, A_n) \\ \mathsf{lhs}^\sharp(\alpha)\langle \mathsf{src}^\sharp(A_1), \ldots, \mathsf{src}^\sharp(A_n)\rangle_\alpha & \text{if } A = \alpha(A_1, \ldots, A_n) \end{cases}$$

where $\mathsf{lhs}^\sharp(\alpha) = \varphi(\mathsf{lhs}(\alpha), \alpha, 0)$ with $\varphi(t, \alpha, i) = t$ if $t \in \mathcal{V}$ and $\varphi(t, \alpha, i) = f_{\alpha^i}(\varphi(t_1, \alpha, i + 1), \ldots, \varphi(t_n, \alpha, i + 1))$ if $t = f(t_1, \ldots, t_n)$. The (partial) function ℓ extracts labels from function symbols: $\ell(f_{\alpha^n}) = \alpha^n$. The amount of overlap $\blacktriangle(A, B)$ between co-initial proof terms A and B is defined as $\blacktriangle(A, B) = |\mathcal{P}\mathsf{os}_L(A) \cap \mathcal{P}\mathsf{os}_L(B)|$ where $\mathcal{P}\mathsf{os}_L(A) = \{p \in \mathcal{P}\mathsf{os}(\mathsf{src}^\sharp(A)) \mid \ell(\mathsf{src}^\sharp(A)(p)) \text{ is defined}\}$. This corresponds exactly to the measure used in [9, 10]. The set $\mathsf{overlaps}(A, B)$ consists of all pairs (p, q) of function symbol positions in the common source s of A and B such that

(a) $\ell(\mathsf{src}^\sharp(A)(p)) = \alpha^0$, $\ell(\mathsf{src}^\sharp(B)(q)) = \beta^0$, and

(b) either $p \leqslant q$ and $\ell(\mathsf{src}^\sharp(A)(q)) = \alpha^{|q \backslash p|}$ or $q < p$ and $\ell(\mathsf{src}^\sharp(B)(p)) = \beta^{|p \backslash q|}$

for some rule symbols α and β. We define the following order on overlaps: $(p_1, q_1) \leqslant (p_2, q_2)$ iff $p_1 \leqslant p_2$ and $q_1 \leqslant q_2$. An *innermost overlap* of co-initial proof terms A and B is a maximal element in $\mathsf{overlaps}(A, B)$ with respect to $\leqslant$.

3 Development Closed Critical Pairs

In this section we briefly recap the already formalized confluence criterion based on development closed critical pairs. Compared to the presentation in [3] we were able to remove some unnecessary results about deletion and joins of proof terms from the formalization. The price for this shortening is a greater focus on possibly less intuitive results involving substitutions and contexts with proof terms. The big advantage however is that the extension to almost development closed critical pairs later on is straightforward. The following definition and theorem are due to van Oostrom [9, 10].

▶ **Definition 4.** *A* TRS *$\mathcal{R}$ is development closed if for every critical pair $s \rtimes t$ of $\mathcal{R}$ we have $s \mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}} t$.*

▶ **Theorem 5.** *If a* TRS *$\mathcal{R}$ is left-linear and development closed then $\mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}}$ has the diamond property.*

Formalized proof. Assume $t \mathrel{\leftarrow\!\!\!\circ\!\!-} s \mathrel{-\!\!\circ\!\!\!\rightarrow} u$ and let A be a proof term representing $s \mathrel{-\!\!\circ\!\!\!\rightarrow} t$ and let B be a proof term representing $s \mathrel{-\!\!\circ\!\!\!\rightarrow} u$. We show $t \mathrel{-\!\!\circ\!\!\!\rightarrow} v \mathrel{\leftarrow\!\!\!\circ\!\!-} u$ for some term v by well-founded induction on the amount of overlap between A and B.

