Development Closed Critical Pairs: Towards a Formalized Proof

Christina Kohl[1] and Aart Middeldorp[1]

Department of Computer Science, University of Innsbruck, Austria
{christina.kohl,aart.middeldorp}@uibk.ac.at

Abstract

Having development closed critical pairs is a well-known sufficient condition for confluence of left-linear term rewrite systems. We present formalized results involving proof terms and unification that play an important role in the proof.

1 Introduction

In recent years several confluence criteria for first-order rewrite systems have been formalized in a proof assistant [3–5]. A well-known condition that has eluded all attempts so far is the result by van Oostrom [8] that a left-linear rewrite system is confluent if its critical pairs are development closed. In [1] it is suggested to use proof terms [7, Chapter 8] to obtain a rigorous proof. In [3] it is further suggested that a formalization of residual theory might be helpful. Here we pursue these suggestions further and present formalizations of several results that we believe will lead to a formal proof of the development closedness condition.

Our formalization is based on IsaFoR[1] and uses the existing formalizations of unification and critical pairs described in [6]. Our own development can be found at http://informatik-protem.uibk.ac.at/DC. To help readers negotiate the theory files we have annotated important results in this paper by a ☑-symbol which directly links to the HTML presentation of the corresponding result in our formalization.

2 Proof Terms

We use Greek letters for rule symbols which are used in proof terms. 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 $(x_1, \dots, x_n)$ of variables appearing in α in some fixed order. The length of this list is the arity of α. The list $\mathsf{varpos}(\alpha) = (p_1, \dots, p_n)$ denotes the corresponding variable positions in $\mathsf{lhs}(\alpha)$ such that $\mathsf{lhs}(\alpha)|_{p_i} = x_i$. Given a rule symbol α with $\mathsf{var}(\alpha) = (x_1, \dots, x_n)$ and terms $t_1, \dots, t_n$, we write $\langle t_1, \dots, t_n \rangle_\alpha$ 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 $\mathsf{st} \in \{\mathsf{src}, \mathsf{tgt}\}$:

$$\begin{aligned}
\mathsf{st}(x) &= x \\
\mathsf{st}(f(A_1, \dots, A_n)) &= f(\mathsf{st}(A_1), \dots, \mathsf{st}(A_n)) \\
\mathsf{src}(\alpha(A_1, \dots, A_n)) &= \mathsf{lhs}(\alpha)\langle \mathsf{src}(A_1), \dots, \mathsf{src}(A_n) \rangle_\alpha \\
\mathsf{tgt}(\alpha(A_1, \dots, A_n)) &= \mathsf{rhs}(\alpha)\langle \mathsf{tgt}(A_1), \dots, \mathsf{tgt}(A_n) \rangle_\alpha
\end{aligned}$$

Proof terms A and B are said to be *co-initial* if they have the same source. The proof term A can be seen as a witness of the multi-step $\mathsf{src}(A) \mathrel{-\!\!\circ\!\!\rightarrow} \mathsf{tgt}(A)$.For every multi-step there exists

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

a proof term witnessing it. In the setting of left-linear TRSs we can extend the definition of src to contexts of proof terms by adding the clause $\mathsf{src}(\Box) = \Box$. Doing the same for tgt or for arbitrary TRSs however could lead to more than one hole appearing in the result. The following result is an easy consequence of the idempotence of src and tgt.

Lemma 1. *For any substitution σ, proof term context C, and proof term A we have*

$$\mathsf{src}(A\sigma) = \mathsf{src}(\mathsf{src}(A)\sigma) \qquad \mathsf{tgt}(A\sigma) = \mathsf{tgt}(\mathsf{tgt}(A)\sigma)$$
$$\mathsf{src}(C[A]) = \mathsf{src}(C[\mathsf{src}(A)]) = \mathsf{src}(C)[\mathsf{src}(A)]) \qquad \mathsf{tgt}(C[A]) = \mathsf{tgt}(C[\mathsf{tgt}(A)])$$

For co-initial proof terms A and B we can define partial operations *residual* ($/$), *join* ($\sqcup$), and *deletion* ($-$). The residual $A \,/\, B$ is used to compute which redexes in A remain after contracting the redexes of B, $A \sqcup B$ is used to obtain a single proof term containing all redexes of A and B, and $A - B$ is used to delete the redexes of B from A. The definitions can be found in Appendix **??**. Straightforward induction proofs on the definitions yield the following result.

