Church–Rosser Modulo for Left-Linear TRSs Revisited

Johannes Niederhauser[1], Nao Hirokawa[2], and Aart Middeldorp[1]

[1] Department of Computer Science, University of Innsbruck, Austria
[2] School of Information Science, JAIST, Japan

Abstract

It is known that ordinary critical pairs suffice to establish the Church–Rosser property modulo an equational theory $\mathcal{B}$ for a left-linear and $\mathcal{B}$-terminating TRS. We extend this result to prime critical pairs by introducing a new confluence criterion for ARSs.

1 Introduction

In this paper, we present a new characterization of the Church–Rosser property modulo an equational theory $\mathcal{B}$ for left-linear TRSs which are terminating modulo $\mathcal{B}$. This works for every variable-preserving (i.e., $\mathcal{V}\mathsf{ar}(\ell) = \mathcal{V}\mathsf{ar}(r)$ for all $\ell \approx r \in \mathcal{B}$) equational theory $\mathcal{B}$. The result is based on an observation due to Huet [3] but allows us to use prime critical pairs [4] instead of ordinary critical pairs. The proof of our new result is facilitated by *peak-and-cliff decreasingness*, an extension of peak decreasingness [2] which is a simple confluence criterion for ARSs designed to replace complicated proof orderings in the correctness proofs of completion procedures. Both the confluence criterion as well as the main result are crucial ingredients of a novel fairness condition for left-linear $\mathcal{B}$-completion presented in our recent paper [5]. For the special case of AC, we also present a novel counterexample which shows the necessity of AC termination as a precondition of the main theorem. To the best of our knowledge, this was not documented before.

2 Preliminaries

We assume that the reader is familiar with term rewriting but recapitulate the important definition of (prime) critical pairs. Let $\mathcal{R}$ be a TRS. An *overlap* is a triple $\langle \ell_1 \to r_1, p, \ell_2 \to r_2 \rangle$ satisfying the following properties:

- $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are variants of rewrite rules of $\mathcal{R}$ without common variables,
- p is a non-variable position in ℓ_2,
- ℓ_1 and $\ell_2|_p$ are unifiable, and
- if $p = \epsilon$ then $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are not variants.

Let σ be a most general unifier of ℓ_1 and $\ell_2|_p$. The corresponding *critical peak*

$$\ell_2\sigma[r_1\sigma]_p \overset{p}{\leftarrow} \ell_2\sigma \overset{\epsilon}{\to} r_2\sigma$$

represents the two ways in which $\ell_2\sigma$ can be rewritten and the equation $\ell_2\sigma[r_1\sigma]_p \approx r_2\sigma$ is its associated *critical pair*. The set of critical pairs of a TRS $\mathcal{R}$ is denoted by $\mathsf{CP}(\mathcal{R})$. A critical peak $t \overset{p}{\leftarrow} s \overset{\epsilon}{\to} u$ is *prime* if all proper subterms of $s|_p$ are in normal form. Critical pairs derived from prime critical peaks are called prime. The set of all prime critical pairs of a TRS $\mathcal{R}$ is denoted by $\mathsf{PCP}(\mathcal{R})$. Throughout the paper, we use the following abbreviations:

$$\begin{aligned}\downarrow_{\mathcal{R}}^{\sim} &= \to_{\mathcal{R}}^{*} \cdot \sim_{\mathcal{B}} \cdot {}_{\mathcal{R}}^{*}\!\leftarrow \\ \mathcal{B}^{\pm} &= \mathcal{B} \cup \{ r \approx \ell \mid \ell \approx r \in \mathcal{B} \} \\ \mathsf{CP}^{\pm}(\mathcal{R}_1, \mathcal{R}_2) &= \mathsf{CP}(\mathcal{R}_1, \mathcal{R}_2) \cup \mathsf{CP}(\mathcal{R}_2, \mathcal{R}_1)\end{aligned}$$

Here $\mathsf{CP}(\mathcal{R}_1, \mathcal{R}_2)$ denotes the set of critical pairs (t, u) that originate from critical peaks of the form $t \; {}_{\mathcal{R}_1}^{\;p}\!\leftarrow s \to_{\mathcal{R}_2}^{\epsilon} u$. The starting point of our work is the following result by Huet [3].

