A Proof Order for Decreasing Diagrams*

Bertram Felgenhauer
Institute of Computer Science, University of Innsbruck, Austria
bertram.felgenhauer@uibk.ac.at

Abstract

In this note we describe a well-founded proof order that entails the decreasing diagrams technique, i.e., it orders peaks of locally decreasing diagrams above their joining sequences. We also investigate an extension that promises to be useful for proving confluence modulo.

Unrelated to this proof order we also present an example showing that witnesses for non-confluence can not always be found by starting from critical pairs alone, even for linear TRSs.

1 Introduction

In this note we revisit the decreasing diagrams technique [8] for proving confluence. Our confluence proof is based on a proof order, which we use to prove termination of the *proof transformation system* defined by the locally decreasing diagrams. A similar approach is used in the correctness proof for completion by Bachmair and Dershowitz [2]. The distinguishing property of a proof order is that proof concatenation becomes a monotone operation, so that admissibility of a proof transformation $P \Rightarrow Q$ can be established by comparing P to Q. This simplifies finding new proof transformations.

This work is also inspired by [6], where Jouannaud and van Oostrom define a well-founded order on proofs in order to establish that local decreasingness implies confluence. However, it is not monotone for concatenation, and therefore not a proof order. Hence they have to consider whole proofs when showing that eliminating a local peak by a locally decreasing diagram results in a decrease in the proof measure. Another influence comes from Aoto and Toyama [1], who prove an abstract lemma for confluence modulo by proof rewriting arguments.

The remainder of this paper is structured as follows: In Section 2, we introduce our proof order abstracted to *proof strings*. We use this order to re-prove validity of the decreasing diagrams technique in Section 3. In Section 4, we explore admissible proof transformations that are helpful for proving confluence modulo, leading to a generalization of a result by Ohlebusch [7].

In Section 5 we depart from the topic of proof orders and proving confluence and turn to establishing non-confluence. An obvious idea for finding counterexamples to confluence is to start with critical peaks and try to find reducts which are not joinable. It is well-known that this is not sufficient for non-left-linear TRSs (Huet, [5]). We give an example that shows that this approach is insufficient even for linear TRSs.

1.1 Preliminaries

For the whole paper, we fix a set of labels $\mathcal{L}$ equipped with a well-founded order $\succ$. Given labels $\alpha, \gamma \in \mathcal{L}$, we define $\Upsilon\alpha = \{\gamma \in \mathcal{L} \mid \alpha \succ \gamma\}$ and $\Upsilon\alpha, \gamma = \Upsilon\alpha \cup \Upsilon\gamma$.

We use $\to$ ($\mapsto$) to denote (symmetric) rewrite relations, with the usual convention that $\leftarrow$, $\leftrightarrow$, $\xrightarrow{=}$, $\xrightarrow{*}$ denote the inverse, symmetric closure, reflexive closure and reflexive, transitive closure of $\to$, respectively. Given a family $(\underset{\alpha}{\to})_{\alpha\in\mathcal{L}}$ and $S \subseteq \mathcal{L}$, we let $\underset{S}{\to} = \bigcup_{\alpha\in S} \underset{\alpha}{\to}$.

The lexicographic product of strict partial orders $>_1$ and $>_2$ is denoted by $>_1 \times_{\text{lex}} >_2$, while $>_{\text{mul}}$ is the multiset extension of $>$. We use $\{\!|$ and $|\!\}$ as brackets for multisets, e.g., $\{\!|\alpha, \alpha, \gamma|\!\}$.

*This research was supported by the Austrian Science Fund (FWF) project P22467-N23.

2 Ordering Proof Strings

This section is devoted to developing our proof order in an abstract setting, where instead of rewrite proofs we consider only proof strings, abstracting from the objects of abstract rewrite systems. The resulting *proof string order* is defined in two stages. First we map proof strings to nested multisets of pairs. Then we compare these multisets by an order related to the recursive path order.

Definition 1. We introduce proof strings, an abstract notation for proofs.

