Certification of Classical Confluence Results for Left-Linear Term Rewrite Systems

Julian Nagele(✉) and Aart Middeldorp

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

Abstract. This paper presents the first formalization of three classic confluence criteria for first-order term rewrite systems by Huet and Toyama. We have formalized proofs, showing that (1) linear strongly closed systems, (2) left-linear parallel closed systems, and (3) left-linear almost parallel closed systems are confluent. The third result is extended to commutation. The proofs were carried out in the proof assistant Isabelle/HOL as part of the library IsaFoR and integrated into the certifier CeTA, significantly increasing the number of certifiable proofs produced by automatic confluence tools.

1 Introduction

Confluence of rewrite systems is an important property, which is intimately connected to uniqueness of normal forms, and hence to determinism of programs. In recent years there has been tremendous progress in establishing confluence or non-confluence of TRSs automatically, with a number of tools under active development, like ACP [2], Saigawa [8,11], CoLL [18], and our own tool, CSI [23].

The recent achievements in confluence research have enabled a competition[1] where such automated tools try to establish/refute confluence. As the proofs produced by these tools are often complicated and large, there is interest in checking them with trustable certifiers like CeTA [21]. (CeTA is a certifier for termination, confluence and complexity proofs for TRSs. Other certifiers exist for termination proofs, notably Rainbow [4] and CiME3 [5].) Given a certificate in CPF (certification problem format) [19], CeTA will either answer CERTIFIED or return a detailed error message why the proof was REJECTED. Its correctness is formally proven as part of IsaFoR, the Isabelle Formalization of Rewriting. IsaFoR contains executable "check"-functions for each formalized proof technique together with formal proofs that whenever such a check succeeds, the technique was indeed applied correctly. Isabelle's code-generation facility is used to obtain a trusted Haskell program from these check functions: the certifier CeTA.[2]

In the recent past, several confluence results have been formalized, starting from the fundamental result by Knuth and Bendix [12] that a terminating

This work is supported by FWF (Austrian Science Fund) project P27528.

[1] http://coco.nue.riec.tohoku.ac.jp/.

[2] IsaFoR/CeTA and CPF are available at http://cl-informatik.uibk.ac.at/software/ceta/.

J.C. Blanchette and S. Merz (Eds.): ITP 2016, LNCS 9807, pp. 290–306, 2016.
DOI: 10.1007/978-3-319-43144-4_18

rewrite system is confluent if and only if all its critical pairs are joinable. For non-terminating rewrite systems, weak orthogonality as well as sufficient conditions for non-joinability of critical pairs based on unification, discrimination pairs [1], interpretations, and tree automata [6] have been formalized. These results are described in [14]. More recently, redundant rules [13] and rule labeling [15] increased the number of certifiable confluence proofs significantly.

In this paper we report on the formalization of three classical confluence results. Two of these are due to Huet [10] and presented in full detail in the textbook of Baader and Nipkow [3, Lemma 6.3 and Sect. 6.4]. The third result is due to Toyama [22].

The remainder of this paper is organized as follows. After recalling basic notions of term rewriting in the next section, in Sect. 3 we report on the formalization of the result that linear strongly closed rewrite systems are confluent. Linearity is an important limitation, but the result does have its uses [7]. Section 4 is devoted to the formalization of the result of Huet that a left-linear rewrite system is confluent if its critical pairs are parallel closed. In Sect. 5 we consider Toyama's generalization of the previous result. Apart from a weaker joinability requirement on overlays, the result is extended to the commutation of two rewrite systems. Our formalization is an important first step for the certification of confluence proofs produced by CoLL [18], which is based on commutation. In Sect. 6 we explain what is needed for the automatic certification of confluence proofs that employ the formalized techniques and we present experimental results. In the final section we conclude with an outlook on future work, in particular the challenges that need to be overcome when extending the results from parallel closed rewrite systems to development closed higher-order rewrite systems [17]. The main Isabelle theories developed and integrated into IsaFoR are `Strongly_Closed.thy`, for the result on strongly closed rewrite systems, `Parallel_Closed.thy` for results on (almost) parallel closed systems (where we make heavy use of multihole contexts, cf. `Multihole_Context.thy`), and `Critical_Pair_Closure_Impl.thy` for the executable check functions.

2 Preliminaries

We assume familiarity with the basics of rewriting [3,20]. Knowledge of Isabelle [16] is not essential but experience with an interactive theorem prover might be helpful.

Let $\mathcal{F}$ be a signature and $\mathcal{V}$ a set of variables disjoint from $\mathcal{F}$. By $\mathcal{T}(\mathcal{F},\mathcal{V})$ we denote the set of terms over $\mathcal{F}$ and $\mathcal{V}$. Positions are strings of positive natural numbers, i.e., elements of $\mathbb{N}_+^*$. We write $q \leqslant p$ if $qq' = p$ for some position q', in which case $p \backslash q$ is defined to be q'. Furthermore $q < p$ if $q \leqslant p$ and $q \neq p$. Finally, positions q and p are parallel, written as $q \parallel p$, if neither $q \leqslant p$ nor $p < q$. Positions are used to address subterm occurrences. The set of positions of a term t is defined as $\mathcal{P}\mathsf{os}(t) = \{\epsilon\}$ if t is a variable and as $\mathcal{P}\mathsf{os}(t) = \{\epsilon\} \cup \{iq \mid 1 \leqslant i \leqslant n \text{ and } q \in \mathcal{P}\mathsf{os}(t_i)\}$ if $t = f(t_1,\ldots,t_n)$. The subterm of t at position $p \in \mathcal{P}\mathsf{os}(t)$ is defined as $t|_p = t$ if $p = \epsilon$ and as $t|_p = t_i|_q$ if $p = iq$ and $t = f(t_1,\ldots,t_n)$. We write $s[t]_p$ for the result of replacing the subterm at position

p of s with t. The size of a term t, i.e., the size of $\mathcal{P}\mathsf{os}(t)$, is denoted by $|t|$. We write $\mathcal{V}\mathsf{ar}(t)$ for the set of variables occurring in the term t. A term t is linear if every variable occurs at most once in it. A substitution is a mapping σ from $\mathcal{V}$ to $\mathcal{T}(\mathcal{F}, \mathcal{V})$ such that its domain $\{x \in \mathcal{V} \mid \sigma(x) \neq x\}$ is finite. We write $t\sigma$ for the result of applying σ to the term t.

Assume a fresh symbol $\square$, called hole. A *multihole* context is a term that may contain an arbitrary number of holes. Filling the holes in a multihole context C with terms $t_1, \ldots, t_n$ is written as $C[t_1, \ldots, t_n]$. (At this point we mention that in the formalization we of course have to make sure that the number of terms n matches the number of holes in C. To ease readability we usually do not make this explicit.) A term with exactly one hole is just called context and we also write $s[]_p$ for the context obtained by replacing position p in s by the hole. If $C[s] = t$ for some context C then s is called a subterm of t and we write $s \trianglelefteq t$. If additionally $C \neq \square$ then s is a proper subterm of t, which is denoted by $s \triangleleft t$.

A rewrite rule is a pair of terms (ℓ, r), written $\ell \to r$.[3] A rewrite rule $\ell \to r$ is left-linear if ℓ is linear, right-linear if r is linear, and linear if it is both left- and right-linear. A variant of a rewrite rule is obtained by renaming its variables. A term rewrite system (TRS) is set of rewrite rules over a signature. In the sequel, signatures are left implicit. A TRS is (left-)linear if all its rules are (left-)linear. A rewrite relation is a binary relation on terms that is closed under contexts and substitutions. For a TRS $\mathcal{R}$ we define $\to_{\mathcal{R}}$ (often written as $\to$) to be the smallest rewrite relation that contains $\mathcal{R}$. As usual $\to^=$ and $\to^*$ denote the reflexive, and reflexive and transitive closure of $\to$, respectively.