Lemma 2.
1. *If $A \,/\, B$ and $B \,/\, A$ are defined then $\mathsf{src}(B \,/\, A) = \mathsf{tgt}(A)$ and $\mathsf{tgt}(A \,/\, B) = \mathsf{tgt}(B \,/\, A)$.*
2. *If $A \star B$ is defined then $\mathsf{src}(A \star B) = \mathsf{src}(A) = \mathsf{src}(B)$ for $\star \in \{\sqcup, -\}$.*

The rules below can be used to compute joins, residuals, and deletions if the proof terms involved adhere to certain patterns.

Lemma 3. *Let $\star \in \{\sqcup, /, -\}$.*

1. $A \star \mathsf{src}(A) = A$
2. *If $A \star B = D$ then $C[A] \star \mathsf{src}(C)[B] = C[D]$ for any proof term context C.*
3. *If $\sigma(x) = \mathsf{src}(\tau(x))$ for all $x \in \mathcal{V}\mathsf{ar}(A)$ then $A\sigma \sqcup \mathsf{src}(A)\tau = A\tau$.*

Since the residual and deletion operations are not symmetric (as opposed to join) there is no obvious extension of the last item to $/$ and $-$.

3 Development Closed Critical Pairs

To show that a left-linear TRS is confluent if it is development closed it suffices to show that $\mathrel{-\!\!\circ\!\!\rightarrow}$ has the diamond property. A sketch of this proof is depicted in Figure 3. There the multi-step $s \mathrel{-\!\!\circ\!\!\rightarrow} t$ is witnessed by the proof term A, the multi-step $s \mathrel{-\!\!\circ\!\!\rightarrow} u$ is witnessed by the proof term B, and we need to show $t \mathrel{-\!\!\circ\!\!\rightarrow} v \mathrel{\leftarrow\!\!\circ\!\!-} u$ for some term v. The idea is to use well-founded induction on the amount of overlap between A and B. The case where A and B do not overlap is straightforward since then the proof terms $A \,/\, B$ and $B \,/\, A$ are well-defined and have the same target (Lemma 2). In the other case we can use the fact that the TRS is development closed to show that the co-initial proof terms $A \,/\, \Delta_1$ and $D \sqcup (B - \Delta_2) \,/\, \Delta_1$ can be constructed and that the overlap between these is less than between A and B. A key ingredient for the proof is the notion of an *innermost overlap* between A and B. Here an overlap is simply a pair of positions (p, q) such that the redex in A at position p overlaps with the redex in B at position q. An innermost overlap is one where no other overlap occurs below it. Formal definitions can be found in Appendix **??**.

Assuming that A and B have overlap, we select an innermost overlap (p, q) and assume $q \leqslant p$ without loss of generality. Now let $q' = p \backslash q$, $\mathsf{varpos}(\mathsf{lhs}(\alpha)) = (p_1, \ldots, p_n)$, $\mathsf{var}(\mathsf{lhs}(\alpha)) =$

$(x_1, \dots, x_n)$, $\mathsf{varpos}(\mathsf{lhs}(\beta)) = (q_1, \dots, q_m)$, and $\mathsf{var}(\mathsf{lhs}(\beta)) = (y_1, \dots, y_m)$. We assume without loss of generality $\mathcal{V}\mathsf{ar}(\mathsf{lhs}(\alpha)) \cap \mathcal{V}\mathsf{ar}(\mathsf{lhs}(\beta)) = \varnothing$ and define a substitution σ that maps the variables of $\mathsf{lhs}(\alpha)$ and $\mathsf{lhs}(\beta)$ to subterms of s such that $\mathsf{lhs}(\alpha)\sigma = s|_p$ and $\mathsf{lhs}(\beta)\sigma = s|_q$:

$$\sigma = \{\, x_i \mapsto s|_{pp_i} \mid 1 \leqslant i \leqslant n \,\} \cup \{\, y_j \mapsto s|_{qq_j} \mid 1 \leqslant j \leqslant m \,\}$$