- A *(proof) step* is either a *left step* $\overleftarrow{\alpha}$ or a *right step* $\overrightarrow{\alpha}$, where $\alpha \in \mathcal{L}$. We define $\overleftrightarrow{S} = \{\overleftarrow{\alpha}, \overrightarrow{\alpha} \mid \alpha \in S\}$ for $S \subseteq \mathcal{L}$ and use $\overleftrightarrow{\alpha}$ for variables ranging over steps ($\overleftrightarrow{\alpha} \in \overleftrightarrow{\mathcal{L}}$), and α for the corresponding labels. We lift $\succ$ to steps by letting $\overleftrightarrow{\alpha} \succ \overleftrightarrow{\gamma}$ iff $\alpha \succ \gamma$.
- A *(proof) string* is a sequence of steps. The set of all proof strings is denoted by $\mathcal{P}$, and $\cdot$ is the concatenation operation on strings. The empty proof is ϵ.
- The *inverse* $(\overleftrightarrow{\alpha})^{-1}$ of a step $\overleftrightarrow{\alpha}$ is defined by $(\overrightarrow{\alpha})^{-1} = \overleftarrow{\alpha}$ and $(\overleftarrow{\alpha})^{-1} = \overrightarrow{\alpha}$. This operation extends to proof strings by $\epsilon^{-1} = \epsilon$, $(P \cdot \overleftrightarrow{\alpha})^{-1} = (\overleftrightarrow{\alpha})^{-1} \cdot P^{-1}$.

Remark 1. Together with inverse and concatenation, proof strings form an involutive monoid (van Oostrom, IWC 2012).

Definition 2. A well-founded order $\gg$ on strings is a *proof string order* if string concatenation and inverse are strictly monotone, i.e., $P \gg Q$ implies $P \cdot R \gg Q \cdot R$, $R \cdot P \gg R \cdot Q$ and $P^{-1} \gg Q^{-1}$.

Next we show how proof strings are mapped to nested multisets.

Definition 3. We define operations $[\cdot]^l$, $[\cdot]^r$ and $[\cdot]^m$, mapping proof strings to (nested) multisets of pairs of steps and transformed strings, inductively as follows:

- $[\epsilon]^l = \varnothing$, $[\overleftarrow{\alpha} \cdot P]^l = \{\!\{(\overleftarrow{\alpha}, [P]^m)\}\!\} \cup [P]^l$, $[\overrightarrow{\alpha} \cdot P]^l = [P]^l$, collecting left steps and the transformations of the substring following each left step into a multiset.
- $[\epsilon]^r = \varnothing$, $[P \cdot \overrightarrow{\alpha}]^r = \{\!\{(\overrightarrow{\alpha}, [P]^m)\}\!\} \cup [P]^r$, $[P \cdot \overleftarrow{\alpha}]^r = [P]^r$, collecting right steps and the transformations of their preceding substrings.
- $[P]^m = [P]^l \cup [P]^r$.

Example 2. We have $[\overleftarrow{\alpha} \cdot \overrightarrow{\gamma}]^m = \{\!\{(\overleftarrow{\alpha}, [\overrightarrow{\gamma}]^m), (\overrightarrow{\gamma}, [\overleftarrow{\alpha}]^m)\}\!\} = \{\!\{(\overleftarrow{\alpha}, \{\!\{(\overrightarrow{\gamma}, \varnothing)\}\!\}), \{\!\{(\overrightarrow{\gamma}, \{\!\{(\overleftarrow{\alpha}, \varnothing)\}\!\})\}\!\}$.

The result of the transformation $[\cdot]^m$ grows exponentially in the string length, but it is highly redundant: each multiset occurring in $[P]^m$ corresponds to a substring of P.

Lemma 4. *The definition of* $[P]^m$ *is symmetric. Formally, we have* $[P^{-1}]^m = ([P]^m)^{-1}$ *and* $[P^{-1}]^l = ([P]^r)^{-1}$*, where the inverse on nested multisets is defined recursively by*

$$s^{-1} = \{\!\{((\overleftrightarrow{\alpha})^{-1}, t^{-1}) \mid (\overleftrightarrow{\alpha}, t) \in s\}\!\}$$