- Base case: If $\blacktriangle(A, B) = 0$ then $A \,/\, B$ and $B \,/\, A$ are well-defined and represent the multi-steps $t \mathrel{-\!\!\circ\!\!\!\rightarrow} \mathsf{tgt}(A \,/\, B)$ and $u \mathrel{-\!\!\circ\!\!\!\rightarrow} \mathsf{tgt}(B \,/\, A)$ respectively. Since $\mathsf{tgt}(A \,/\, B) = \mathsf{tgt}(B \,/\, A)$ this proves the base case of the induction.
- Step case: Assume $\blacktriangle(A, B) > 0$. The induction hypothesis states that if A' and B' are two co-initial proof terms such that $\blacktriangle(A', B') < \blacktriangle(A, B)$ then there exists a term v and and multi-steps $\mathsf{tgt}(A') \mathrel{-\!\!\circ\!\!\!\rightarrow} v \mathrel{\leftarrow\!\!\!\circ\!\!-} \mathsf{tgt}(B')$. We show that $t \mathrel{-\!\!\circ\!\!\!\rightarrow} v \mathrel{\leftarrow\!\!\!\circ\!\!-} u$:
  1. First we select an innermost overlap (p, q) and assume without loss of generality that $q \leqslant p$. Let $q' = p \backslash q$ and α and β be the rule symbols at positions p and q in $\mathsf{src}(A)$ and $\mathsf{src}(B)$ such that $\ell(\mathsf{src}^\sharp(A)(p)) = \alpha^0$ and $\ell(\mathsf{src}^\sharp(B)(q)) = \beta^0$. Furthermore let $\mathsf{vpos}(\alpha) = (p_1, \ldots, p_n)$, $\mathsf{var}(\alpha) = (x_1, \ldots, x_n)$, $\mathsf{vpos}(\beta) = (q_1, \ldots, q_m)$, and $\mathsf{var}(\beta) = (y_1, \ldots, y_m)$ where we assume $\{x_1, \ldots, x_n\} \cap \{y_1, \ldots, y_m\} = \varnothing$ without loss of generality.
  2. Then we split the proof term A into two proof terms: First the single step $s \to t'$ represented by $\Delta_1 = s[\alpha(s|_{pp_1}, \ldots, s|_{pp_n})]_p$ and second the residual $A \,/\, \Delta_1$ witnessing $t' \mathrel{-\!\!\circ\!\!\!\rightarrow} t$ for some term t'. We do the same for B obtaining $\Delta_2 = s[\beta(s|_{qq_1}, \ldots, s|_{qq_m})]_q$ witnessing $s \to u'$ and the residual $B \,/\, \Delta_2$ witnessing $u' \mathrel{-\!\!\circ\!\!\!\rightarrow} u$ for some term u'.
  3. We define the substitution
$$\begin{aligned}\tau &= \{x_i \mapsto \mathsf{lhs}(\beta)|_{q'p_i} \mid 1 \leqslant i \leqslant n \text{ and } q'p_i \in \mathcal{P}\mathsf{os}(\mathsf{lhs}(\beta))\}\\ &\cup \{y_j \mapsto lhs(\alpha)|_{q_j \backslash q} \mid 1 \leqslant j \leqslant m \text{ and } q_j \backslash q \in \mathcal{P}\mathsf{os}_{\mathcal{F}}(\mathsf{lhs}(\alpha))\}\end{aligned}$$
     which yields the critical peak $\mathsf{lhs}(\beta)[\mathsf{rhs}(\alpha)\tau]_{q'} \leftarrow \mathsf{lhs}(\beta)[\mathsf{lhs}(\alpha)\tau]_{q'} = \mathsf{lhs}(\beta)\tau \to \mathsf{rhs}(\beta)\tau$ [3, Lemma 7.2] and the position $q_\beta \in \mathcal{P}\mathsf{os}(B)$ such that $B = B[\beta(B_1, \ldots, B_m)]_{q_\beta}$ and $\mathsf{src}(B)[\;]_q = \mathsf{src}(B[\;]_{q_\beta})$. I.e, q_β is the unique position of the rule symbol β in B corresponding to the critical peak.
  4. By the development closedness assumption we know that there exists a multi-step $\mathsf{lhs}(\beta)[\mathsf{rhs}(\alpha)\tau]_{q'} \mathrel{-\!\!\circ\!\!\!\rightarrow} \mathsf{rhs}(\beta)\tau$. Let D' be a proof term representing this multi-step.
  5. Next we define the substitution
$$\rho = \{y_j \mapsto B_j \mid 1 \leqslant j \leqslant m\} \cup \{x_i \mapsto \mathsf{lhs}(\beta)\langle B_1, \ldots, B_m\rangle_\beta|_{q'p_i} \mid 1 \leqslant i \leqslant n\}$$
     and show that the proof term $B[D'\rho]_{q_\beta}$ witnesses a multi-step $t' \mathrel{-\!\!\circ\!\!\!\rightarrow} u$ [3, Lemma 7.7].
  6. We show $\blacktriangle(A \,/\, \Delta_1, B[D'\rho]_{q_\beta}) < \blacktriangle(A, B)$ [3, Lemma 7.8].
  7. The previous items allow us to apply the induction hypothesis to obtain multi-steps $t \mathrel{-\!\!\circ\!\!\!\rightarrow} v$ and $u \mathrel{-\!\!\circ\!\!\!\rightarrow} v$ for some common term v. ◀