Lemma 1. *For left-linear* TRS*s* $\mathcal{R}$*, the inclusion* ${}_{\mathcal{R}}\!\leftarrow \cdot \leftrightarrow_{\mathcal{B}} \subseteq \downarrow_{\mathcal{R}}^{\sim} \cup \leftrightarrow_{\mathsf{CP}^{\pm}(\mathcal{R}, \mathcal{B}^{\pm})}$ *holds.* □

Note that Lemma 1 allows us to use ordinary critical pairs instead of $\mathcal{B}$-critical pairs. In particular, equational unification modulo $\mathcal{B}$ can be replaced by syntactic unification which improves efficiency. Furthermore, the form of the joining sequence ($\downarrow_{\mathcal{R}}^{\sim}$) is advantageous as it uses the normal rewrite relation and just one $\mathcal{B}$-equality check in the end as opposed to rewrite steps modulo the theory ($\sim_{\mathcal{B}} \cdot \to_{\mathcal{R}} \cdot \sim_{\mathcal{B}}$). However, left-linearity is necessary in Lemma 1 as the following example illustrates.

Example 1. *Consider the* TRS $\mathcal{R}$ *consisting of the single rule* $\mathsf{f}(x, x) \to x$ *with* $+$ *as an additional AC function symbol. Consider the conversion*

$$x + y \;{}_{\mathcal{R}}\!\leftarrow \mathsf{f}(x + y, x + y) \sim_{\mathsf{AC}} \mathsf{f}(x + y, y + x)$$

There are no critical pairs in $\mathcal{R}$ *and between* $\mathcal{R}$ *and* $\mathsf{AC}^{\pm}$*, so* $\mathsf{CP}(\mathcal{R}) = \mathsf{CP}^{\pm}(\mathcal{R}, \mathsf{AC}^{\pm}) = \varnothing$*. Moreover,* $x + y \downarrow_{\mathcal{R}}^{\sim} \mathsf{f}(x + y, y + x)$ *does not hold because* $x + y$ *and* $\mathsf{f}(x + y, y + x)$ *are* $\mathcal{R}$*-normal forms which are not* AC *equivalent.*

3 Peak-and-Cliff Decreasingness

In the following, we assume that equivalence relations $\sim$ are defined as the reflexive and transitive closure of a symmetric relation $\vdash\!\dashv$, so $\sim \,=\, \vdash\!\dashv^*$. We refer to conversions of the form $\leftarrow \cdot \vdash\!\dashv$ or $\vdash\!\dashv \cdot \to$ as *local cliffs*. Furthermore, we assume that steps are labeled with labels from a set I, so let $\mathcal{A} = \langle A, \{\to_\alpha\}_{\alpha \in I}\rangle$ be an ARS and $\sim \,=\, (\bigcup\{\vdash\!\dashv_\alpha \mid \alpha \in I\})^*$ an equivalence relation on A.

Definition 1. *The* ARS $\mathcal{A}$ *is* peak-and-cliff decreasing *if there is a well-founded order* $>$ *on* I *such that for all* $\alpha, \beta \in I$ *the inclusions*

$$ {}_\alpha\!\leftarrow \cdot \to_\beta \;\subseteq\; \overset{*}{\underset{\vee\alpha\beta}{\Longleftrightarrow}} \qquad\qquad {}_\alpha\!\leftarrow \cdot \vdash\!\dashv_\beta \;\subseteq\; \overset{*}{\underset{\vee\alpha}{\Longleftrightarrow}} \cdot \overset{=}{\underset{\beta}{\leftarrow}} $$

hold. Here $\vee\alpha\beta$ *denotes the set* $\{\gamma \in I \mid \alpha > \gamma \text{ or } \beta > \gamma\}$ *and if* $J \subseteq I$ *then* $\to_J$ *denotes* $\bigcup\{\to_\gamma \mid \gamma \in J\}$*. We abbreviate* $\vee\alpha\alpha$ *to* $\vee\alpha$*.*

In the remainder of this section, we show that peak-and-cliff decreasingness implies the Church–Rosser modulo $\sim$ property.