Proof. By induction on the length of P. □

Definition 5. We order these multisets by $\succ_\oplus$, defined inductively: $s \succ_\oplus \{\!\{(\overleftrightarrow{\gamma_1}, t_1), \ldots, (\overleftrightarrow{\gamma_m}, t_m)\}\!\}$ if $s \succ_\oplus t_j$ for $1 \le j \le m$ and $s \gg_{\text{mul}} t$, where $\gg = \succ \times_{\text{lex}} \succ_\oplus$. Furthermore, we define the proof string order $\succ_\bullet$ as follows:

$$P \succ_\bullet Q \quad \text{iff} \quad [P]^m \succ_\oplus [Q]^m$$

Lemma 6. *The relations $\succ_\oplus$ and $\succ_\bullet$ are well-founded partial orders.*

Proof. We only have to establish that $\succ_\oplus$ is a well-founded order. First we show transitivity, i.e., that $s \succ_\oplus t \succ_\oplus u$ implies $s \succ_\oplus u$, by induction on u. Assume that $u = \{\!\{(\overleftrightarrow{\eta_1}, u_1), \dots, (\overleftrightarrow{\eta_n}, u_n)\}\!\}$. Now from $t \succ_\oplus u$ follows $t \succ_\oplus u_i$, hence $s \succ_\oplus u_i$ by the induction hypothesis. Furthermore with $\gg = \succ \times_{\text{lex}} \succ_\oplus$, we have $s \gg_{\text{mul}} t \gg_{\text{mul}} u$, and therefore $s \gg_{\text{mul}} u$ by the induction hypothesis, because the transitivity proofs for $\times_{\text{lex}}$ and $\cdot_{\text{mul}}$ only rely on the transitivity for elements actually present in the pairs respectively multisets. Hence $s \succ_\oplus u$, as claimed.

Now it remains to show that $\succ_\oplus$ is well-founded. In order to do that, we exhibit a relation between $\succ_\oplus$ and the recursive path order with custom status as introduced by Ferreira [3]. To this end, we define a signature $\mathcal{F}$, a mapping $[\cdot]^t$ of nested multisets to ground terms over $\mathcal{F}$ and a lifting Λ on relations between terms over $\mathcal{F}$ as follows:

- $\mathcal{F} = \mathcal{P}$, where each proof string in $\mathcal{F}$ has its length as arity.
- $[\{\!\{(\overleftrightarrow{\alpha_1}, s_1), \dots, (\overleftrightarrow{\alpha_n}, s_n)\}\!\}]^t = \overleftrightarrow{\alpha_1} \dots \overleftrightarrow{\alpha_n}([s_1]^t, \dots, [s_n]^t)$, using any order of the multiset elements.
- $s >^\Lambda t$, if and only if $s^\lambda \gg_{\text{mul}} t^\lambda$, where $[\overleftrightarrow{\alpha_1} \dots \overleftrightarrow{\alpha_n}(s_1, \dots, s_n)]^\lambda = \{\!\{(\overleftrightarrow{\alpha_1}, s_1), \dots, (\overleftrightarrow{\alpha_n}, s_n)\}\!\}$ and $\gg = \succ \times_{\text{lex}} >$.

It is easy to see that Λ is a *term lifting* [3, Definition 3.16] and also a *status* [3, Definition 4.7]. Let $\gg_\bullet$ be the rpo defined by this status, namely: $s \gg_\bullet t$ iff $s = \overleftrightarrow{\alpha_1} \dots \overleftrightarrow{\alpha_n}(s_1, \dots, s_n)$, $t = \overleftrightarrow{\gamma_1} \dots \overleftrightarrow{\gamma_m}(t_1, \dots, t_m)$ and

1. $s_i = t$ or $s_i \gg_\bullet t$ for some $1 \le i \le n$, or
2. $s \gg_\bullet t_j$ for $1 \le j \le m$ and $s \gg_\bullet^\Lambda t$.

By the properties of rpo [3, Theorem 4.19], $\gg_\bullet$ is well-founded. We conclude that $\succ_\oplus$ is well-founded by noting that $[P]^m \succ_\oplus [Q]^m$ implies $[[P]^m]^t \gg_\bullet [[Q]^m]^t$, which can be shown by unfolding the definitions of $\succ_\oplus$, $[\cdot]^t$ and $\gg_\bullet$, using only the second case in the definition of $\gg_\bullet$. Note in particular that each application $[\cdot]^\lambda$ reverses one level of the transformation $[\cdot]^t$. □

Remark 3. It would be nice to avoid the complications of using a general status for rpo. However, both the lexicographic and the multiset comparisons are essential, and splitting the signature $\mathcal{F}$ into several levels conflicts with the requirement that if $s \gg f(t_1, \dots, t_n)$, then $s \gg t_i$ for all i.