A relation $\to$ is said to have the diamond property if $\leftarrow \cdot \to \; \subseteq \; \to \cdot \leftarrow$ and is called confluent if its reflexive transitive closure has the diamond property. It is strongly confluent if $\leftarrow \cdot \to \; \subseteq \; \to^= \cdot {}^*\!\leftarrow$. The results in Sect. 5 will be proved in the more general setting of commutation. Two relations $\to_1$ and $\to_2$ commute if ${}_1^*\!\leftarrow \cdot \to_2^* \; \subseteq \; \to_2^* \cdot {}_1^*\!\leftarrow$, they strongly commute if ${}_1\!\leftarrow \cdot \to_2 \; \subseteq \; \to_2^= \cdot {}_1^*\!\leftarrow$. The following lemma captures the well-known connections between the diamond property, (strong) confluence and (strong) commutation.

Lemma 1. *Let $\to$, $\to_1$, $\to_2$, $\to_{1'}$, and $\to_{2'}$ be binary relations.*

1. *If $\to$ has the diamond property then it is confluent.*
2. *If $\to$ is strongly confluent then it is confluent.*
3. *If $\to_1$ and $\to_2$ strongly commute then they commute.*
4. *If $\to$ commutes with itself then it is confluent.*
5. *If $\to_1 \; \subseteq \; \to_{1'} \; \subseteq \; \to_1^*$ and $\to_{1'}$ is confluent then $\to_1$ is confluent.*
6. *If $\to_1 \; \subseteq \; \to_{1'} \; \subseteq \; \to_1^*$ and $\to_2 \; \subseteq \; \to_{2'} \; \subseteq \; \to_2^*$ and $\to_{1'}$ and $\to_{2'}$ commute then $\to_1$ and $\to_2$ commute.*

Later, when applying the last two statements, the relations $\to_{1'}$ and $\to_{2'}$ between one and many step rewriting that we will use is parallel rewriting.

[3] We do not impose the common *variable conditions*, i.e., the restriction that ℓ is not a variable and all variables in r are contained in ℓ.

Definition 1. *For a TRS* $\mathcal{R}$*, the* parallel rewrite relation $\mathrel{+\!\!\!\!\to}_{\mathcal{R}}$ *is defined inductively by*

- $x \mathrel{+\!\!\!\!\to}_{\mathcal{R}} x$ *if* x *is a variable,*
- $\ell\sigma \mathrel{+\!\!\!\!\to}_{\mathcal{R}} r\sigma$ *if* $\ell \to r \in \mathcal{R}$*, and*
- $f(s_1, \dots, s_n) \mathrel{+\!\!\!\!\to}_{\mathcal{R}} f(t_1, \dots, t_n)$ *if* f *is a function symbol of arity* n *and* $s_i \mathrel{+\!\!\!\!\to}_{\mathcal{R}} t_i$ *for all* $1 \leqslant i \leqslant n$.

The following properties of parallel rewriting are well-known and follow by straight-forward induction proofs.

Lemma 2. *The following properties of* $\mathrel{+\!\!\!\!\to}$ *hold:*

- $\to_{\mathcal{R}} \subseteq \mathrel{+\!\!\!\!\to}_{\mathcal{R}} \subseteq \to^*_{\mathcal{R}}$,
- $s \mathrel{+\!\!\!\!\to}_{\mathcal{R}} s$ *for all terms* s,
- *if* $x\sigma \mathrel{+\!\!\!\!\to}_{\mathcal{R}} x\tau$ *for all* $x \in \mathcal{V}\mathsf{ar}(s)$ *then* $s\sigma \mathrel{+\!\!\!\!\to}_{\mathcal{R}} s\tau$.

The confluence results formalized in this work are based on (left-)linearity and restricted joinability of critical pairs. Critical pairs arise from situations where two redexes overlap with each other. The definition we use here is slightly non-standard in two regards. First we consider critical pairs for two rewrite systems to use them in a commutation setting later on. Second we do not exclude root overlaps of a rule with (a variant of) itself as is commonly done. This allows us to dispense with the variable condition that all variables in the right-hand side of a rule must also occur on the left. Moreover, if a TRS does satisfy the condition then all extra critical pairs that would normally be excluded are trivial.

A critical overlap $(\ell_1 \to r_1, C, \ell_2 \to r_2)_\mu$ of two TRSs $\mathcal{R}_1$ and $\mathcal{R}_2$ consists of variants $\ell_1 \to r_1$ and $\ell_2 \to r_2$ of rewrite rules in $\mathcal{R}_1$ and $\mathcal{R}_2$ without common variables, a context C, such that $\ell_2 = C[\ell']$ with $\ell' \notin \mathcal{V}$ and a most general unifier μ of ℓ_1 and ℓ'. From a critical overlap $(\ell_1 \to r_1, C, \ell_2 \to r_2)_\mu$ we obtain a critical peak $C\mu[r_1\mu] \;{}_{\mathcal{R}_1}\!\!\leftarrow C\mu[\ell_1\mu] \to_{\mathcal{R}_2} r_2\mu$ and the corresponding critical pair $C\mu[r_1\mu] \;{}_{\mathcal{R}_1}\!\!\leftarrow\!\rtimes\!\rightarrow_{\mathcal{R}_2} r_2\mu$. If $C = \Box$, the corresponding critical pair is called an overlay and written as $r_1\mu \;{}_{\mathcal{R}_1}\!\!\leftarrow\!\bowtie\!\rightarrow_{\mathcal{R}_2} r_2\mu$, otherwise it is called an inner critical pair, and denoted using ${}_{\mathcal{R}_1}\!\!\leftarrow\!\cdot\!\!\rtimes\!\rightarrow_{\mathcal{R}_2}$. When considering the critical pairs of a TRS $\mathcal{R}$ with itself we drop the subscripts and write $\leftarrow\!\rtimes\!\rightarrow$ instead of ${}_{\mathcal{R}}\!\!\leftarrow\!\rtimes\!\rightarrow_{\mathcal{R}}$.

3 Strongly Closed Critical Pairs

The first confluence criterion we consider is due to Huet [10] and based on the observation that in a linear rewrite system it suffices to have strong-confluence like joins for all critical pairs in order to guarantee strong confluence of the rewrite system. A preliminary version of the formalization described in this section was reported in [14].

Definition 2. *A TRS* $\mathcal{R}$ *is* strongly closed *if every critical pair* $s \leftarrow\!\rtimes\!\rightarrow t$ *of* $\mathcal{R}$ *satisfies both* $s \to^{=} \cdot {}^{*}\!\!\leftarrow t$ *and* $s \to^{*} \cdot {}^{=}\!\!\leftarrow t$.

The following folklore lemma tells us that in a linear term applying a substitution can be done by replacing the one subterm where the variable occurs and applying the remainder of the substitution.

Lemma 3. *Let t be a linear term and let $p \in \mathcal{P}\mathsf{os}(t)$ be a position with $t|_p = x$. Then for substitutions σ and τ with $\sigma(y) = \tau(y)$ for all $y \in \mathcal{V}\mathsf{ar}(t)$ different from x we have $t\tau = t\sigma[\tau(x)]_p$.*

The proof that linear strongly closed systems are strongly confluent is very similar to the one of the famous critical pair lemma, by analyzing the relative positions of the rewrite steps in a peak. The next lemma, which appears implicitly in Huet's proof of Corollary 1, takes care of the case where one position is above the other.

Lemma 4. *Let $\mathcal{R}$ be a linear, strongly closed TRS and assume $s \to_{\mathcal{R}} t$ with rule $\ell_1 \to r_1$ and substitution σ_1 at position p_1 and let $s \to_{\mathcal{R}} u$ with rule $\ell_2 \to r_2$ and substitution σ_2 at position p_2 with $p_1 \leqslant p_2$. Then there are terms v and w with $t \to_{\mathcal{R}}^{*} v \mathrel{{}_{\mathcal{R}}^{=}\!\!\leftarrow} u$ and $t \to_{\mathcal{R}}^{=} w \mathrel{{}_{\mathcal{R}}^{*}\!\!\leftarrow} u$.*

Proof (Sketch). Since the proof is standard and the formalization closely follows the paper proof, we only sketch the idea and refer to the formalization for full details. We distinguish whether the step from s to u overlaps with the one from s to t or takes place in the substitution. If there is a critical pair, we can close it by the assumption that the system is strongly closed. If the step from s to u happens in the substitution we can join in the required shape due to linearity of $\mathcal{R}$, which avoids duplication of the redex, by using Lemma 3.