Lemma 2. *Every conversion modulo* $\sim$ *is a valley modulo* $\sim$ *or contains a local peak or cliff:*

$$\Leftrightarrow^* \;\subseteq\; \downarrow^{\sim} \cup \Leftrightarrow^* \cdot \leftarrow \cdot \to \cdot \Leftrightarrow^* \cup \Leftrightarrow^* \cdot \vdash\!\dashv \cdot \to \cdot \Leftrightarrow^* \cup \Leftrightarrow^* \cdot \leftarrow \cdot \vdash\!\dashv \cdot \Leftrightarrow^*$$

Proof. We define $\leftharpoonup\!\!\rightharpoonup \;=\; \Leftrightarrow^* \cdot \leftarrow \cdot \rightarrow \cdot \Leftrightarrow^* \cup \Leftrightarrow^* \cdot \vdash\!\dashv \cdot \rightarrow \cdot \Leftrightarrow^* \cup \Leftrightarrow^* \cdot \leftarrow \cdot \vdash\!\dashv \cdot \Leftrightarrow^*$ in order to simplify the notation. Suppose $a \Leftrightarrow^n b$. We show that $a \downarrow^\sim b$ or $a \leftharpoonup\!\!\rightharpoonup b$ by induction on n. If $n = 0$ then $a = b$ and therefore also $a \downarrow^\sim b$. If $n > 0$ then $a \Leftrightarrow c \Leftrightarrow^{n-1} b$ for some c. The induction hypothesis yields $c \downarrow^\sim b$ or $c \leftharpoonup\!\!\rightharpoonup b$. In the latter case we are already done because $\Leftrightarrow \cdot \leftharpoonup\!\!\rightharpoonup \subseteq \leftharpoonup\!\!\rightharpoonup$. In the former case, we distinguish between three subcases: $a \rightarrow c$, $a \leftarrow c$ or $a \sim c$. If $a \rightarrow c$, we immediately obtain $a \downarrow^\sim c$. For the remaining two cases, note that there exists a k such that $c \rightarrow^k \cdot \sim \cdot {}^*\!\!\leftarrow b$. We continue with a case analysis on k:

- $k = 0$: If $a \leftarrow c$ we have $a \leftarrow c \sim c' \;{}^*\!\!\leftarrow b$ for some c'. Now either $c = c'$ and $a \downarrow^\sim b$ or $c \vdash\!\dashv \cdot \sim c'$ and therefore $a \leftharpoonup\!\!\rightharpoonup b$. If $a \sim c$ we have $a \downarrow^\sim b$ because $\sim$ is transitive.
- $k > 0$: If $a \leftarrow c$ then there exists a c' such that $a \leftarrow c \rightarrow c' \Leftrightarrow^* b$ and therefore $a \leftharpoonup\!\!\rightharpoonup b$. Finally, if $a \sim c$ then $a \sim c \rightarrow c' \Leftrightarrow^* b$ for some c'. If $a = c$ then we obtain $a \downarrow^\sim b$ from the induction hypothesis as there is a conversion between a and b of length $n - 1$. Otherwise, $a \sim \cdot \vdash\!\dashv c$ and therefore $a \leftharpoonup\!\!\rightharpoonup b$. □

The proof of the following theorem is based on a well-founded order on multisets. We denote the multiset extension of an order $>$ by $>_{\mathsf{mul}}$. It is well-known that the multiset extension of a well-founded order is also well-founded.

Theorem 1. *If $\mathcal{A}$ is peak-and-cliff decreasing then $\mathcal{A}$ is Church–Rosser modulo $\sim$.*

Proof. With every conversion C we associate a multiset M_C consisting of labels of its rewrite and equivalence relation steps. Since $\mathcal{A}$ is peak-and-cliff decreasing, there is a well-founded order $>$ on I which allows us to replace conversions C of the forms ${}_\alpha\!\!\leftarrow \cdot \rightarrow_\beta$, ${}_\alpha\!\!\leftarrow \cdot \vdash\!\dashv_\beta$ and $\vdash\!\dashv_\beta \cdot \rightarrow_\alpha$ by conversions C' where $M_C >_{\mathsf{mul}} M_{C'}$. Hence, we prove that $\mathcal{A}$ is Church–Rosser modulo $\sim$, i.e., $\Leftrightarrow^* \subseteq \downarrow^\sim$, by well-founded induction on $>_{\mathsf{mul}}$. Consider a conversion $a \Leftrightarrow^* b$ which we call C. By Lemma 2 we either have $a \downarrow^\sim b$ (which includes the case that C is empty) or one of the following cases holds:

$$a \Leftrightarrow^* \cdot \leftarrow \cdot \rightarrow \cdot \Leftrightarrow^* b \qquad a \Leftrightarrow^* \cdot \leftarrow \cdot \vdash\!\dashv \cdot \Leftrightarrow^* b \qquad a \Leftrightarrow^* \cdot \vdash\!\dashv \cdot \rightarrow \cdot \Leftrightarrow^* b$$