Theorem 7. *The order $\succ_\bullet$ is a proof string order.*

Proof. By Lemma 6, $\succ_\bullet$ is a well-founded order. To see that string inverse is monotone with respect to $\succ_\bullet$, apply Lemma 4 and observe that $\succ_\oplus$ is invariant under inversion of steps.

For concatenation we first prove that it is monotone in the second argument, i.e., $Q \succ_\bullet Q'$ implies $P \cdot Q \succ_\bullet P \cdot Q'$. We proceed by induction on the length of P. If $P = \epsilon$, then there is nothing to prove. Otherwise, there are two cases to consider, $P = P' \cdot \overleftarrow{\alpha}$ and $P = P' \cdot \overrightarrow{\alpha}$. Their proofs are very similar, so we only handle the first case here.

Assume that $P = P' \cdot \overleftarrow{\alpha}$. We let $\gg = \succ \times_{\text{lex}} \succ_\oplus$. We prove by induction on Q that $[\overleftarrow{\alpha} \cdot Q]^m \gg_{\text{mul}} [\overleftarrow{\alpha} \cdot Q']^m$. Unfolding one level of $[\cdot]^m$, we can relate $[\overleftarrow{\alpha} \cdot Q]^m$ to $[Q]^m$:

$$[\overleftarrow{\alpha} \cdot Q]^m = \{\!\{(\overleftarrow{\alpha}, [Q]^m)\}\!\} \cup \{\!\{(\overleftarrow{\gamma}, [R]^m) \mid (\overleftarrow{\gamma}, [R]^m) \in [Q]^m\}\!\} \cup \{\!\{(\overrightarrow{\gamma}, [\overleftarrow{\alpha} \cdot R]^m) \mid (\overrightarrow{\gamma}, [R]^m) \in [Q]^m\}\!\}.$$

We say that $(\overleftarrow{\gamma}, [R]^m)$, $(\overrightarrow{\gamma}, [\overleftarrow{\alpha} \cdot R]^m)$ are derived from $(\overleftarrow{\gamma}, [R]^m)$, $(\overrightarrow{\gamma}, [R]^m)$, respectively.

We know by assumption that $[Q]^m \gg_\oplus [Q']^m$. Therefore, $(\overleftarrow{\alpha}, [Q]^m) \gg (\overleftarrow{\alpha}, [Q]^m)$ (which deals with the elements not derived from $[Q]^m$ or $[Q']^m$) and $[Q]^m \gg_{\mathrm{mul}} [Q']^m$. The latter multiset comparison can be established by comparing various elements of $[Q]^m$ and $[Q']^m$ using equality and $\gg$. These comparisons carry over to the derived elements in $[\overleftarrow{\alpha} \cdot Q]^m$ and $[\overleftarrow{\alpha} \cdot Q']^m$: Let $s = (\overleftrightarrow{\gamma}, [R]^m) \in [Q]^m$ and $t = (\overleftrightarrow{\gamma}', [R']^m) \in [Q']^m$. If $s = t$ then the derived elements are also equal. If $s \gg t$, there is only one interesting case: $\gamma = \gamma'$, $s = (\overrightarrow{\gamma}, [R]^m)$ and $t = (\overrightarrow{\gamma}, [R']^m)$, with derived elements $s' = (\overrightarrow{\gamma}, [\overleftarrow{\alpha} \cdot R]^m)$ and $t' = (\overrightarrow{\gamma}, [\overleftarrow{\alpha} \cdot R']^m)$. Since R is a proper subproof of Q, if $[R]^m \succ_\oplus [R']^m$, we conclude that $[\overleftarrow{\alpha} \cdot R]^m \succ_\oplus [\overleftarrow{\alpha} \cdot R]^m$ by the induction hypothesis. This concludes the proof of $[\overleftarrow{\alpha} \cdot Q]^m \gg_{\mathrm{mul}} [\overleftarrow{\alpha} \cdot Q']^m$.