4 Almost Development Closed Critical Pairs

Van Oostrom [9, 10] realized that the previous result could be strengthened analogously to Toyama's extension [8] for *almost* parallel closed term rewrite systems. The main observation is that by proving confluence of $\mathcal{R}$ via strong confluence of $\mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}}$ instead of the diamond property of $\mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}}$, the condition on overlays can be weakened to $\mathrel{-\!\!\circ\!\!\!\rightarrow} \cdot {}^*\!\!\leftarrow$ instead of $\mathrel{-\!\!\circ\!\!\!\rightarrow}$.

▶ **Definition 6.** *A* TRS $\mathcal{R}$ *is almost development closed if for every critical pair* $s \rtimes t$ *of* $\mathcal{R}$

1. $s \mathrel{-\!\!\circ\!\!\!\rightarrow} t$ *if* $s \rtimes t$ *is not an overlay,*
2. $s \mathrel{-\!\!\circ\!\!\!\rightarrow} \cdot {}^*\!\!\leftarrow t$ *if* $s \rtimes t$ *is an overlay.*

Since $s \mathrel{-\!\!\circ\!\!\!\rightarrow} t$ implies $s \mathrel{-\!\!\circ\!\!\!\rightarrow} \cdot {}^*\!\!\leftarrow t$ one can also simply drop the requirement that $s \rtimes t$ is an overlay in the second item.

▶ **Theorem 7.** *If a* TRS $\mathcal{R}$ *is left-linear and almost development closed then* $\mathrel{-\!\!\circ\!\!\!\rightarrow}$ *is strongly confluent.* ☑

Strong confluence of $\mathrel{\circ\!\!\!\!\!\longrightarrow}_{\mathcal{R}}$ immediately yields confluence of the TRS $\mathcal{R}$ by Lemma 1.

▶ **Corollary 8.** *Left-linear, almost development closed* TRS*s are confluent.* ◀

4.1 Original Proof

In [9, 10] van Oostrom indicates that the induction part of the proof of Theorem 5 can be easily adapted for proving Theorem 7, only the base case becomes more difficult since the possibility of overlays needs to be taken into account here. To be precise, in [9] it is stated that the second part of the proof of Theorem 5 *"can be essentially followed, proving strong confluence instead of the diamond property . . . and changing the measure defined above by not counting the function symbols in critical intersections for overlays."* And according to [10] *"The idea is not to take symbols taking part in overlays between the development steps into account, for the amount of interference. This changes nothing in the second (induction) part of the proof."* Hence a natural first step to formalizing Theorem 7 seems to be defining the new measure – let us call it $\blacktriangle'$ – as follows:

▶ **Definition 9.** $\blacktriangle'(A, B) = \{p \mid \ell(\mathsf{src}^\sharp(A)(p)) = \alpha^m,\ \ell(\mathsf{src}^\sharp(A)(p)) = \beta^n$ *and* $m \neq n$ *for some* α*,* β*,* m *and* $n\}$

As indicated in [9, 10] proving strong confluence of $\mathrel{\circ\!\!\!\!\!\longrightarrow}$ should now proceed as in the proof of Theorem 5, where the inductive case should be easy using the new measure. However, as the following example shows, things are not that easy. The problem is that function positions, that were previously not counted because they were involved in overlays, might be counted after constructing $B[D'\rho]_{q_\beta}$.