If $a \downarrow^\sim b$ we are immediately done. In the remaining cases, we have a local peak or cliff with concrete labels α and β, so $M_C = \Gamma_1 \uplus \{\alpha, \beta\} \uplus \Gamma_2$. Since $\mathcal{A}$ is peak-and-cliff decreasing, there is a conversion C' with $M_{C'} = \Gamma_1 \uplus \Gamma \uplus \Gamma_3$ where $\{\alpha, \beta\} >_{\mathsf{mul}} \Gamma$. Hence, $M_C >_{\mathsf{mul}} M_{C'}$ and we finish the proof by applying the induction hypothesis. □

For the main result of this paper, a simpler version of peak-and-cliff decreasingness suffices.

Definition 2. *Let $\mathcal{A} = \langle A, \rightarrow \rangle$ be an* ARS *equipped with a $\sim$-compatible well-founded order $>$ on A and $\sim = \vdash\!\dashv^*$ an equivalence relation on A. We write $b \xrightarrow{a} c$ ($b \overset{a}{\vdash\!\dashv} c$) if $b \rightarrow c$ ($b \vdash\!\dashv c$) and $b \sim a$. We say that $\mathcal{A}$ is* source decreasing modulo $\sim$ *if the inclusions*

$$\leftarrow a \rightarrow \;\subseteq\; \overset{*}{\underset{\vee a}{\Longleftrightarrow}} \qquad\qquad \leftarrow a \vdash\!\dashv \;\subseteq\; \overset{*}{\underset{\vee a}{\Longleftrightarrow}} \cdot \overset{=}{\underset{a}{\longleftarrow}}$$

hold for all $a \in A$. Here $\leftarrow a \rightarrow$ ($\leftarrow a \vdash\!\dashv$) denotes the binary relation consisting of all pairs (b, c) such that $a \rightarrow b$ and $a \rightarrow c$ ($a \vdash\!\dashv c$). Furthermore, $\overset{*}{\underset{\vee a}{\Longleftrightarrow}}$ denotes the binary relation consisting of all pairs of elements which are connected by a conversion where each step is labeled by an element smaller than a.

Corollary 1. *Every* ARS *which is source decreasing modulo $\sim$ is Church–Rosser modulo $\sim$.*

Proof. In the definition of peak decreasingness we set $I = A$. Note that this implies $\alpha = \beta$ for all local peaks and cliffs. Hence, the ARS is peak-and-cliff decreasing and we can conclude by an appeal to Theorem 1. □

4 Prime Critical Pairs

In the following, $\mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm})$ denotes the restriction of $\mathsf{CP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm})$ to prime critical pairs but where irreducibility is always checked with respect to $\mathcal{R}$, i.e., the critical peaks $t\ {}_{\mathcal{R}}^{p}\!\leftarrow s \leftrightarrow_{\mathcal{B}}^{\epsilon} u$ and $t' \leftrightarrow_{\mathcal{B}}^{p} s \rightarrow_{\mathcal{R}}^{\epsilon} u'$ are both prime if proper subterms of $s|_p$ are irreducible with respect to $\mathcal{R}$.

Example 2. *Consider the TRS $\mathcal{R}$ consisting of the rewrite rules*

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

and let $\mathcal{B} = \{x+y \approx y+x\}$. The TRS *$\mathcal{R}$ admits six (modulo symmetry) critical peaks of the form $t\ {}_{\mathcal{R}}^{p}\!\leftarrow s \rightarrow_{\mathcal{R}}^{\epsilon} u$:*

$$\begin{array}{cccccc}
\underline{\mathsf{f}(\mathsf{a}+\mathsf{a})} & \underline{\mathsf{f}(\mathsf{a}+\mathsf{b})} & \underline{\mathsf{f}(\mathsf{b}+\mathsf{a})} & \underline{\mathsf{f}(\mathsf{b}+\mathsf{b})} & \mathsf{f}(\underline{\mathsf{a}}+x) & \mathsf{f}(x+\underline{\mathsf{a}}) \\
\swarrow\ \searrow & \swarrow\ \searrow & \swarrow\ \searrow & \swarrow\ \searrow & \swarrow\ \searrow & \swarrow\ \searrow \\
\mathsf{a}\qquad\mathsf{a} & \mathsf{a}\qquad\mathsf{b} & \mathsf{a}\qquad\mathsf{b} & \mathsf{b}\qquad\mathsf{b} & \mathsf{f}(\mathsf{b}+x)\quad x & \mathsf{f}(x+\mathsf{b})\quad x
\end{array}$$