Therefore, $\overleftarrow{\alpha} \cdot Q \succ_\bullet \overleftarrow{\alpha} \cdot Q'$ by definition and $P \cdot Q \succ_\bullet P \cdot Q'$ by the induction hypothesis.

Monotonicity of concatenation in its first argument now follows because $Q \succ_\bullet Q'$ implies $P^{-1} \cdot Q^{-1} \succ_\bullet P^{-1} \cdot (Q')^{-1}$. Inverting both sides yields $Q \cdot P \succ_\bullet Q' \cdot P$. □

3 Decreasing Diagrams

In this section, use the proof string order of Section 2 to give an alternative proof for the conversion version of the decreasing diagram technique [8]. First we establish the corresponding result for proof strings. We let S^* be the Kleene star of S and $S^= = S \cup \{\epsilon\}$.

Lemma 8. *The proof strings corresponding to the peaks and joins of locally decreasing diagrams are decreasing with respect to $\succ_\bullet$, that is,*

1. *if $P = \overleftarrow{\alpha}$ and $Q \in \overleftrightarrow{\Upsilon\alpha}^*$ then $P \succ_\bullet Q$, and*
2. *if $P = \overleftarrow{\alpha} \cdot \overrightarrow{\gamma}$ and $Q \in (\overleftrightarrow{\Upsilon\alpha})^* \cdot (\overrightarrow{\gamma})^= \cdot (\overleftrightarrow{\Upsilon\alpha, \gamma})^* \cdot (\overleftarrow{\alpha})^= \cdot (\overleftrightarrow{\Upsilon\gamma})^*$ then $P \succ_\bullet Q$.*

Proof. In both cases we show that $[P]^m \succ_\oplus [Q]^m$ by induction on the length of Q.

1. We have $[Q]^m = \{\!\{(\overleftrightarrow{\gamma_1}, t_1), \ldots, (\overleftrightarrow{\gamma_n}, t_n)\}\!\}$ for some n, $\overleftrightarrow{\gamma_i}$ and t_i. By the induction hypothesis, the multisets t_i satisfy $[P]^m \succ_\oplus t_i$, since they correspond to proper subproofs of Q. Because $\overleftarrow{\alpha} \succ \overleftrightarrow{\gamma_i}$ in the precedence for all i, we conclude that $\{\!\{(\overleftarrow{\alpha}, \varnothing)\}\!\} \succ_\oplus \{\!\{(\overleftrightarrow{\gamma_i}, t_i) \mid 1 \le i \le n\}\!\}$, which is equivalent to our claim, $[P]^m \succ_\oplus [Q]^m$.

2. We have
$$[P]^m = \{\!\{(\overleftarrow{\alpha}, \{\!\{(\overrightarrow{\gamma}, \varnothing)\}\!\}), (\overrightarrow{\gamma}, \{\!\{(\overleftarrow{\alpha}, \varnothing)\}\!\})\}\!\},$$
and for some $G \in (\overleftrightarrow{\Upsilon\gamma})^*$ and $A \in (\overleftrightarrow{\Upsilon\alpha})^*$,
$$[Q]^m = \{\!\{\ldots, (\overleftarrow{\alpha}, [G]^m), \ldots, (\overrightarrow{\gamma}, [A]^m), \ldots\}\!\}$$
with the $(\overleftarrow{\alpha}, [G]^m)$ or $(\overrightarrow{\gamma}, [A]^m)$ elements possibly missing. For all elements $(\overleftrightarrow{\eta}, u) \in [Q]^m$, $u = [R]^m$ for a proper subproof R of Q, and therefore $[P]^m \succ_\oplus u$ holds by the induction hypothesis. All omitted elements are of the shape $(\overleftrightarrow{\eta}, u)$ with $\alpha \succ \eta$ or $\gamma \succ \eta$, and compare less to one of $(\overleftarrow{\alpha}, \{\!\{\overrightarrow{\gamma}, \varnothing\}\!\})$ or $(\overrightarrow{\gamma}, \{\!\{\overleftarrow{\alpha}, \varnothing\}\!\})$ lexicographically. The remaining (up to two) elements are also dominated by elements of $[P]^m$: By the first part of the proof, $(\overleftarrow{\alpha}, [G]^m)$ is less than $(\overleftarrow{\alpha}, [\overrightarrow{\gamma}]^m)$ and $(\overrightarrow{\gamma}, [A]^m)$ is less than $(\overrightarrow{\gamma}, [\overleftarrow{\alpha}]^m)$. □