▶ **Example 10.** The TRS consisting of the five rewrite rules

$$\begin{array}{llll}
\alpha\colon & \mathsf{f}(\mathsf{g}(x),\mathsf{a}) \to \mathsf{f}(x,\mathsf{a}) & \gamma\colon\ \mathsf{g}(\mathsf{a}) \to \mathsf{b} & \epsilon\colon\ \mathsf{f}(\mathsf{b},\mathsf{a}) \to \mathsf{f}(\mathsf{a},\mathsf{a}) \\
\beta\colon & \mathsf{f}(\mathsf{g}(\mathsf{g}(y_1)),y_2) \to \mathsf{f}(\mathsf{g}(y_1),y_2) & \delta\colon\ \mathsf{g}(\mathsf{b}) \to \mathsf{g}(\mathsf{a}) &
\end{array}$$

is left-linear and development closed[2] and hence also almost development closed.

Consider the proof terms $A = \alpha(\gamma)$ and $B = \beta(\mathsf{a},\mathsf{a})$. We have

$$\mathsf{src}^\sharp(A) = \mathsf{f}_{\alpha^0}(\mathsf{g}_{\alpha^1}(\mathsf{g}_{\gamma^0}(\mathsf{a}_{\gamma^1})),\mathsf{a}_{\beta^1}) \qquad \text{and} \qquad \mathsf{src}^\sharp(B) = \mathsf{f}_{\beta^0}(\mathsf{g}_{\beta^1}(\mathsf{g}_{\beta^2}(\mathsf{a})),\mathsf{a})$$

and hence $\blacktriangle(A, B) = 3$. The function symbols at positions ϵ and 1 do not count in the new measure since they correspond to the overlay between rules α and β. So $\blacktriangle'(A, B) = 1$. Now we pick the innermost overlap between γ in A and β in B. So $\Delta_1 = \mathsf{f}(\mathsf{g}(\gamma),\mathsf{a})$ and $\Delta_2 = \beta(\mathsf{a},\mathsf{a})$. The critical peak is $\mathsf{f}(\mathsf{g}(\mathsf{b}),y_2) \leftarrow \mathsf{f}(\mathsf{g}(\mathsf{g}(\mathsf{a})),y_2) \to \mathsf{f}(\mathsf{g}(\mathsf{a}),y_2)$. It can be closed by simply applying rule δ at position 1 – as a proof term take $D' = \mathsf{f}(\delta, y_2)$. Since $\rho = \{y_1 \mapsto \mathsf{a}, y_2 \mapsto \mathsf{a}, x \mapsto \mathsf{g}(\mathsf{a})\}$ and $q_\beta = \epsilon$ we have $B[D'\rho]_{q_\beta} = D'\rho = \mathsf{f}(\delta,\mathsf{a})$ and $A \,/\, \Delta_1 = \alpha(\mathsf{b})$, and hence

$$\mathsf{src}^\sharp(B[D'\rho]_{q_\beta}) = \mathsf{f}(\mathsf{g}_{\delta^0}(\mathsf{b}_{\delta^1}),\mathsf{a}) \qquad\qquad \mathsf{src}^\sharp(A \,/\, \Delta_1) = \mathsf{f}_{\alpha^0}(\mathsf{g}_{\alpha^1}(\mathsf{b}),\mathsf{a}_{\alpha^1})$$

$$\blacktriangle'(A \,/\, \Delta_1, B[D'\rho]_{q_\beta}) = \blacktriangle(A \,/\, \Delta_1, B[D'\rho]_{q_\beta}) = 1$$

Note that the measure $\blacktriangle'$ did not decrease, showing that proving Theorem 7 in this way is impossible.