Here the positions p in s are indicated by underlining. The first three peaks are not prime due to the reducible proper subterm a *in $s|_p$. So $\mathsf{PCP}(\mathcal{R}) = \{\mathsf{b} \approx \mathsf{b}, \mathsf{f}(\mathsf{b}+x) \approx x, \mathsf{f}(x+\mathsf{b}) \approx x\}$. Similarly, $\mathcal{R}$ and $\mathcal{B}$ admit four critical peaks of the forms $t\ {}_{\mathcal{R}}^{p}\!\leftarrow s \leftrightarrow_{\mathcal{B}}^{\epsilon} u$ and $t \leftrightarrow_{\mathcal{B}}^{p} s \rightarrow_{\mathcal{R}}^{\epsilon} u$:*

$$\begin{array}{cccc}
\mathsf{f}(\underline{\mathsf{a}+x}) & \mathsf{f}(\underline{x+\mathsf{a}}) & \mathsf{f}(\underline{\mathsf{b}+x}) & \mathsf{f}(\underline{x+\mathsf{b}}) \\
\swarrow\ \searrow & \swarrow\ \searrow & \swarrow\ \searrow & \swarrow\ \searrow \\
\mathsf{f}(x+\mathsf{a})\quad x & \mathsf{f}(\mathsf{a}+x)\quad x & \mathsf{f}(x+\mathsf{b})\quad x & \mathsf{f}(\mathsf{b}+x)\quad x
\end{array}$$

Here the first two peaks are not prime and thus $\mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm}) = \{\mathsf{f}(\mathsf{b}+x) \approx x, \mathsf{f}(x+\mathsf{b}) \approx x\}$.

Definition 3. *Given a* TRS *$\mathcal{R}$ and terms s, t and u, we write $t \bigtriangledown_s u$ if $s \rightarrow_{\mathcal{R}}^{+} t$, $s \rightarrow_{\mathcal{R}}^{+} u$, and $t \downarrow_{\mathcal{R}} u$ or $t \leftrightarrow_{\mathsf{PCP}(\mathcal{R})} u$. We write $t \bigtriangledown_s^{\sim} u$ if $s \rightarrow_{\mathcal{R}}^{+} t$, $s \sim u$ and $t \downarrow_{\mathcal{R}}^{\sim} u$ or $t \leftrightarrow_{\mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm})} u$. Furthermore, ${}_{s}^{\sim}\!\bigtriangledown = \{(u,t) \mid t \bigtriangledown_s^{\sim} u\}$.*

Note that the joinability of ordinary critical peaks is not affected by incorporating $\mathcal{B}$ into conversions. Hence, the following result is taken from [2, Lemma 2.15] and therefore stated without a proof.

Lemma 3. *Let $\mathcal{R}$ be a* TRS. *If $t \xleftarrow[\mathcal{R}]{p} s \xrightarrow[\mathcal{R}]{\epsilon} u$ is a critical peak then $t \bigtriangledown_s^2 u$.* ☐

Lemma 4. *Let $\mathcal{R}$ be a* TRS. *The following two inclusions hold:*

1. *If $t \xleftarrow[\mathcal{R}]{p} s \xleftrightarrow[\mathcal{B}]{\epsilon} u$ is a critical peak then $t \bigtriangledown_s \cdot \bigtriangledown_s^{\sim} u$.*

2. *If $t \xleftrightarrow[\mathcal{B}]{p} s \xrightarrow[\mathcal{R}]{\epsilon} u$ is a critical peak then $t\ {}_{s}^{\sim}\!\bigtriangledown \cdot \bigtriangledown_s u$.*