Now the main result of this section follows easily.

Corollary 1 (Huet [10]). *If a TRS $\mathcal{R}$ is linear and strongly closed then $\to_{\mathcal{R}}$ is strongly confluent.*

Proof. Assume $s \to_{\mathcal{R}} t$ and $s \to_{\mathcal{R}} u$. Then there are positions $p_1, p_2 \in \mathcal{P}\mathsf{os}(s)$, substitutions σ_1, σ_2 and rules $\ell_1 \to r_1$, $\ell_2 \to r_2$ in $\mathcal{R}$ with $s|_{p_1} = \ell_1\sigma_1$, $s|_{p_2} = \ell_2\sigma_2$ and $t = s[r_1\sigma_1]_{p_1}$, $u = s[r_2\sigma_2]_{p_2}$. We show existence of a term v with $t \to^* v$ and $u \to^= v$ by analyzing the positions p_1 and p_2. If they are parallel then $t \to t[r_2\sigma_2]_{p_2} = u[r_1\sigma_1]_{p_1} \leftarrow u$. If they are not parallel then one is above the other. In both cases we conclude by Lemma 4.

Then by Lemma 1 $\mathcal{R}$ is also confluent.

Example 1. Consider the TRS $\mathcal{R}$ consisting of the two rewrite rules

$$\mathsf{f}(\mathsf{f}(x,y),z) \to \mathsf{f}(x,\mathsf{f}(y,z)) \qquad\qquad \mathsf{f}(x,y) \to \mathsf{f}(y,x)$$

There are four non-trivial critical pairs

$$\begin{array}{cc}
\mathsf{f}(\mathsf{f}(x,\mathsf{f}(y,z)),v) \leftarrow\!\rtimes\!\to \mathsf{f}(\mathsf{f}(x,y),\mathsf{f}(z,v)) & \mathsf{f}(x,\mathsf{f}(y,z)) \leftarrow\!\rtimes\!\to \mathsf{f}(z,\mathsf{f}(x,y)) \\
\mathsf{f}(z,\mathsf{f}(x,y)) \leftarrow\!\rtimes\!\to \mathsf{f}(x,\mathsf{f}(y,z)) & \mathsf{f}(\mathsf{f}(y,x),z) \leftarrow\!\rtimes\!\to \mathsf{f}(x,\mathsf{f}(y,z))
\end{array}$$

Since $\mathcal{R}$ is linear and all critical pairs are strongly closed, $\mathcal{R}$ is confluent.

The next example shows how to apply the criterion to a TRS that does not fulfill the variable conditions.

Example 2. Consider the linear TRS $\mathcal{R}$ consisting of the following three rules:

$$\mathsf{a} \to \mathsf{f}(x) \qquad \mathsf{f}(x) \to \mathsf{b} \qquad x \to \mathsf{f}(\mathsf{g}(x))$$

There are five critical pairs modulo symmetry:

$$\begin{array}{ccc} \mathsf{f}(y) \leftarrow\!\rtimes\!\rightarrow \mathsf{f}(x) & \mathsf{f}(\mathsf{g}(\mathsf{a})) \leftarrow\!\rtimes\!\rightarrow \mathsf{f}(x) & \mathsf{b} \leftarrow\!\rtimes\!\rightarrow \mathsf{b} \\ \mathsf{f}(\mathsf{g}(\mathsf{f}(x))) \leftarrow\!\rtimes\!\rightarrow \mathsf{b} & \mathsf{f}(\mathsf{g}(x)) \leftarrow\!\rtimes\!\rightarrow \mathsf{f}(\mathsf{g}(x)) & \end{array}$$

Using the second rule it is easy to see that all of them are strongly closed. Hence $\mathcal{R}$ is confluent.

The next example shows that, if the variable condition is not satisfied, critical pairs that arise from overlapping a rule with itself at the root are essential.

Example 3. Consider the linear rewrite system $\mathcal{R}$ consisting of the rule $\mathsf{a} \to y$. Because of the peak $x \leftarrow \mathsf{a} \to y$, $\mathcal{R}$ is not confluent and indeed $x \leftarrow\!\rtimes\!\rightarrow y$ is a non-joinable critical pair according to our definition.

In the next section we consider a criterion that drops the condition on $\mathcal{R}$ to be right-linear.

4 Parallel Closed Critical Pairs

The criterion from the previous section requires the TRS to be linear and while left-linearity is a common restriction, right-linearity is a rather unnatural one. Thus we turn our attention to criteria for left-linear systems that change the restriction on the joinability of critical pairs. The crucial observation is that in a non-right-linear system executing the upper step in variable overlap can duplicate the redex below. Thus to join such a situation multiple steps might be necessary, all of which take place at parallel positions. Consequently we consider parallel rewriting. The following definition describes the new joinability condition.

Definition 3. *A TRS $\mathcal{R}$ is* parallel closed *if every critical pair $s \leftarrow\!\rtimes\!\rightarrow t$ of $\mathcal{R}$ satisfies $s \mathrel{+\!\!\!\!\!\to}_{\mathcal{R}} t$.*

Together with left-linearity this guarantees the diamond property of the parallel rewrite relation.

Theorem 1 (Huet [10]). *If a TRS $\mathcal{R}$ is left-linear and parallel closed then $\mathrel{+\!\!\!\!\!\to}_{\mathcal{R}}$ has the diamond property.*

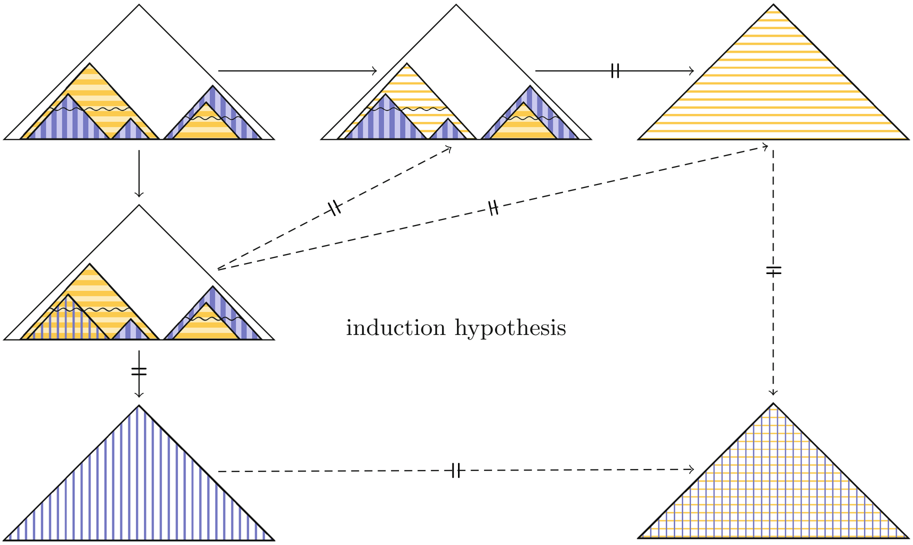

Fig. 1. Overview of the proof of Theorem 1.