[2] This is easily verified using CSI [4] together with CeTA.

4.2 Formalized Proof

We found that keeping the measure ▲ and doing a simple case distinction in the inductive step suffices to show strong confluence of $\mathrel{-\!\!\circ\!\!\!\rightarrow}$.

Proof of Theorem 7 (Adaptations). The proof requires only minimal changes to the proof of Theorem 5. We only highlight the differences here. Assume $t \mathrel{\leftarrow\!\!\!\circ\!\!-} s \mathrel{-\!\!\circ\!\!\!\rightarrow} u$ and let A be a proof term representing $s \mathrel{-\!\!\circ\!\!\!\rightarrow} t$ and let B be a proof term representing $s \mathrel{-\!\!\circ\!\!\!\rightarrow} u$. We show $t \mathrel{-\!\!\circ\!\!\!\rightarrow} v \mathrel{{}^{*}\!\!\leftarrow} u$ for some term v by well-founded induction on the amount of overlap between A and B.

- Base case: Just like in the proof of Theorem 5 we obtain the residuals $A \,/\, B$ and $B \,/\, A$. Since $\mathsf{tgt}(A \,/\, B) = \mathsf{tgt}(B \,/\, A)$ and $\mathrel{-\!\!\circ\!\!\!\rightarrow} \subseteq \rightarrow^*$ this implies $t \mathrel{-\!\!\circ\!\!\!\rightarrow} v \mathrel{{}^{*}\!\!\leftarrow} u$ for $v = \mathsf{tgt}(A \,/\, B) = \mathsf{tgt}(B \,/\, A)$.
- Step case: Items 1–3 of the proof of Theorem 5 remain almost exactly the same. Since strong confluence is an asymmetric condition, we cannot simply assume without loss of generality that $q \leqslant p$. However, the two cases $q < p$ and $p < q$ still work as in the proof of Theorem 5 by constructing a proof term for $\mathsf{tgt}(\Delta_1) \mathrel{-\!\!\circ\!\!\!\rightarrow} \mathsf{tgt}(B \,/\, \Delta_2)$ and $\mathsf{tgt}(\Delta_2) \mathrel{-\!\!\circ\!\!\!\rightarrow} \mathsf{tgt}(A \,/\, \Delta_1)$ respectively and showing that the measure decreases for the new steps. In both cases this allows us to apply the induction hypothesis and obtain steps $t \mathrel{-\!\!\circ\!\!\!\rightarrow} v \mathrel{{}^{*}\!\!\leftarrow} u$. If $p = q$ then we have an overlay and the remainder of the proof changes as follows. A graphical representation of this case is displayed in Figure 1.
  4. By the almost development closedness assumption there exists a term v', a proof term D' witnessing $\mathsf{rhs}(\alpha)\tau \mathrel{-\!\!\circ\!\!\!\rightarrow} v'$, and a rewrite sequence $\mathsf{rhs}(\beta)\tau \rightarrow^* v'$.
  5. We define the substitution ρ as in item 5 of the previous proof and show that $B[D'\rho]_{q_\beta}$ witnesses a multi-step $t' \mathrel{-\!\!\circ\!\!\!\rightarrow} w$ for some term w.
  6. Again $\blacktriangle(A \,/\, \Delta_1, B[D'\rho]_{q_\beta}) < \blacktriangle(A, B)$ just like in the previous proof.
  7. We apply the induction hypothesis to obtain a term v, multi-step $t \mathrel{-\!\!\circ\!\!\!\rightarrow} v$, and rewrite sequence $w \rightarrow^* v$.
  8. It remains to show that there exists a rewrite sequence $u \rightarrow^* w$. Since $u = \mathsf{tgt}(B) = \mathsf{tgt}(B \,/\, \Delta_1)$ we know $u = \mathsf{tgt}(B[\mathsf{rhs}(\beta)\tau\rho]_{q_\beta})$ using properties of τ and ρ. Moreover since $w = \mathsf{tgt}(B[D'\rho]_{q_\beta})$ and $\mathsf{tgt}(D') = v'$ we know $w = \mathsf{tgt}(B[v'\rho]_{q_\beta})$ by an application of Lemma 2. From item 4 we know that there exists a rewrite sequence $\mathsf{rhs}(\beta)\tau \rightarrow^* v'$ so together with Lemma 3 we obtain the desired rewrite sequence $u \rightarrow^* w$. ◀

In the formalized proof we combined the cases $q = p$ and $q < p$ since in both cases steps 4–8 from the proof above can be applied, and dropping the additional case distinction saves a few lines of code.