Theorem 9 ([8, Theorem 3])**.** *We are given a family of abstract rewrite systems $(\underset{\alpha}{\to})_{\alpha \in \mathcal{L}}$. Assume that all local peaks can be joined decreasingly, i.e., for all $\alpha, \gamma \in \mathcal{L}$,*

$$\underset{\alpha}{\leftarrow} \cdot \underset{\gamma}{\rightarrow} \subseteq \overset{*}{\underset{\Upsilon\alpha}{\longleftrightarrow}} \cdot \overset{=}{\underset{\gamma}{\rightarrow}} \cdot \overset{*}{\underset{\Upsilon\alpha,\gamma}{\longleftrightarrow}} \cdot \overset{=}{\underset{\alpha}{\leftarrow}} \cdot \overset{*}{\underset{\Upsilon\gamma}{\longleftrightarrow}}$$

Then $\underset{\mathcal{L}}{\to} = \bigcup_{\alpha \in \mathcal{L}} \underset{\alpha}{\to}$ is Church-Rosser.

Proof. We map each rewrite proof to the string obtained by considering just the directions and labels of the proof steps in the proof, mapping $s \underset{\alpha}{\leftarrow} t$ to $\overleftarrow{\alpha}$ and $s \underset{\alpha}{\rightarrow} t$ to $\overrightarrow{\alpha}$. If the rewrite proof has a local peak, then we can replace it by the corresponding joining sequence from a decreasing diagram. The strings P, corresponding to the local peak, and Q, for the joining sequence, satisfy $[P]^m \succ_\bullet [Q]^m$ by Lemma 8. By monotonicity (Lemma 7), this comparison extends to the whole proof string. Because $\succ_\bullet$ is well-founded, this process must terminate in some normal form. This normal form will be a valley proof that is equivalent to the original rewrite proof. □

4 Towards Church-Rosser Modulo

In this section we sketch two approaches to deal with confluence modulo by mapping proofs to proof strings. The first approach is to use the previously developed order directly. The second approach is to extend the proof strings by introducing symmetric proof steps, $\overline{\alpha}$, and incorporate them into the definitions of $\succ_\bullet$. Due to space constraints, we can only sketch it below. There are many notions of confluence modulo (see [7]). We use the following one.

Definition 10. Let $\rightarrow$ and $\vdash\!\dashv$ be abstract rewrite relations, where $\vdash\!\dashv$ is symmetric. We say that $\rightarrow$ is Church-Rosser modulo $\overset{*}{\vdash\!\dashv}$ if

$$(\leftrightarrow \cup \vdash\!\dashv)^* \subseteq \overset{*}{\rightarrow} \cdot \overset{*}{\vdash\!\dashv} \cdot \overset{*}{\leftarrow}.$$

In the proof transformation setting, this means that whenever we have a subproof $\leftarrow \cdot \rightarrow$, $\vdash\!\dashv \cdot \rightarrow$ or $\leftarrow \cdot \vdash\!\dashv$, we must be able to replace it by a different subproof.

First we sketch how one can use the order from Section 2 directly. Then all proof steps in $\vdash\!\dashv$ must be directed and labeled. In that case, in addition to removing local peaks (except those between $\vdash\!\dashv$ steps, i.e., from $\vdash\!\dashv \cdot \vdash\!\dashv$) one also has to eliminate subproofs of the shape $\underset{\alpha}{\rightarrow} \cdot \underset{\gamma}{\rightarrow}$ whenever $\underset{\alpha}{\rightarrow}$ is a $\vdash\!\dashv$ step and $\underset{\gamma}{\rightarrow}$ is a $\rightarrow$ step. The following lemma shows that any proof in $\overset{*}{\underset{\Upsilon\alpha}{\longleftrightarrow}} \cdot \underset{\gamma}{\overset{=}{\rightarrow}} \cdot \overset{*}{\underset{\Upsilon\alpha,\gamma}{\longleftarrow}}$ is a suitable replacement in this case.