The proof of this theorem is much more involved than the one for strongly closed systems. The first observation is that we will now have to consider a peak of parallel steps, in order to show the diamond property of $\mathrel{-\!\!\!|\!|\!\!\!\rightarrow}$. In case the two parallel steps are orthogonal to each other, they simply commute by the well-known Parallel Moves Lemma. However, if they do interfere the assumption of the theorem only allows us to close a single critical pair to reduce the amount of interference. Thus we will have to use some form of induction on how much the patterns of the two parallel steps overlap. Figure 1 shows the setting for the overlapping case. The horizontal parallel step, described by the horizontally striped redexes, and the vertical step, described by the vertically striped redexes, overlap. Hence there is a critical pair, say the one obtained from overlapping the leftmost vertical redex with the leftmost horizontal redex. Then, by assumption there is a closing parallel step, which, since it takes place inside the critical pair, can be combined with the remaining horizontal redexes to obtain a new peak with less overlap, which can be closed by the induction hypothesis. When making this formal we identified two crucial choices. First the representation of the parallel rewrite relation and second the way to measure the amount of overlap between two parallel steps with the same source. Huet in his original proof heavily uses positions. That is, a parallel step is defined as multiple single steps that happen at parallel positions and for measuring overlap he takes the sum of the sizes of the subterms that are affected by both steps. More precisely, writing $\mathrel{-\!\!\!|\!|\!\!\!\rightarrow}_P$ for a parallel step that takes place at positions in a set P, for a peak $t \;{}_{P_1}\!\!\mathrel{\leftarrow\!\!\!|\!|\!\!\!-}\; s \mathrel{-\!\!\!|\!|\!\!\!\rightarrow}_{P_2} u$ he uses

$$\sum_{q \in Q} |s|_q|$$

where $Q = \{p_1 \in P_1 \mid p_2 \leqslant p_1 \text{ for some } p_2 \in P_2\} \cup \{p_2 \in P_2 \mid p_1 \leqslant p_2 \text{ for some } p_1 \in P_1\}$. This formulation is also adopted in the text book by Baader and Nipkow [3]. Consequently, when starting the present formalization, we also adopted this definition. However, the book keeping required by working with sets of positions as well as formally reasoning about this measure in Isabelle became so convoluted that it very much obscured the ingenuity and elegance of Huet's original idea while at the same time defeating our formalization efforts. Hence in the end we had to adopt a different approach.

Toyama [22], in the proof of his extension of Huet's result, does not use positions at all and instead relies on (multihole) contexts, which means a parallel step is then described by a context and a list of root steps that happen in the holes. To measure overlap he collects those redexes that are subterms of some redex in the other step, i.e., decorating the parallel rewrite relation with the redexes contracted in the step, for a peak $t \;{}_{t_1,\ldots,t_n}\!\!\leftarrow\!\!\!\!\shortparallel\;\; s \;\shortparallel\!\!\!\!\rightarrow_{u_1,\ldots,u_m} u$ Toyama's measure is

$$\sum_{s \in S} |s|$$

where $S = \{u_i \mid u_i \trianglelefteq t_j \text{ for some } t_j\} \cup \{t_j \mid t_j \trianglelefteq u_i \text{ for some } u_i\}$. However, this measure turns out to be problematic as shown in the following example.

Example 4. Consider the TRS consisting of the following five rewrite rules:

$$\mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}) \to \mathsf{f}(\mathsf{c},\mathsf{c},\mathsf{c},\mathsf{c}) \qquad \mathsf{a} \to \mathsf{b} \qquad \mathsf{a} \to \mathsf{c} \qquad \mathsf{b} \to \mathsf{a} \qquad \mathsf{b} \to \mathsf{c}$$

Then we have the peak $\mathsf{f}(\mathsf{b},\mathsf{b},\mathsf{a},\mathsf{a}) \overset{\mathsf{a,a,b,b}}{\longleftarrow\!\!\!\!\!\shortparallel\;\;} \mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}) \overset{\mathsf{f(a,a,b,b)}}{\;\;\shortparallel\!\!\!\!\!\longrightarrow} \mathsf{f}(\mathsf{c},\mathsf{c},\mathsf{c},\mathsf{c})$. The measure of this peak according to the definition above is 2, since $S = \{\mathsf{a},\mathsf{b}\} \cup \varnothing$. Now after splitting of one of the four critical steps—it does not matter which one—and closing the corresponding critical pair, we arrive at

$$\begin{tikzcd}
\mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}) \arrow[r] \arrow[d] & \mathsf{f}(\mathsf{c},\mathsf{c},\mathsf{c},\mathsf{c}) \\
\mathsf{f}(\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}) \arrow[ur, "\shortparallel" marking] \arrow[d, "\shortparallel" marking] & \\
\mathsf{f}(\mathsf{b},\mathsf{b},\mathsf{a},\mathsf{a}) &
\end{tikzcd}$$

The measure of the new peak $\mathsf{f}(\mathsf{b},\mathsf{b},\mathsf{a},\mathsf{a}) \overset{\mathsf{a,b,b}}{\longleftarrow\!\!\!\!\!\shortparallel\;\;} \mathsf{f}(\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}) \overset{\mathsf{b,a,b,b}}{\;\;\shortparallel\!\!\!\!\!\longrightarrow} \mathsf{f}(\mathsf{c},\mathsf{c},\mathsf{c},\mathsf{c})$ is still 2 since $S = \{\mathsf{a},\mathsf{b}\} \cup \{\mathsf{a},\mathsf{b}\}$.

Note that using multisets instead of sets does not help, since then the measure of the initial peak is 4 ($S = \{\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}\}$) and of the new peak, after closing the critical pair, it is 7 since $S = \{\mathsf{a},\mathsf{b},\mathsf{b}\} \uplus \{\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}\}$ (and even if we take into account that three of the redexes are counted twice we still get 4). The problem is that in the new peak the redex at position 1 of the closing step is counted again, because b is a subterm of one the redexes of the other step. Hence it is crucial to only count redexes at overlapping positions.

To remedy this situation we will collect all *overlapping* redexes of a peak in a multiset. These multisets will then be compared by $\rhd_{\mathsf{mul}}$, the multiset extension of the proper superterm relation. We start by characterizing parallel rewrite steps using multihole contexts.

Definition 4. *We write* $s \overset{C,a_1,\ldots,a_n}{\relbar\!\!\shortparallel\!\!\relbar\!\!\rightarrow}_{\mathcal{R}} t$ *if* $s = C[a_1,\ldots,a_n]$ *and* $t = C[b_1,\ldots,b_n]$ *for some* $b_1,\ldots,b_n$ *with* $a_i \to^{\epsilon}_{\mathcal{R}} b_i$ *for all* $1 \leqslant i \leqslant n$*.*

To save space we sometimes abbreviate a list of terms $a_1,\ldots,a_n$ by $\overline{a}$ and write $s \overset{C,\overline{a}}{\relbar\!\!\shortparallel\!\!\rightarrow}_{\mathcal{R}} t$ leaving length implicit. The following expected correspondence is easily shown by induction.

Lemma 5. *We have* $s \relbar\!\!\shortparallel\!\!\rightarrow_{\mathcal{R}} t$ *if and only if* $s \overset{C,\overline{s}}{\relbar\!\!\shortparallel\!\!\rightarrow}_{\mathcal{R}} t$ *for some* C *and* $\overline{s}$*.*

Now we can formally measure the overlap between two parallel rewrite steps by collecting those redexes that are below some redex in the other step.

Definition 5. *The overlap between two co-initial parallel rewrite steps is defined by the following equations*

$$\blacktriangle\left(\overset{\Box,a}{\leftarrow\!\!\shortparallel\!\!\relbar}\; s \;\overset{\Box,b}{\relbar\!\!\shortparallel\!\!\rightarrow}\right) = \{s\}$$

$$\blacktriangle\left(\overset{C,a_1,\ldots,a_c}{\leftarrow\!\!\relbar\!\!\shortparallel\!\!\relbar\!\!\relbar}\; s \;\overset{\Box,b}{\relbar\!\!\shortparallel\!\!\rightarrow}\right) = \{a_1,\ldots,a_c\}$$

$$\blacktriangle\left(\overset{\Box,a}{\leftarrow\!\!\shortparallel\!\!\relbar}\; s \;\overset{D,b_1,\ldots,b_d}{\relbar\!\!\relbar\!\!\shortparallel\!\!\relbar\!\!\rightarrow}\right) = \{b_1,\ldots,b_d\}$$

$$\blacktriangle\left(\overset{f(C_1,\ldots,C_n),\overline{a}}{\leftarrow\!\!\relbar\!\!\relbar\!\!\shortparallel\!\!\relbar\!\!\relbar\!\!\relbar}\; f(s_1,\ldots,s_n) \;\overset{f(D_1,\ldots,D_n),\overline{b}}{\relbar\!\!\relbar\!\!\relbar\!\!\shortparallel\!\!\relbar\!\!\relbar\!\!\rightarrow}\right) = \bigcup_{i=1}^{n} \blacktriangle\left(\overset{C_i,\overline{a}_i}{\leftarrow\!\!\shortparallel\!\!\relbar}\; s_i \;\overset{D_i,\overline{b}_i}{\relbar\!\!\shortparallel\!\!\rightarrow}\right)$$

where $\overline{a}_1,\ldots,\overline{a}_n = \overline{a}$ *and* $\overline{b}_1,\ldots,\overline{b}_n = \overline{b}$ *are partitions of* $\overline{a}$ *and* $\overline{b}$ *such that the length of* $\overline{a}_i$ *and* $\overline{b}_i$ *matches the number of holes in* C_i *and* D_i*, for all* $1 \leqslant i \leqslant n$*.*