Furthermore we can use Lemma **??** of Appendix **??** to obtain another substitution τ which is an mgu of $\mathsf{lhs}(\alpha)$ and $\mathsf{lhs}(\beta)|_{q'}$:

$$\begin{aligned}\tau = &\{\, x_i \mapsto \mathsf{lhs}(\beta)|_{q'p_i} \mid 1 \leqslant i \leqslant n \text{ and } q'p_i \in \mathcal{P}\mathsf{os}(\mathsf{lhs}(\beta)) \,\} \cup \\ &\{\, y_j \mapsto \mathsf{lhs}(\alpha)|_{q_j \backslash q'} \mid 1 \leqslant j \leqslant m \text{ and } q_j \backslash q' \in \mathcal{P}\mathsf{os}_{\mathcal{F}}(\mathsf{lhs}(\alpha)) \,\}\end{aligned}$$

Hence we obtain the critical peak

$$\mathsf{lhs}(\beta)[\mathsf{rhs}(\alpha)\tau]_{q'} \xleftarrow[\alpha]{q'} \mathsf{lhs}(\beta)[\mathsf{lhs}(\alpha)\tau]_{q'} = \mathsf{lhs}(\beta)\tau \xrightarrow[\beta]{\epsilon} \mathsf{rhs}(\beta)\tau$$ ☑

Assuming that the given TRS is development closed, we know there exists a multi-step $\mathsf{lhs}(\beta)[\mathsf{rhs}(\alpha)\tau]_{q'} \mathrel{\circ\!\!\!\!\!\twoheadrightarrow} \mathsf{rhs}(\beta)\tau$. Let D' be the proof term representation of such a multi-step and define $D = s[D'\sigma]_q$. Then we can prove the following result.

Lemma 4. *The proof term D witnesses the multi-step* $\mathsf{tgt}(\Delta_1) \mathrel{\circ\!\!\!\!\!\twoheadrightarrow} \mathsf{tgt}(\Delta_2)$. ☑

Ultimately we need to also show that $D \sqcup (B - \Delta_2) \,/\, \Delta_1$ is well-defined and witnesses $\mathsf{tgt}(\Delta_1) \mathrel{\circ\!\!\!\!\!\twoheadrightarrow} \mathsf{tgt}(B)$. For this purpose we introduce another substitution ρ:

$$\rho = \{\, y_j \mapsto B_j \mid 1 \leqslant j \leqslant m \,\} \cup \{\, x_i \mapsto \mathsf{lhs}(\beta)\langle B_1, \dots, B_m\rangle_\beta|_{q'p_i} \mid 1 \leqslant i \leqslant n \,\}$$

Note the similarity to σ: ρ maps to subterms of B while σ maps to the sources of these proof terms. The key property that makes ρ useful for computing $(B - \Delta_2) \,/\, \Delta_1$ is the following:

Lemma 5. *If $1 \leqslant j \leqslant m$ then $\tau(y_j)\rho = B_j$.* ☑

Proof. We distinguish two cases: $\tau(y_j) = y_j$ and $\tau(y_j) \neq y_j$. In the first case we immediately obtain $\tau(y_j)\rho = \rho(y_j) = B_j$ from the definition of ρ. For the second case first observe that if all function symbols of $\mathsf{lhs}(\alpha)$ also appear in $\mathsf{lhs}(\beta)\langle B_1, \dots, B_m\rangle_\beta|_{q'}$ (i.e., no rule symbols are in the way) then it follows from the definition of ρ that

$$\mathsf{lhs}(\alpha)\rho = \mathsf{lhs}(\beta)\langle B_1, \dots, B_m\rangle_\beta|_{q'} \tag{$*$}$$

Checking that all function symbols of $\mathsf{lhs}(\alpha)$ also appear in $\mathsf{lhs}(\beta)\langle B_1, \dots, B_m\rangle_\beta|_{q'}$ can be done by verifying

$$p' \in \mathcal{P}\mathsf{os}_{\mathcal{F}}(\mathsf{lhs}(\alpha)) \quad\Longrightarrow\quad \mathsf{src}^\sharp(\mathsf{lhs}(\beta)\langle B_1, \dots, B_m\rangle_\beta|_{q'})(p') \text{ is unlabeled}$$ ☑

which relies on the fact that having a labeled function symbol at such a position p' would contradict the assumption that (p, q) is an innermost overlap of A and B. With $(*)$ we obtain $\tau(y_j)\rho = \mathsf{lhs}(\alpha)|_{q_j \backslash q'}\rho = (\mathsf{lhs}(\beta)\langle B_1, \dots, B_m\rangle_\beta|_{q'})|_{q_j \backslash q'} = \mathsf{lhs}(\beta)\langle B_1, \dots, B_m\rangle_\beta|_{q_j} = B_j$. □