Lemma 11. *If* $P = \overrightarrow{\alpha} \cdot \overrightarrow{\gamma}$ *and* $Q \in (\overleftrightarrow{\Upsilon\alpha})^* \cdot (\overrightarrow{\gamma})^= \cdot (\overleftarrow{\Upsilon\alpha,\gamma})^*$*, then* $P \succ_\bullet Q$.

Proof. Similar to Lemma 8. □

We have not yet investigated this approach in detail. In this note, Lemma 11 only serves as a point of reference to show that introducing undirected proof steps is useful.

So let us turn to the second approach. We extend the order $\succ_\bullet$ by introducing *undirected* proof steps: Let $\overline{\alpha}$ denote an undirected proof step that is symmetric: $(\overline{\alpha})^{-1} = \overline{\alpha}$. For $[\cdot]^m$, in addition to $[\cdot]^l$ and $[\cdot]^r$, we need an operation $[\cdot]^u$ that collects these undirected proof steps. So we define

- $[\epsilon]^l = \varnothing$, $[\overleftarrow{\alpha} \cdot P]^l = \{\!\{(\overleftarrow{\alpha}, [P]^m)\}\!\} \cup [P]^l$, $[\overrightarrow{\alpha} \cdot P]^l = [P]^l$, $[\overline{\alpha} \cdot P]^l = [P]^l$,
- $[\epsilon]^r = \varnothing$, $[P \cdot \overrightarrow{\alpha}]^r = \{\!\{(\overrightarrow{\alpha}, [P]^m)\}\!\} \cup [P]^r$, $[P \cdot \overleftarrow{\alpha}]^r = [P]^r$, $[P \cdot \overline{\alpha}]^r = [P]^r$,
- $\epsilon^u = \varnothing$, $[\overline{\alpha} \cdot P]^u = \{\!\{(\overline{\alpha}, \varnothing)\}\!\} \cup [P]^u$, $[\overleftarrow{\alpha} \cdot P]^u = [P]^u$, $[\overrightarrow{\alpha} \cdot P]^u = [P]^u$, and
- $[P]^m = [P]^l \cup [P]^r \cup [P]^u$.

Variables $\overleftrightarrow{\alpha}$ can now equal $\overline{\alpha}$. Correspondingly we define $\overleftrightarrow{S} = \{\overleftarrow{\alpha}, \overrightarrow{\alpha}, \overline{\alpha} \mid \alpha \in S\}$. Even with these changed notions (which result in extended definitions for $\succ_\oplus$ and $\succ_\bullet$), Theorem 7 and Lemmata 4, 8 and 11 remain valid. The following lemma shows how one can eliminate subproofs of the shape $\overline{\alpha} \cdot \overrightarrow{\gamma}$.

Lemma 12. *Let $P = \overline{\alpha} \cdot \overrightarrow{\gamma}$. The following statements are true.*

1. *If $Q \in (\overleftrightarrow{\Upsilon\alpha \cap \Upsilon\gamma})^* \cdot (\overrightarrow{\gamma})^{=} \cdot (\overleftrightarrow{\Upsilon\gamma})^* \cdot \overline{\alpha} \cdot (\overleftrightarrow{\Upsilon\gamma})^*$ then $P \succ_\bullet Q$.*
2. *If $Q \in (\overleftrightarrow{\Upsilon\alpha})^* \cdot (\overrightarrow{\gamma})^{=} \cdot (\overleftrightarrow{\Upsilon\alpha, \gamma})^*$ then $P \succ_\bullet Q$.*

Proof. Similar to Lemma 8. □

Lemma 12 adds some flexibility over Lemma 11 (where we use a directed α step instead of the undirected one), at the cost of reduced flexibility for eliminating peaks $\overleftarrow{\alpha} \cdot \overrightarrow{\gamma}$ (where again we use a directed α step, but this time pointing left, cf. Lemma 8).