Example 5. Applying this definition for the two peaks from Example 4 yields

$$\blacktriangle\left(\overset{\mathsf{f}(\Box,\Box,\Box,\Box),\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}}{\leftarrow\!\!\relbar\!\!\relbar\!\!\relbar\!\!\shortparallel\!\!\relbar\!\!\relbar\!\!\relbar}\; \mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}) \;\overset{\Box,\mathsf{f}(\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b})}{\relbar\!\!\relbar\!\!\shortparallel\!\!\relbar\!\!\rightarrow}\right) = \{\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}\}$$

$$\blacktriangle\left(\overset{\mathsf{f}(\mathsf{b},\Box,\Box,\Box),\mathsf{a},\mathsf{b},\mathsf{b}}{\leftarrow\!\!\relbar\!\!\relbar\!\!\shortparallel\!\!\relbar\!\!\relbar}\; \mathsf{f}(\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}) \;\overset{\mathsf{f}(\Box,\Box,\Box,\Box),\mathsf{b},\mathsf{a},\mathsf{b},\mathsf{b}}{\relbar\!\!\relbar\!\!\relbar\!\!\shortparallel\!\!\relbar\!\!\relbar\!\!\rightarrow}\right) = \{\mathsf{a},\mathsf{b},\mathsf{b}\}$$

and $\{\mathsf{a},\mathsf{a},\mathsf{b},\mathsf{b}\} \rhd_{\mathsf{mul}} \{\mathsf{a},\mathsf{b},\mathsf{b}\}$ as desired.

Note that our definition of $\blacktriangle$ is in fact an over-approximation of the actual overlap between the steps. That is because we do not split redexes into the left-hand side of the applied rule and a substitution but take the redex as a whole. The following example illustrates the effect.

Example 6. Consider the rewrite system consisting of the two rules

$$\mathsf{f}(x) \to x \qquad\qquad\qquad \mathsf{a} \to \mathsf{b}$$

and the peak $\mathsf{a} \leftarrow \mathsf{f}(\mathsf{a}) \to \mathsf{f}(\mathsf{b})$. We have

$$\blacktriangle\left(\overset{\Box,\mathsf{f}(\mathsf{a})}{\longleftarrow\!\!\!\!\!\!\!\!\!\shortparallel\;\;\;}\ \mathsf{f}(\mathsf{a})\ \overset{\mathsf{f}(\Box),\mathsf{a}}{\;\;\;\shortparallel\!\!\!\!\!\!\!\!\!\longrightarrow}\right) = \{\mathsf{a}\}$$

although the two steps do not overlap—the step to the right takes place completely in the substitution of the one to the left (in fact the rewrite system in question is orthogonal).

However, since we are dealing with parallel rewriting, no problems arise from this over-approximation. This changes when extending the results to development steps, see Sect. 7 for further discussion.

The following properties of $\blacktriangle$ turned out to be crucial in our proof of Theorem 1.

Lemma 6. *For a peak* $\overset{C,\overline{a}}{\longleftarrow\!\!\!\!\!\!\!\!\!\shortparallel\;\;\;}\ s\ \overset{D,\overline{b}}{\;\;\;\shortparallel\!\!\!\!\!\!\!\!\!\longrightarrow}$ *the following properties of* $\blacktriangle$ *hold.*

- *If* $s = f(s_1, \ldots, s_n)$ *with* $C = f(C_1, \ldots, C_n)$ *and* $D = f(D_1, \ldots, D_n)$ *then*

$$\blacktriangle\left(\overset{C_i,\overline{a}_i}{\longleftarrow\!\!\!\!\!\!\!\!\!\shortparallel\;\;\;}\ s_i\ \overset{D_i,\overline{b}_i}{\;\;\;\shortparallel\!\!\!\!\!\!\!\!\!\longrightarrow}\right) \subseteq \blacktriangle\left(\overset{C,\overline{a}}{\longleftarrow\!\!\!\!\!\!\!\!\!\shortparallel\;\;\;}\ s\ \overset{D,\overline{b}}{\;\;\;\shortparallel\!\!\!\!\!\!\!\!\!\longrightarrow}\right)$$

  for all $1 \leqslant i \leqslant n$.
- *The overlap is bounded by* $\overline{a}$, *i.e.,* $\{a_1, \ldots, a_c\} \rhd^{=}_{\mathsf{mul}} \blacktriangle\left(\overset{C,\overline{a}}{\longleftarrow\!\!\!\!\!\!\!\!\!\shortparallel\;\;\;}\ s\ \overset{D,\overline{b}}{\;\;\;\shortparallel\!\!\!\!\!\!\!\!\!\longrightarrow}\right)$.
- *The overlap is symmetric, i.e.,* $\blacktriangle\left(\overset{C,\overline{a}}{\longleftarrow\!\!\!\!\!\!\!\!\!\shortparallel\;\;\;}\ s\ \overset{D,\overline{b}}{\;\;\;\shortparallel\!\!\!\!\!\!\!\!\!\longrightarrow}\right) = \blacktriangle\left(\overset{D,\overline{b}}{\longleftarrow\!\!\!\!\!\!\!\!\!\shortparallel\;\;\;}\ s\ \overset{C,\overline{a}}{\;\;\;\shortparallel\!\!\!\!\!\!\!\!\!\longrightarrow}\right)$.

There is one more high-level difference between the formalization and the paper proof. In the original proof one needs to combine the closing step for the critical pair with the remainder of the original step in order to obtain a new peak, to which the induction hypothesis can then be applied. This reasoning can be avoided, by using an additional induction on the source of the peak. Then the case where neither of the two parallel steps is a root step (and thus a single step) can be discharged by the induction hypothesis of that induction.

The following technical lemma tells us that a parallel rewrite step starting from $s\sigma$ is either inside s, i.e., we can split off a critical pair, or we can do the step completely inside σ.

Lemma 7. *Let s be a linear term. If* $s\sigma \overset{C,s_1,\ldots,s_n}{\;\;\;\shortparallel\!\!\!\!\!\!\!\!\!\longrightarrow}_{\mathcal{R}} t$ *then either* $t = s\tau$ *for some substitution* τ *such that* $x\sigma \;\shortparallel\!\!\!\!\!\!\longrightarrow x\tau$ *for all* $x \in \mathcal{V}\mathsf{ar}(s)$ *or there exist a context* D, *a non-variable term* s', *a rule* $\ell \to r \in \mathcal{R}$, *a substitution* τ, *and a multihole context* C' *such that* $s = D[s']$, $s'\sigma = \ell\tau$, $D\sigma[r\tau] = C'[s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n]$ *and* $t = C'[t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n]$ *for some* $1 \leqslant i \leqslant n$.

We are now ready to prove the main result of this section. To ease presentation, the following proof does use the condition that the left-hand sides of rewrite rules are not variables. By employing additional technical case analyses this restriction can be easily dropped. We refer to the formalization for details.

Proof (of Theorem 1). Assume $t \overset{C,\overline{a}}{\mathrel{\longleftarrow\mkern-16mu\|\mkern9mu}} s \overset{D,\overline{b}}{\mathrel{\mkern9mu\|\mkern-16mu\longrightarrow}} u$. We show $t \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} v \mathrel{\leftarrow\mkern-13mu\|\mkern5mu} u$ for some term v by well-founded induction on the overlap between the two parallel steps using the order $\rhd_{\mathsf{mul}}$ and continue by induction on s with respect to $\rhd$. If $s = x$ for some variable x then $t = u = x$. So let $s = f(s_1, \ldots, s_n)$. We distinguish four cases.