The term $s = \mathsf{src}(A) = \mathsf{src}(B)$ contains a redex with respect to β at position q. In the following we denote by q_β the corresponding position of the rule symbol β in the proof term B, i.e., the position q_β such that $B = B[\beta(B_1, \dots, B_m)]_{q_\beta}$ and $\mathsf{src}(B)[\ ]_q = \mathsf{src}(B[\ ]_{q_\beta})$. It can be shown that such a position exists for arbitrary proof terms B and positions q where $\mathsf{src}^\sharp(B)(q) = \beta^0$. ☑

Lemma 6. *1.* $D \sqcup (B - \Delta_2) \,/\, \Delta_1 = B[D'\rho]_{q_\beta}$ ☑

2. $D \sqcup (B - \Delta_2) \,/\, \Delta_1$ *witnesses* $\mathsf{tgt}(\Delta_1) \mathrel{\circ\!\!\!\!\longrightarrow} \mathsf{tgt}(B)$ ☑ ☑

Proof. From Lemma 3 we obtain $B - \Delta_2 = B[\mathsf{lhs}(\beta)\langle B_1, \ldots, B_m\rangle_\beta]_{q_\beta}$ and with Lemma 5 we further obtain $B[\mathsf{lhs}(\beta)\langle B_1, \ldots, B_m\rangle_\beta]_{q_\beta} = B[\mathsf{lhs}(\beta)\tau\rho]_{q_\beta} = B[\mathsf{lhs}(\beta)[\mathsf{lhs}(\alpha)\tau]_{q'}\rho]_{q_\beta}$. Another application of Lemma 3 yields $(B - \Delta_2) \,/\, \Delta_1 = B[\mathsf{lhs}(\beta)[\mathsf{rhs}(\alpha)\tau]_{q'}\rho]_{q_\beta}$. From Lemma 3(3) we obtain $D'\sigma \sqcup \mathsf{lhs}(\beta)[\mathsf{rhs}(\alpha)\tau]_{q'}\rho = D'\rho$ and since $\mathsf{src}(B[\;]_{q_\beta}) = s[\;]_q$ and $D = s[D'\sigma]_q$ we can apply Lemma 3(2) (modulo symmetry of $\sqcup$) to obtain the desired $D \sqcup (B - \Delta_2) \,/\, \Delta_1 = B[D'\rho]_{q_\beta}$. From Lemma 2 and Lemma 4 we obtain $\mathsf{src}((B - \Delta_2) \,/\, \Delta_1) = \mathsf{tgt}(\Delta_1) = \mathsf{src}(D)$ and hence $\mathsf{src}(D \sqcup (B - \Delta_2) \,/\, \Delta_1) = \mathsf{tgt}(\Delta_1)$. It remains to show that $\mathsf{tgt}(D \sqcup (B - \Delta_2) \,/\, \Delta_1) = \mathsf{tgt}(B)$. We have

$$\begin{aligned}
\mathsf{tgt}(D \sqcup (B - \Delta_2) \,/\, \Delta_1) &= \mathsf{tgt}(B[D'\rho]_{q_\beta}) \\
&= \mathsf{tgt}(B[\mathsf{tgt}(\mathsf{rhs}(\beta)\tau\rho)]_{q_\beta}) && \text{(Lemma 1 and definition of } D'\text{)} \\
&= \mathsf{tgt}(B[\mathsf{tgt}(\mathsf{rhs}(\beta)\langle B_1, \ldots, B_m\rangle_\beta)]_{q_\beta}) && \text{(Lemma 5)} \\
&= \mathsf{tgt}(B[\beta(B_1, \ldots, B_m)]_{q_\beta}) && \text{(Lemma 1)} \\
&= \mathsf{tgt}(B) && \square
\end{aligned}$$

In order to apply the induction hypothesis and to conclude the proof in Figure 3 it remains to show that the amount of overlap between the proof terms $A \,/\, \Delta_1$ and $D \sqcup (B - \Delta_2) \,/\, \Delta_1$ is less than the amount of overlap between A and B. Like the proof of Lemma 5 this relies on the fact that we chose an innermost overlap (p, q) during the construction of D. At the time of writing the formalization of this fact is still work in progress.