Proof. We only prove (1) as the other case is symmetrical. If all proper subterms of $s|_p$ are in normal form with respect to $\rightarrow_{\mathcal{R}}$, $t \approx u \in \mathsf{PCP}(\mathcal{R},\mathcal{B}^{\pm})$ which establishes $t \bigtriangledown_s^{\sim} u$. Since also $t \bigtriangledown_s t$, we obtain the desired result. Otherwise, there are a position $q > p$ and a term v such that $s \xrightarrow[\mathcal{R}]{q} v$ and all proper subterms of $s|_q$ are in normal form with respect to $\rightarrow_{\mathcal{R}}$. Together with Lemma 1 we obtain either $v \downarrow_{\mathcal{R}}^{\sim} u$ or $v \leftrightarrow_{\mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm})} u$. In both cases $v \bigtriangledown_s^{\sim} u$ holds. A similar case analysis applies to the local peak $t \xleftarrow[\mathcal{R}]{p} s \xrightarrow[\mathcal{R}]{q} v$: By the Critical Pair Lemma, either $t \downarrow_{\mathcal{R}} v$ or $t \leftrightarrow_{\mathsf{CP}(\mathcal{R})} v$. In the latter case

$$v|_p \xleftarrow[\mathcal{R}]{q\backslash p} s|_p \xrightarrow[\mathcal{R}]{\epsilon} t|_p$$

is an instance of a prime critical peak as $q > p$ and all proper subterms of $s|_q$ are in normal form with respect to $\to_{\mathcal{R}}$. Closure of rewriting under contexts and substitutions yields $t \leftrightarrow_{\mathsf{PCP}(\mathcal{R})} v$. Therefore, we have $t \mathrel{\triangledown_s} v$ in both cases, concluding the proof. □

The following lemma generalizes the previous results of this section to arbitrary local peaks and cliffs.

Lemma 5. *Let $\mathcal{R}$ be a left-linear* TRS. *The following two properties hold:*

1. *If $t \mathrel{{}_{\mathcal{R}}{\leftarrow}} s \to_{\mathcal{R}} u$ then $t \mathrel{\triangledown_s^2} u$.*
2. *If $t \mathrel{{}_{\mathcal{R}}{\leftarrow}} s \leftrightarrow_{\mathcal{B}} u$ then $t \mathrel{\triangledown_s} \cdot \mathrel{\triangledown_s^{\sim}} u$.*

Proof. We only prove (2) as the proof of (1) (which depends on the Critical Pair Lemma) can be found in [2, Lemma 2.16]. Let $t \mathrel{{}_{\mathcal{R}}{\leftarrow}} s \leftrightarrow_{\mathcal{B}} u$. From Lemma 1 we obtain $t \downarrow_{\mathcal{R}}^{\sim} u$ or $t \leftrightarrow_{\mathsf{CP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm})} u$. In the former case we are done as $t \mathrel{\triangledown_s} u \mathrel{\triangledown_s} u$. For the latter case we further distinguish between the two subcases $t \to_{\mathsf{CP}(\mathcal{R},\mathcal{B}^{\pm})} u$ and $u \to_{\mathsf{CP}(\mathcal{B}^{\pm},\mathcal{R})} t$. Note that this list of subcases is exhaustive due to the direction of the local cliff. If $t \to_{\mathsf{CP}(\mathcal{R},\mathcal{B}^{\pm})} u$, $t \mathrel{\triangledown_s} \cdot \mathrel{\triangledown_s^{\sim}} u$ follows from Lemma 4(1) and closure of rewriting under contexts and substitutions. If $u \to_{\mathsf{CP}(\mathcal{B}^{\pm},\mathcal{R})} t$, $u \mathrel{{}_s^{\sim}{\triangledown}} \cdot \mathrel{\triangledown_s} t$ and therefore $t \mathrel{\triangledown_s} \cdot \mathrel{\triangledown_s^{\sim}} u$ follows from Lemma 4(2) as well as closure of rewriting under contexts and substitutions. □

Now, we are able to prove the main result of this section, a novel necessary and sufficient condition for the Church–Rosser property modulo an equational theory $\mathcal{B}$ which strengthens the original result from [3] to prime critical pairs.

Theorem 2. *A left-linear* TRS $\mathcal{R}$ *which is terminating modulo $\mathcal{B}$ is Church–Rosser modulo $\mathcal{B}$ if and only if* $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm}) \subseteq \downarrow_{\mathcal{R}}^{\sim}$.

Proof. The "only if" direction is trivial. For a proof of the "if" direction, we show that $\mathcal{R}$ is source decreasing; the Church–Rosser property modulo $\mathcal{B}$ is then an immediate consequence of Corollary 1. From the termination of $\mathcal{R}$ modulo $\mathcal{B}$ we obtain the well-founded order $> = \to_{\mathcal{R}/\mathcal{B}}^{+}$.