1. If $C = f(C_1, \ldots, C_n)$ and $D = f(D_1, \ldots, D_n)$ then $t = f(t_1, \ldots, t_n)$ and $u = f(u_1, \ldots, u_n)$ and we obtain partitions $\overline{a}_1, \ldots, \overline{a}_n = \overline{a}$ and $\overline{b}_1, \ldots, \overline{b}_n = \overline{b}$ of $\overline{a}$ and $\overline{b}$ with $t_i \overset{C_i,\overline{a}_i}{\mathrel{\longleftarrow\mkern-16mu\|\mkern9mu}} s_i \overset{D_i,\overline{b}_i}{\mathrel{\mkern9mu\|\mkern-16mu\longrightarrow}} u_i$ for all $1 \leqslant i \leqslant n$. Then, since we have

   $$\blacktriangle\left(\overset{C_i,\overline{a}_i}{\mathrel{\longleftarrow\mkern-16mu\|\mkern9mu}} s_i \overset{D_i,\overline{b}_i}{\mathrel{\mkern9mu\|\mkern-16mu\longrightarrow}}\right) \subseteq \blacktriangle\left(\overset{C,\overline{a}}{\mathrel{\longleftarrow\mkern-16mu\|\mkern9mu}} s \overset{D,\overline{b}}{\mathrel{\mkern9mu\|\mkern-16mu\longrightarrow}}\right)$$

   by Lemma 6 and thus also

   $$\blacktriangle\left(\overset{C,\overline{a}}{\mathrel{\longleftarrow\mkern-16mu\|\mkern9mu}} s \overset{D,\overline{b}}{\mathrel{\mkern9mu\|\mkern-16mu\longrightarrow}}\right) \rhd_{\mathsf{mul}}^{=} \blacktriangle\left(\overset{C_i,\overline{a}_i}{\mathrel{\longleftarrow\mkern-16mu\|\mkern9mu}} s_i \overset{D_i,\overline{b}_i}{\mathrel{\mkern9mu\|\mkern-16mu\longrightarrow}}\right)$$

   we can apply the inner induction hypothesis and obtain terms v_i with $t_i \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} v_i \mathrel{\leftarrow\mkern-13mu\|\mkern5mu} u_i$ for all $1 \leqslant i \leqslant n$ and thus we have $t \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} f(v_1, \ldots, v_n) \mathrel{\leftarrow\mkern-13mu\|\mkern5mu} u$.
2. If $C = D = \Box$ then both steps are root steps and thus single rewrite steps and we can write $t = r_1\sigma_1 \overset{\epsilon}{\leftarrow} \ell_1\sigma_1 = s = \ell_2\sigma_2 \overset{\epsilon}{\rightarrow} r_2\sigma_2 = u$. Hence, since $\ell_1\sigma_1 = \ell_2\sigma_2$, there is a critical pair $r_1'\mu \leftarrow\!\bowtie\!\rightarrow r_2'\mu$ for variable disjoint variants $\ell_1' \to r_1'$, $\ell_2' \to r_2'$ of $\ell_1 \to r_1$, $\ell_2 \to r_2$ with μ a most general unifier of ℓ_1' and ℓ_2'. Then by assumption $r_1'\mu \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} r_2'\mu$ and by closure under substitution also $t = r_1\sigma_1 \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} r_2\sigma_2 = u$.
3. If $C = f(C_1, \ldots, C_n)$ and $D = \Box$ then the step to the right is a single root step and we write $t = f(t_1, \ldots, t_n) \overset{C,\overline{a}}{\mathrel{\longleftarrow\mkern-16mu\|\mkern9mu}} s = \ell\sigma \overset{\epsilon}{\rightarrow} r\sigma = u$. Since ℓ is linear by assumption, we can apply Lemma 7 and either obtain τ with $t = \ell\tau$ and $x\sigma \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} x\tau$ for all $x \in \mathcal{V}\mathsf{ar}(\ell)$ or a critical pair.
   - In the first case define

     $$\delta(x) = \begin{cases} \tau(x) & \text{if } x \in \mathcal{V}\mathsf{ar}(\ell) \\ \sigma(x) & \text{otherwise} \end{cases}$$

     We have $t = \ell\tau = \ell\delta$ by definition of δ and hence $t \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} r\delta$ by a single root step. Moreover we have $u = r\sigma \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} r\delta$ since $x\sigma \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} x\delta$ for all variables $x \in \mathcal{V}\mathsf{ar}(r)$. This holds because either $x \in \mathcal{V}\mathsf{ar}(\ell)$ and then $x\sigma \mathrel{\mkern5mu\|\mkern-13mu\rightarrow} x\tau = x\delta$ or $x \notin \mathcal{V}\mathsf{ar}(\ell)$ and then $x\sigma = x\delta$.
   - In the second case Lemma 7 yields a context E, a non-variable term ℓ'', a rule $\ell' \to r' \in \mathcal{R}$, a substitution τ, and a multihole context C' such

that $\ell = E[\ell'']$, $\ell''\sigma = \ell'\tau$, $E\sigma[r'\tau] = C'[a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_c]$ and $t = C'[a'_1, \ldots, a'_{i-1}, a'_{i+1}, \ldots, a'_c]$ for some $1 \leqslant i \leqslant c$. Since $\ell''\sigma = \ell'\tau$ there is a critical pair $E\mu[r'\mu] \leftarrow\!\rtimes\!\rightarrow r\mu$ and by assumption $E\mu[r'\mu] \mathrel{\|\!\!\!\twoheadrightarrow} r\mu$ and thus also $E\sigma[r'\tau] \mathrel{\|\!\!\!\twoheadrightarrow} r\sigma$. That is, we obtain a new peak

$$t \mathrel{\overset{C',\overline{a}'}{\leftarrow\!\!\|\!\!-}} E\sigma[r'\tau] \mathrel{\|\!\!\!\twoheadrightarrow} r\sigma$$

with $\overline{a}' = a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_c$. Since

$$\blacktriangle\left(\mathrel{\overset{C,\overline{a}}{\leftarrow\!\!\|\!\!-}} s \mathrel{\overset{\Box,\ell\sigma}{-\!\!\|\!\!\rightarrow}}\right) = \{a_1, \ldots, a_c\} \rhd_{\mathsf{mul}} \{a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_c\}$$
$$\rhd^{=}_{\mathsf{mul}} \blacktriangle\left(\mathrel{\overset{C',\overline{a'}}{\leftarrow\!\!\|\!\!-}} E\sigma[r'\tau] \mathrel{\|\!\!\!\twoheadrightarrow}\right)$$

by Lemma 6, we can apply the induction hypothesis and obtain v with $t \mathrel{\|\!\!\!\twoheadrightarrow} v \mathrel{\twoheadleftarrow\!\!\!\|} r\sigma = u$.

4. The final case, $D = f(D_1, \ldots, D_n)$ and $C = \Box$, is completely symmetric.

Finally, by Lemmas 1 and 2 we obtain confluence of $\rightarrow_{\mathcal{R}}$.

Example 7. Consider the TRS $\mathcal{R}$ consisting of the following three rewrite rules:

$$x + y \rightarrow y + x \qquad (x + y) * z \rightarrow (x * z) + (y * z) \qquad (y + x) * z \rightarrow (x * z) + (y * z)$$

Since the four critical pairs of $\mathcal{R}$

$$\begin{array}{ll} (y + x) * z \leftarrow\!\rtimes\!\rightarrow (x * z) + (y * z) & (y * z) + (x * z) \leftarrow\!\rtimes\!\rightarrow (x * z) + (y * z) \\ (x + y) * z \leftarrow\!\rtimes\!\rightarrow (x * z) + (y * z) & (x * z) + (y * z) \leftarrow\!\rtimes\!\rightarrow (y * z) + (x * z) \end{array}$$

are parallel closed, $\mathcal{R}$ is confluent.

5 Almost Parallel Closed Critical Pairs and Commutation

In this section we consider two extensions to Huet's result due to Toyama [22]. The first one allows us to weaken the joining condition for some critical pairs.