The example below illustrates the constructions of Lemma 6 for specific proof terms A and B. It can be retraced in the tool ProTeM [2] where we implemented all important operations.

Example 7. Consider the left-linear and development closed TRS $\mathcal{R}$ consisting of the rules

$$\boldsymbol{\alpha}\colon \mathsf{f}(x_1, \mathsf{g}(x_2)) \to \mathsf{f}(x_1, \mathsf{g}(x_1)) \qquad \boldsymbol{\beta}\colon \mathsf{f}(\mathsf{g}(y_1), y_2) \to \mathsf{f}(\mathsf{g}(y_1), \mathsf{g}(y_1)) \qquad \boldsymbol{\gamma}\colon \mathsf{g}(\mathsf{a}) \to \mathsf{g}(\mathsf{b}) \qquad \boldsymbol{\delta}\colon \mathsf{b} \to \mathsf{a}$$

and the proof terms $A = \mathsf{g}(\boldsymbol{\alpha}(\boldsymbol{\gamma}, \mathsf{a}))$ and $B = \mathsf{g}(\boldsymbol{\beta}(\mathsf{a}, \boldsymbol{\gamma}))$. We have $\mathsf{src}(A) = \mathsf{src}(B) = \mathsf{g}(\mathsf{f}(\mathsf{g}(\mathsf{a}), \mathsf{g}(\mathsf{a})))$ and $\mathsf{overlaps}(A, B) = \{(1, 1), (1, 12), (11, 1)\}$ where both the second and third overlap are innermost. For the overlap $(11, 1)$ we obtain the substitution $\tau = \{y_1 \mapsto \mathsf{a}\}$ with corresponding critical peak

$$\mathsf{f}(\mathsf{g}(\mathsf{b}), y_2) \xleftarrow[\gamma]{1} \mathsf{f}(\mathsf{g}(\mathsf{a}), y_2) \xrightarrow[\beta]{\epsilon} \mathsf{f}(\mathsf{g}(\mathsf{a}), \mathsf{g}(\mathsf{a}))$$

This critical peak can be closed by applying β at the root and δ at position 11 in the term $\mathsf{f}(\mathsf{g}(\mathsf{b}), y_2)$ as witnessed by the proof term $D' = \boldsymbol{\beta}(\boldsymbol{\delta}, y_2)$. Since $\sigma = \{y_1 \mapsto \mathsf{a},\ y_2 \mapsto \mathsf{g}(\mathsf{a})\}$ we have $D = s[D'\sigma]_1 = s[\boldsymbol{\beta}(\boldsymbol{\delta}, \mathsf{g}(\mathsf{a}))]_1 = \mathsf{g}(\boldsymbol{\beta}(\boldsymbol{\delta}, \mathsf{g}(\mathsf{a})))$. Furthermore, $\Delta_1 = \mathsf{g}(\mathsf{f}(\boldsymbol{\gamma}, \mathsf{g}(\mathsf{a})))$, $\Delta_2 = \mathsf{g}(\boldsymbol{\beta}(\mathsf{a}, \mathsf{g}(\mathsf{a})))$, $\rho = \{y_1 \mapsto \mathsf{a},\ y_2 \mapsto \boldsymbol{\gamma}\}$ and hence

$$\begin{aligned}
B - \Delta_2 &= \mathsf{g}(\mathsf{f}(\mathsf{g}(\mathsf{a}), \boldsymbol{\gamma})) = B[\mathsf{lhs}(\beta)\tau\rho]_1 \\
(B - \Delta_2) \,/\, \Delta_1 &= \mathsf{g}(\mathsf{f}(\mathsf{g}(\mathsf{b}), \boldsymbol{\gamma})) = B[\mathsf{lhs}(\beta)[\mathsf{rhs}(\gamma)\tau]_1\rho]_1 \\
D \sqcup (B - \Delta_2) \,/\, \Delta_1 &= \mathsf{g}(\boldsymbol{\beta}(\boldsymbol{\delta}, \boldsymbol{\gamma})) \quad\;\; = B[D'\rho]_1
\end{aligned}$$