Consider an arbitrary local peak $t \mathrel{{}_{\mathcal{R}}{\leftarrow}} s \to_{\mathcal{R}} u$. Lemma 5(1) yields a term v such that $t \mathrel{\triangledown_s} v \mathrel{\triangledown_s} u$. Together with $\mathsf{PCP}(\mathcal{R}) \subseteq \downarrow_{\mathcal{R}}^{\sim}$ we obtain $t \downarrow_{\mathcal{R}}^{\sim} v \downarrow_{\mathcal{R}}^{\sim} u$. By definition, $s > t, v, u$ so the corresponding condition required by source decreasingness is fulfilled.

Now consider an arbitrary local cliff $t \mathrel{{}_{\mathcal{R}}{\leftarrow}} s \leftrightarrow_{\mathcal{B}} u$. Lemma 5(2) yields a term v such that $t \mathrel{\triangledown_s} v \mathrel{\triangledown_s^{\sim}} u$. Together with $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm}) \subseteq \downarrow_{\mathcal{R}}^{\sim}$ we obtain $t \downarrow_{\mathcal{R}}^{\sim} v \downarrow_{\mathcal{R}}^{\sim} u$. By definition, $s > t, v$ and $s \sim u$. The conversion between v and u is of the form $v \to_{\mathcal{R}}^{*} \cdot \sim \cdot \mathrel{{}_{\mathcal{R}}^{k}{\leftarrow}} u$ for some k. If $k = 0$ then all steps between v and u are labeled with terms which are smaller than s. If $k > 0$ then there exists a $w < s$ such that $v \to_{\mathcal{R}}^{*} \cdot \sim \cdot \mathrel{{}_{\mathcal{R}}^{k-1}{\leftarrow}} w \mathrel{{}_{\mathcal{R}}{\leftarrow}} u$. In this case all steps of the conversion are labeled with terms which are smaller than s except for the rightmost step which we may label with s. Hence, the corresponding condition required by source decreasingness is fulfilled in all cases. □

Example 3 (continued from Example 2)**.** *One can verify the termination of $\mathcal{R}/\mathcal{B}$ and the inclusion* $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R},\mathcal{B}^{\pm}) \subseteq \downarrow_{\mathcal{R}}^{\sim}$. *By Theorem 2 the Church–Rosser modulo property holds.*

Finally, we show that the previous result does not hold if we just demand termination of $\mathcal{R}$. The counterexample shows this for the concrete case of AC and is based on Example 4.1.8 from [1] which uses an ARS. Note that the usage of prime critical pairs instead of critical pairs has no effect.

Example 4. *Consider the* TRS $\mathcal{R}$ *consisting of the rules*

$$\begin{array}{lll} (\mathsf{b}+\mathsf{a})+\mathsf{a} \to \mathsf{a}+(\mathsf{a}+\mathsf{b}) & (\mathsf{a}+\mathsf{b})+\mathsf{a} \to \mathsf{a}+(\mathsf{a}+\mathsf{b}) & (\mathsf{a}+\mathsf{a})+\mathsf{b} \to \mathsf{a}+(\mathsf{a}+\mathsf{b}) \\ \mathsf{a}+(\mathsf{a}+\mathsf{b}) \to \mathsf{b}+(\mathsf{a}+\mathsf{a}) & \mathsf{b}+(\mathsf{a}+\mathsf{a}) \to \mathsf{c} & \\ \mathsf{a}+(\mathsf{a}+\mathsf{b}) \to \mathsf{a}+(\mathsf{b}+\mathsf{a}) & \mathsf{a}+(\mathsf{b}+\mathsf{a}) \to \mathsf{d} & \end{array}$$

where $+$ *is an* AC *function symbol. Clearly, the (prime) critical pairs of* $\mathcal{R}$ *are joinable modulo* AC *because* $\mathsf{b}+(\mathsf{a}+\mathsf{a}) \sim_{\mathsf{AC}} \mathsf{a}+(\mathsf{b}+\mathsf{a})$. *For* $\mathsf{PCP}^{\pm}(\mathcal{R},\mathsf{AC}^{\pm})$ *we only have to consider the rules which rewrite to* c *and* d *respectively since all other rules only involve* AC *equivalent terms. Modulo symmetry, these (prime) critical pairs are*