4.3 Commutation

Theorem 7 can easily be extended to commutation. For proving commutation it is important to keep track of the underlying TRS for each proof term involved in the proof. In the formalization this is done via the predicate `wf_pterm` $\mathcal{R}$. The predicate checks whether all rule symbols belong to a certain TRS $\mathcal{R}$ (and whether the correct number of arguments is provided for each rule symbol). It is easy to see that whenever $A \in$ `wf_pterm` $\mathcal{R}_1$ and $B \in$ `wf_pterm` $\mathcal{R}_2$ and $A \,/\, B$ is defined then $A \,/\, B \in$ `wf_pterm` $\mathcal{R}_1$ ☑. Similar results hold for contexts and subsitutions of proof terms, e.g. if $A \in$ `wf_pterm` $\mathcal{R}_1$ and σ a substitution from variables to proof terms over $\mathcal{R}_1$ then $A\sigma \in$ `wf_pterm` $\mathcal{R}_1$.

▶ **Theorem 11.** *Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be left-linear* TRSs*. If*

1. *$s \mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}_2} \cdot {}_{\mathcal{R}_1}^{\;*}\!\!\leftarrow t$ for all critical pairs $s \;{}_{\mathcal{R}_1}\!\!\leftarrow \rtimes \rightarrow_{\mathcal{R}_2} t$, and*
2. *$s \mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}_1} t$ for all critical pairs $s \;{}_{\mathcal{R}_2}\!\!\leftarrow \rtimes \rightarrow_{\mathcal{R}_1} t$ which are not overlays*

then $\rightarrow_{\mathcal{R}_1}$ and $\rightarrow_{\mathcal{R}_2}$ commute. ☑

$$\begin{tikzcd}
s \arrow[rr, "\Delta_2"] \arrow[dddd, "\Delta_1"'] & & u' \arrow[r, "B \,/\, \Delta_2", "\circ" marking] & u \arrow[ddd, dashed, "*"] \\
& \mathsf{lhs}(\alpha)\tau = \mathsf{lhs}(\beta)\tau \arrow[r, "\beta"'] \arrow[d, "\alpha"] \arrow[dr, phantom, "\text{assumption}"] & \mathsf{rhs}(\beta)\tau \arrow[d, "*"] & \\
& \mathsf{rhs}(\alpha)\tau \arrow[r, "D'", "\circ" marking] & v' & \\
& & & \\
t' \arrow[rrr, dashed, "B[D'\rho]_{q_\beta}"', "\circ" marking] \arrow[d, "A \,/\, \Delta_1"', "\circ" marking] & & & w \arrow[d, dashed, "*"] \arrow[dll, phantom, "\text{IH}"] \\
t \arrow[rrr, dashed, "\circ" marking] & & & v
\end{tikzcd}$$

Figure 1 Overlay case in the proof of Theorem 7.