For the non-innermost overlap $(1, 1)$ the term $(B - \Delta_2) \,/\, \Delta_1$ as well as the substitution ρ are not well-defined. We have $\Delta_1 = \mathsf{g}(\boldsymbol{\alpha}(\mathsf{g}(\mathsf{a}), \mathsf{a}))$ and $\Delta_2 = \mathsf{g}(\boldsymbol{\beta}(\mathsf{a}, \mathsf{g}(\mathsf{a})))$ and hence $B - \Delta_2 = s[(\mathsf{f}(\mathsf{g}(\mathsf{a}), \boldsymbol{\gamma}))]_1$. Since $\mathsf{f}(\mathsf{g}(\mathsf{a}), \boldsymbol{\gamma})$ does not match $\mathsf{lhs}(\alpha)$ the result of $(B - \Delta_2) \,/\, \Delta_1$ is undefined. Also the substitution ρ cannot be computed since the variable binding $x_2 \mapsto \mathsf{lhs}(\beta)\langle B_1, \ldots, B_m\rangle_\beta|_{21} = \mathsf{f}(\mathsf{g}(\mathsf{a}), \boldsymbol{\gamma})|_{21}$ does not make sense.

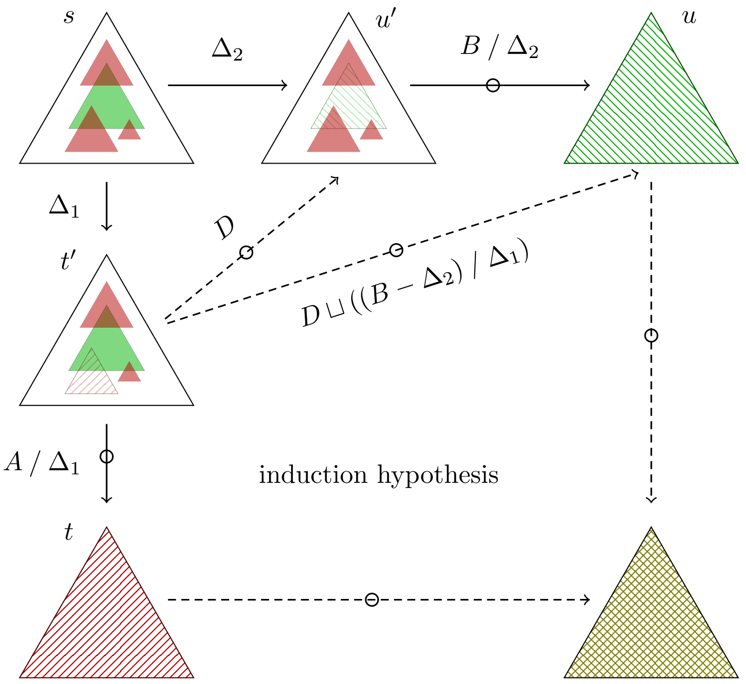

Figure 1: Picture proof.

References

[1] Nao Hirokawa and Aart Middeldorp. Commutation via relative termination. In *Proc. 2th IWC*, pages 29–33, 2013.

[2] Christina Kohl and Aart Middeldorp. ProTeM: A proof term manipulator (system description). In *Proc. 3rd FSCD*, volume 108 of *LIPIcs*, pages 31:1–31:8, 2018. doi:10.4230/LIPIcs.FSCD.2018.31.

[3] Julian Nagele and Aart Middeldorp. Certification of classical confluence results for left-linear term rewrite systems. In *Proc. 7th ITP*, volume 9807 of *LNCS*, pages 290–306, 2016. doi:10.1007/978-3-319-43144-4_18.

[4] Julian Nagele and Harald Zankl. Certified rule labeling. In *Proc. 26th RTA*, volume 36 of *LIPIcs*, pages 269–284, 2015. doi:10.4230/LIPIcs.RTA.2015.269.

[5] Ana Cristina Rocha-Oliveira, André Luiz Galdino, and Mauricio Ayala-Rincón. Confluence of orthogonal term rewriting systems in the prototype verification system. *Journal of Automated Reasoning*, 58(2):231–251, 2017. doi:10.1007/s10817-016-9376-2.

[6] Christian Sternagel and René Thiemann. Formalizing Knuth–Bendix orders and Knuth–Bendix completion. In *Proc. 23rd RTA*, volume 21 of *LIPIcs*, pages 287–302, 2013. doi:10.4230/LIPIcs.RTA.2013.287.

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

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