$$\begin{array}{rclrclrcl} \mathsf{c} & \approx & \mathsf{b}+(\mathsf{a}+\mathsf{a}) & \mathsf{c} & \approx & (\mathsf{a}+\mathsf{a})+\mathsf{b} & \mathsf{c} & \approx & (\mathsf{b}+\mathsf{a})+\mathsf{a} \\ \mathsf{c}+x & \approx & \mathsf{b}+((\mathsf{a}+\mathsf{a})+x) & x+\mathsf{c} & \approx & (x+\mathsf{b})+(\mathsf{a}+\mathsf{a}) & & & \\ \mathsf{d} & \approx & \mathsf{a}+(\mathsf{a}+\mathsf{b}) & \mathsf{d} & \approx & (\mathsf{b}+\mathsf{a})+\mathsf{a} & \mathsf{d} & \approx & (\mathsf{a}+\mathsf{b})+\mathsf{a} \\ \mathsf{d}+x & \approx & \mathsf{a}+((\mathsf{b}+\mathsf{a})+x) & x+\mathsf{d} & \approx & (x+\mathsf{a})+(\mathsf{b}+\mathsf{a}) & & & \end{array}$$

which can be joined by adding the rules

$$\begin{array}{ll} \mathsf{b}+((\mathsf{a}+\mathsf{a})+x) \to (\mathsf{b}+(\mathsf{a}+\mathsf{a}))+x & (x+\mathsf{b})+(\mathsf{a}+\mathsf{a}) \to x+(\mathsf{b}+(\mathsf{a}+\mathsf{a})) \\ \mathsf{a}+((\mathsf{b}+\mathsf{a})+x) \to (\mathsf{a}+(\mathsf{b}+\mathsf{a}))+x & (x+\mathsf{a})+(\mathsf{b}+\mathsf{a}) \to x+(\mathsf{a}+(\mathsf{b}+\mathsf{a})) \end{array}$$

to $\mathcal{R}$. *The new (prime) critical pairs in* $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R},\mathsf{AC}^{\pm})$ *are trivially joinable modulo* AC *as they are* AC *equivalent. To sum up,* $\mathsf{PCP}(\mathcal{R}) \cup \mathsf{PCP}^{\pm}(\mathcal{R},\mathsf{AC}^{\pm}) \subseteq \downarrow_{\mathcal{R}}^{\sim}$. *Termination of* $\mathcal{R}$ *can be checked by e.g.* $\mathsf{T_TT_2}$, *but the loop*

$$\mathsf{a}+(\mathsf{a}+\mathsf{b}) \to_{\mathcal{R}} \mathsf{a}+(\mathsf{b}+\mathsf{a}) \sim_{\mathsf{AC}} \mathsf{a}+(\mathsf{a}+\mathsf{b})$$

shows that $\mathcal{R}$ *is not* AC *terminating. We have* $\mathsf{c} \Leftrightarrow^* \mathsf{d}$ *but not* $\mathsf{c} \downarrow_{\mathcal{R}}^{\sim} \mathsf{d}$ *as the terms are normal forms and not* AC *equivalent. Hence,* $\mathcal{R}$ *is not Church–Rosser modulo* AC.

References

[1] Jürgen Avenhaus. *Reduktionssysteme*. Springer Berlin Heidelberg, 1995. In German. doi:10.1007/978-3-642-79351-6.

[2] Nao Hirokawa, Aart Middeldorp, Christian Sternagel, and Sarah Winkler. Abstract completion, formalized. *Logical Methods in Computer Science*, 15(3):19:1–19:42, 2019. doi:10.23638/LMCS-15(3:19)2019.

[3] Gérard Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the ACM*, 27(4):797–821, 1980. doi:10.1145/322217.322230.

[4] Deepak Kapur, David R. Musser, and Paliath Narendran. Only prime superpositions need be considered in the Knuth–Bendix completion procedure. *Journal of Symbolic Computation*, 6(1):19–36, 1988. doi:10.1016/S0747-7171(88)80019-1.

[5] Johannes Niederhauser, Nao Hirokawa, and Aart Middeldorp. Left-linear completion with AC axioms. In Brigitte Pientka and Cesare Tinelli, editors, *Proc. 29th International Conference on Automated Deduction*, volume 14132 of *Lecture Notes in Computer Science*, 2023. To appear.