When carefully examining the proof of Theorem 1 one realizes that in the case where both steps of the peak are single root steps, i.e., the case where $C = D = \Box$, the induction hypothesis does not need to be applied, since closing the critical pair immediately closes the whole peak. This suggests that the joining condition can be weakened for overlays. A first idea could be to take $\leftarrow\!\bowtie\!\rightarrow \subseteq \mathrel{\|\!\!\!\twoheadrightarrow} \cdot \mathrel{\twoheadleftarrow\!\!\!\|}$ since then we would still have the diamond property in the overlay case. However Toyama realized that one can do even better by weakening the diamond property to strong confluence. The following definition captures the new conditions.

Definition 6. *A TRS $\mathcal{R}$ is* almost parallel closed *if $s \mathrel{\|\!\!\!\twoheadrightarrow} \cdot {}^{*}\!\!\leftarrow t$ for all overlays $s \leftarrow\!\bowtie\!\rightarrow t$ and $s \mathrel{\|\!\!\!\twoheadrightarrow} t$ for all inner critical pairs $s \leftarrow\!\rtimes\!\rightarrow t$.*

$$\begin{tikzcd}
s \arrow[r, "2"'] \arrow[d, "1"'] & u \arrow[d, "1"', "*"] \\
E\sigma[r'\tau] \arrow[r, "\shortparallel" marking, "2"'] \arrow[d, "=" marking, "1"'] & v \arrow[d, "1"', "*"] \\
t \arrow[r, "\shortparallel" marking, "2"'] & v'
\end{tikzcd}
\qquad
\begin{tikzcd}
s \arrow[r, "2"'] \arrow[d, "1"'] & \cdot \arrow[r, "\shortparallel" marking, "2"'] \arrow[dl, "\shortparallel" marking, "1"] & u \arrow[d, "1"', "*"] \\
t \arrow[rr, "\shortparallel" marking, "2"'] & & v
\end{tikzcd}$$

Fig. 2. Asymmetry in the proof of Theorem 2.

Using exactly the same proof structure as before we could now prove strong confluence of $⤁$ for left-linear almost parallel closed systems. However, considering Toyama's second extension of Theorem 1, we will prove the theorem in the more general setting of commutation.

Theorem 2 (Toyama [22]). *Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be left-linear TRSs. If $s \mathrel{⤁}_2 \cdot {}_1^{*}\!\!\leftarrow t$ for all critical pairs $s \;{}_1\!\leftarrow\!\rtimes\!\rightarrow_2\; t$ and additionally $s \mathrel{⤁}_1 t$ for all inner critical pairs $s \;{}_2\!\leftarrow\!\rtimes\!\rightarrow_1\; t$ then $⤁_1$ and $⤁_2$ strongly commute.*

Proof (Adaptations). We only highlight the differences to the proof of Theorem 1 and refer to the formalization for the full proof details. Assume

$$t \;{}_1\!\overset{C,\bar{a}}{\longleftarrow\!\!\shortparallel\!\!-}\; s \;\overset{D,\bar{b}}{-\!\!\shortparallel\!\!\longrightarrow}_2\; u$$

We show $t \mathrel{⤁}_2 v \;{}_1^{*}\!\!\leftarrow u$ for some term v. We apply the same inductions and case analyses as before. The cases $C = f(C_1, \ldots, C_n)$, $D = f(D_1, \ldots, D_n)$ and $C = D = \square$ require no noteworthy adaptation. The main difference is that now the cases $D = f(D_1, \ldots, D_n)$, $C = \square$ and $C = f(C_1, \ldots, C_n)$, $D = \square$ become asymmetric for the critical pair case—the corresponding diagrams are shown in Fig. 2.

First, suppose $C = f(C_1, \ldots, C_n)$ and $D = \square$, write $t = f(t_1, \ldots, t_n) \;{}_1\!\overset{C,\bar{a}}{\longleftarrow\!\!\shortparallel\!\!-}\; s = \ell\sigma \xrightarrow{\epsilon}_2 r\sigma = u$, and assume there is a critical pair according to Lemma 7. That is, we obtain $E\mu[r'\mu] \;{}_1\!\leftarrow\!\rtimes\!\rightarrow_2\; r\mu$ with $E\sigma[r'\tau] \mathrel{⤁}_1 t$ and by assumption we obtain a v such that $E\sigma[r'\tau] \mathrel{⤁}_2 v \;{}_1^{*}\!\!\leftarrow r\sigma$. Then using the same reasoning as before, for the new peak

$$t \;{}_1\!\overset{C',\overline{a'}}{\longleftarrow\!\!\shortparallel\!\!-}\; E\sigma[r'\tau] \mathrel{⤁}_2 v$$

we have

$$\blacktriangle\left(\overset{C,\bar{a}}{\longleftarrow\!\!\shortparallel\!\!-}\; s \;\overset{\square,\ell\sigma}{-\!\!\shortparallel\!\!\longrightarrow}\right) \rhd_{\mathsf{mul}} \blacktriangle\left(\overset{C',\overline{a'}}{\longleftarrow\!\!\shortparallel\!\!-}\; E\sigma[r'\tau] \mathrel{⤁}\right)$$

and can apply the induction hypothesis to obtain a v' with $t \mathrel{⤁}_2 v' \;{}_1^{*}\!\!\leftarrow v$, which combined with $u = r\sigma \rightarrow_1^{*} v$ concludes this case.

In the second case, i.e., when $D = f(D_1, \ldots, D_n)$ and $C = \square$, observe that the critical pair we obtain is an inner critical pair between $\mathcal{R}_2$ and $\mathcal{R}_1$, since

$D \neq \square$. Thus, after applying the assumption for critical pairs ${}_2{\leftarrow}\!\rtimes\!{\rightarrow}_1$, the proof is the same as for Theorem 1.

Instantiating $\mathcal{R}_1$ and $\mathcal{R}_2$ with the same TRS $\mathcal{R}$ yields the corresponding result for confluence.

Corollary 2 (Toyama [22]). *If the TRS $\mathcal{R}$ is left-linear and almost parallel closed then $\mathrel{+\!\!\!\!\!\twoheadrightarrow}_{\mathcal{R}}$ is strongly confluent.*

Proof. Immediate from the definition of almost parallel closed, Theorem 2 and the fact that $s \leftarrow\!\rtimes\!\rightarrow t$ if and only if $s \leftarrow\!\bowtie\!\rightarrow t$ or $s \leftarrow\!\cdot\!\!\rtimes\!\rightarrow t$.

Example 8. Recall the rewrite system from Example 4. One easily verifies that all its critical pairs are almost parallel closed, and hence it is confluent.

6 Certification and Experiments

To facilitate checking of confluence proofs generated by automatic tools based on Corollarys 1 and 2 we extended the CPF to represent such proofs. Since in order to check that a given TRS is strongly or almost parallel closed, CeTA has to compute all critical pairs anyway, in the certificate we just require the claim that the system is strongly or almost parallel closed, together with a bound on the length of the rewrite sequences to join the critical pairs.[4] Certificates for commutation are not yet supported, since currently no tool produces them, and CPF does not contain a specification for commutation proofs.

For experiments we considered all 277 TRSs in the Cops[5] database and used the confluence tool CSI to obtain certificates in CPF for confluence proofs. All generated certificates have been certified by CeTA. Table 1 shows the results of running CSI with different strategies. The first and second column show the results of applying just Corollarys 1 and 2 respectively, the third column is the combination. In the fourth column we show the result when additionally adding and removing redundant rewrite rules [13], which yields a considerable boost in power. The idea of that technique is to add and remove rules that can be simulated by other rules, which consequently does not change confluence of the system, but often makes other criteria, like the ones we consider here, applicable. Column "full" shows the results for the full certified strategy of CSI, which additionally includes Knuth and Bendix' criterion, weak orthogonality (which is subsumed by Corollary 2, however) and the rule labeling heuristic [15] as well as several criteria for non-confluence. The last column shows the difference to last year's version of CSI's certified strategy, which already included Corollary 1, but not Corollary 2. In addition to the new certifiable proofs, several existing proofs of CSI 2015 could be simplified and no longer require complicated reasoning via decreasing diagrams.

[4] This bound is necessary to ensure termination of the certifier.