Proof (Adaptations). According to Lemma 1 it suffices to show strong commutation of $\mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}_1}$ and $\mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}_2}$. Assume $t \mathrel{\leftarrow\!\!\!\circ\!\!-}_{\mathcal{R}_1} s \mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}_2} u$ and let $A \in$ *wf_pterm* $\mathcal{R}_1$ be a proof term representing $s \mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}_1} t$ and let $B \in$ *wf_pterm* $\mathcal{R}_2$ be a proof term representing $s \mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}_2} u$. We show $t \mathrel{-\!\!\circ\!\!\!\rightarrow}_{\mathcal{R}_2} v \;{}_{\mathcal{R}_1}^{*}\!\!\leftarrow u$ for some term v by induction on $\blacktriangle(A, B)$. The base case now additionally requires that $A \,/\, B \in$ *wf_pterm* $\mathcal{R}_1$ and $B \,/\, A \in$ *wf_pterm* $\mathcal{R}_2$, which is easy to show as mentioned above. For the step case similar observations hold. In particular $B[D'\rho]_{q_\beta} \in$ *wf_pterm* $\mathcal{R}_2$ since by assumption $D' \in$ *wf_pterm* $\mathcal{R}_2$ and the substitution ρ maps to subterms of B which are also in *wf_pterm* $\mathcal{R}_2$. Hence all arrows pointing to the right in Figure 1 can be labeled with $\mathcal{R}_2$ and all arrows pointing down can be labeled with $\mathcal{R}_1$. Consequently, the proof of Theorem 7 can be followed again. ◀

5 Conclusion

We described extensions of our recent formalization of the development-closedness criterion to almost development closed critical pairs and commutation. During the process of formalizing these extensions we were able to simplify the formalization in [3] to the one presented here in Section 3. This version allowed for a straightforward adaptation to almost development closed critical pairs. The amount of Isabelle code before and after implementing the extension stayed roughly the same, since some previous results could be dropped while only one really new lemma (Lemma 3) had to be added in addition to the case distinction described in Section 4. Some more work was required to provide an executable "check"-function to integrate the result into CeTA.[3] Extending Theorem 7 to the commutation version (Theorem 11) was even more straightforward and required only minimal adaptations by providing more information about which proof term belongs to which of the two involved TRSs.

References

1 Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998. doi:10.1017/CBO9781139172752.

[3] ∼ 150 lines of Isabelle code for the check-function together with a proof that it corresponds to Theorem 7 ☑.

2 Christina Kohl and Aart Middeldorp. ProTeM: A proof term manipulator (system description). In Hélène Kirchner, editor, *Proc. 3rd International Conference on Formal Structures for Computation and Deduction*, volume 108 of *Leibniz International Proceedings in Informatics*, pages 31:1–31:8, 2018. doi:10.4230/LIPIcs.FSCD.2018.31.

3 Christina Kohl and Aart Middeldorp. A formalization of the development closedness criterion for left-linear term rewrite systems. In Robbert Krebbers, Dmitriy Traytel, Brigitte Pientka, and Steve Zdancewic, editors, *Proc. 12th International Conference on Certified Programs and Proofs*, pages 197–210, 2023. doi:10.1145/3573105.3575667.

4 Julian Nagele, Bertram Felgenhauer, and Aart Middeldorp. CSI: New evidence — a progress report. In Leonardo de Moura, editor, *Proc. 26th International Conference on Automated Deduction*, volume 10395 of *Lecture Notes in Artificial Intelligence*, pages 385–397, 2017. doi:10.1007/978-3-319-63046-5_24.

5 Julian Nagele and René Thiemann. Certification of confluence proofs using CeTA. In Takahito Aoto and Delia Kesner, editors, *Proc. 3rd International Workshop on Confluence*, pages 19–23, 2014. Available from http://cl-informatik.uibk.ac.at/iwc/iwc2014.pdf.

6 Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer, 2002. doi:10.1007/3-540-45949-9.

7 TeReSe, editor. *Term Rewriting Systems*, volume 55 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2003.

8 Yoshihito Toyama. Commutativity of term rewriting systems. In Kazuhiro Fuchi and Laurent Kott, editors, *Programming of Future Generation Computers II*, pages 393–407. North-Holland, 1988.

9 Vincent van Oostrom. Development closed critical pairs. In Gilles Dowek, Jan Heering, Karl Meinke, and Bernhard Möller, editors, *Proc. 2nd International Workshop on Higher-Order Algebra, Logic, and Term Rewriting*, volume 1074 of *Lecture Notes in Computer Science*, pages 185–200, 1995. doi:10.1007/3-540-61254-8_26.

10 Vincent van Oostrom. Developing developments. *Theoretical Computer Science*, 175(1):159–181, 1997. doi:10.1016/S0304-3975(96)00173-9.