[5] http://cops.uibk.ac.at.

Table 1. Experimental results.

	SC	PC	SC+PC	SC+PC+RR	full	2015
yes	38	21	41	92	110	104
no	0	0	0	0	48	48
maybe	239	256	236	185	119	125

7 Conclusion

In this paper we presented the first formalization of three classical criteria for confluence and commutation of (left-)linear rewrite systems. Building on top of IsaFoR—which provided invaluable support on the one hand, e.g. by its theories on critical pairs and multihole contexts, and on the other hand, as expected, was also extended with new basic facts about lists, multisets, multihole contexts etc.—we formalized proofs that linear strongly closed systems, and left-linear (almost) parallel closed systems are confluent (commute). The major difference to the paper proof is our definition of the overlap between two parallel steps that are represented via multihole contexts.

Concerning future work, another important extension of the results of Huet and Toyama due to van Oostrom [17] is using multisteps (also called development steps) $\mathrel{-\!\!\circ\!\!\rightarrow}$ which allow nested non-overlapping redexes. This extension not only strengthens Huet's criterion in the first-order world but also makes it applicable to higher-order rewriting, where using parallel steps fails due to β-reduction.

However, although the paper proofs superficially look very similar, and do employ similar ideas, obtaining a formalized proof will require serious effort. In fact neither our representation of (parallel) rewrite steps, nor our definition of $\blacktriangle$, nor the idea of using an induction on the source of the peak to avoid reasoning about combining steps, carry over. To make the concepts that are hard to formalize in a proof assistant, e.g. measuring the amount of overlap between two multisteps or the descendants of a multistep, Hirokawa and Middeldorp [9] suggested to use proof terms to obtain a rigorous proof (and at the same time extended the result to commutation). This is a step forward but more is needed to obtain a formalized proof, also for the extension to higher-order systems. In particular, we anticipate the extensive use of sets of positions (in [9]) to be problematic without alternative notions. We plan to employ residual theory [20, Sect. 8.7] and to develop a notion of overlap for multisteps similar to Definition 5 to close the gap.

Acknowledgments. We thank Nao Hirokawa for suggesting Lemma 6 and Bertram Felgenhauer and Christian Sternagel for insightful discussion.

References

1. Aoto, T.: Disproving confluence of term rewriting systems by interpretation and ordering. In: Fontaine, P., Ringeissen, C., Schmidt, R.A. (eds.) FroCoS 2013. LNCS, vol. 8152, pp. 311–326. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40885-4_22
2. Aoto, T., Yoshida, J., Toyama, Y.: Proving confluence of term rewriting systems automatically. In: Treinen, R. (ed.) RTA 2009. LNCS, vol. 5595, pp. 93–102. Springer, Heidelberg (2009). doi:10.1007/978-3-642-02348-4_7
3. Baader, F., Nipkow, T.: Term Rewriting and All That. Cambridge University Press, Cambridge (1998)
4. Blanqui, F., Koprowski, A.: CoLoR, a Coq library on well-founded rewrite relations and its application to the automated verification of termination certificates. Math. Struct. Comput. Sci. **21**(4), 827–859 (2011). doi:10.1017/S0960129511000120
5. Contejean, E., Courtieu, P., Forest, J., Pons, O., Urbain, X.: Automated certified proofs with CiME3. In: Schmidt-Schauß, M. (ed.) RTA 2011. LIPIcs, vol. 10. pp. 21–30. Schloss Dagstuhl–Leibniz-Zentrum für Informatik (2011). doi:10.4230/LIPIcs.RTA.2011.21
6. Felgenhauer, B., Thiemann, R.: Reachability analysis with state-compatible automata. In: Dediu, A.-H., Martín-Vide, C., Sierra-Rodríguez, J.-L., Truthe, B. (eds.) LATA 2014. LNCS, vol. 8370, pp. 347–359. Springer, Heidelberg (2014). doi:10.1007/978-3-319-04921-2_28
7. Geser, A., Middeldorp, A., Ohlebusch, E., Zantema, H.: Relative undecidability in the term rewriting, part 2: The confluence hierarchy. Inf. Comput. **178**(1), 132–148 (2002). doi:10.1006/inco.2002.3150
8. Hirokawa, N., Klein, D.: Saigawa: a confluence tool. In: Hirokawa, N., Middeldorp, A. (eds.) IWC 2012, p. 49 (2012). http://cl-informatik.uibk.ac.at/events/iwc-2012/
9. Hirokawa, N., Middeldorp, A.: Commutation via relative termination. In: Hirokawa, N., van Oostrom, V. (eds.) IWC 2013, pp. 29–33 (2013). http://www.jaist.ac.jp/~hirokawa/iwc2013/
10. Huet, G.: Confluent reductions: abstract properties and applications to term rewriting systems. J. ACM **27**(4), 797–821 (1980). doi:10.1145/322217.322230
11. Klein, D., Hirokawa, N.: Confluence of non-left-linear TRSs via relative termination. In: Bjørner, N., Voronkov, A. (eds.) LPAR-18 2012. LNCS, vol. 7180, pp. 258–273. Springer, Heidelberg (2012). doi:10.1007/978-3-642-28717-6_21
12. Knuth, D., Bendix, P.: Simple word problems in universal algebras. In: Leech, J. (ed.) Computational Problems in Abstract Algebra, pp. 263–297. Pergamon Press (1970)
13. Nagele, J., Felgenhauer, B., Middeldorp, A.: Improving automatic confluence analysis of rewrite systems by redundant rules. In: Fernández, M. (ed.) RTA 2015. LIPIcs, vol. 36, pp. 257–268. Schloss Dagstuhl–Leibniz-Zentrum für Informatik (2015). doi:10.4230/LIPIcs.RTA.2015.257
14. Nagele, J., Thiemann, R.: Certification of confluence proofs using CeTA. In: Aoto, T., Kesner, D. (eds.) IWC 2014, pp. 19–23 (2014). http://www.nue.riec.tohoku.ac.jp/iwc2014/
15. Nagele, J., Zankl, H.: Certified rule labeling. In: Fernández, M. (ed.) RTA 2015. LIPIcs, vol. 36, pp. 269–284. Schloss Dagstuhl–Leibniz-Zentrum für Informatik (2015). doi:10.4230/LIPIcs.RTA.2015.269
16. Nipkow, T., Paulson, L., Wenzel, M.: Isabelle/HOL - A Proof Assistant for Higher-Order Logic. LNCS, vol. 2283. Springer, Heidelberg (2002)

17. van Oostrom, V.: Developing developments. Theoret. Comput. Sci. **175**(1), 159–181 (1997). doi:10.1016/S0304-3975(96)00173-9
18. Shintani, K., Hirokawa, N.: CoLL: A confluence tool for left-linear term rewrite systems. In: Felty, A., Middeldorp, A. (eds.) CADE 2015. LNCS, vol. 9195, pp. 127–136. Springer, Heidelberg (2015). doi:10.1007/978-3-319-21401-6_8
19. Sternagel, C., Thiemann, R.: The certification problem format. In: Benzmüller, C., Woltzenlogel Paleo, B. (eds.) UITP 2014. EPTCS, vol. 167, pp. 61–72. Open Publishing Association (2014). doi:10.4204/EPTCS.167.8
20. Terese: Term Rewriting Systems. Cambridge Tracts in Theoretical Computer-Science, vol. 55. Cambridge University Press, Cambridge (2003)
21. Thiemann, R., Sternagel, C.: Certification of termination proofs using CeTA. In: Berghofer, S., Nipkow, T., Urban, C., Wenzel, M. (eds.) TPHOLs 2009. LNCS, vol. 5674, pp. 452–468. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03359-9_31
22. Toyama, Y.: Commutativity of term rewriting systems. In: Fuchi, K., Kott, L. (eds.) Programming of Future Generation Computers II, pp. 393–407. North-Holland (1988)
23. Zankl, H., Felgenhauer, B., Middeldorp, A.: CSI – a confluence tool. In: Bjørner, N., Sofronie-Stokkermans, V. (eds.) CADE 2011. LNCS, vol. 6803, pp. 499–505. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22438-6_38