Theorem 13. *Let $\mathcal{L}$ be a set of labels equipped with a well-founded order $\succ$. Furthermore, let $(\underset{\alpha}{\longrightarrow})_{\alpha\in\mathcal{L}}$ and $(\underset{\alpha}{\vdash\!\!\dashv})_{\alpha\in\mathcal{L}}$ be families of abstract rewrite relations, where each $\underset{\alpha}{\vdash\!\!\dashv}$ is symmetric. If*

$$\underset{\alpha}{\longleftarrow} \cdot \underset{\gamma}{\longrightarrow} \subseteq \overset{*}{\underset{\Upsilon\alpha}{\Longleftrightarrow}} \cdot \overset{=}{\underset{\gamma}{\longrightarrow}} \cdot \overset{*}{\underset{\Upsilon\alpha,\gamma}{\Longleftrightarrow}} \cdot \overset{=}{\underset{\alpha}{\longleftarrow}} \cdot \overset{*}{\underset{\Upsilon\gamma}{\Longleftrightarrow}}$$

and

$$\underset{\alpha}{\vdash\!\!\dashv} \cdot \underset{\gamma}{\longrightarrow} \subseteq \left(\overset{*}{\underset{\Upsilon\alpha\cap\Upsilon\gamma}{\Longleftrightarrow}} \cdot \overset{=}{\underset{\gamma}{\longrightarrow}} \cdot \overset{*}{\underset{\Upsilon\gamma}{\Longleftrightarrow}} \cdot \underset{\alpha}{\vdash\!\!\dashv} \cdot \overset{*}{\underset{\Upsilon\gamma}{\Longleftrightarrow}} \right) \cup \left(\overset{*}{\underset{\Upsilon\alpha}{\Longleftrightarrow}} \cdot \overset{=}{\underset{\gamma}{\longrightarrow}} \cdot \overset{*}{\underset{\Upsilon\alpha,\gamma}{\Longleftrightarrow}} \right),$$

for all $\alpha, \gamma \in \mathcal{L}$, where $\underset{\alpha}{\Leftrightarrow} = \underset{\alpha}{\longleftarrow} \cup \underset{\alpha}{\vdash\!\!\dashv} \cup \underset{\alpha}{\longrightarrow}$, then $\underset{\mathcal{L}}{\longrightarrow}$ is Church-Rosser modulo $\overset{*}{\underset{\mathcal{L}}{\vdash\!\!\dashv}}$.

Proof. The proof proceeds in the same way as that of Theorem 9: Whenever a given rewrite proof contains a peak of the shapes $\underset{\alpha}{\longleftarrow} \cdot \underset{\gamma}{\longrightarrow}$, $\underset{\alpha}{\vdash\!\!\dashv} \cdot \underset{\gamma}{\longrightarrow}$, or $\underset{\gamma}{\longleftarrow} \cdot \underset{\alpha}{\vdash\!\!\dashv}$, we can find a replacement proof by assumption. Considering the corresponding proof strings, the replacement is smaller than the peak with respect to $\succ_\bullet$. This extends to the whole strings by monotonicity. By well-foundedness of $\succ_\bullet$, this process will terminate. It is easy to see that the resulting normal forms are of the shape $\overset{*}{\underset{\mathcal{L}}{\longrightarrow}} \cdot \overset{*}{\underset{\mathcal{L}}{\vdash\!\!\dashv}} \cdot \overset{*}{\underset{\mathcal{L}}{\longleftarrow}}$, which establishes Church-Rosser modulo. □

Corollary 14 (Main Theorem of [7])**.** *Let $\mathcal{L}$ be a set of labels equipped with a well-founded order $\succ$. Furthermore, let $(\underset{\alpha}{\longrightarrow})_{\alpha\in\mathcal{L}}$ be a family of abstract rewrite relations and $\vdash\!\!\dashv$ be a symmetric relation. Then $\underset{\mathcal{L}}{\longrightarrow}$ is Church-Rosser modulo $\overset{*}{\vdash\!\!\dashv}$, if for all $\alpha, \gamma \in \mathcal{L}$*

$$\underset{\alpha}{\longleftarrow} \cdot \underset{\gamma}{\longrightarrow} \subseteq \overset{*}{\underset{\Upsilon\alpha}{\longrightarrow}} \cdot \overset{=}{\underset{\gamma}{\longrightarrow}} \cdot \overset{*}{\underset{\Upsilon\alpha,\gamma}{\longrightarrow}} \cdot \overset{*}{\vdash\!\!\dashv} \cdot \overset{*}{\underset{\Upsilon\alpha,\gamma}{\longleftarrow}} \cdot \overset{=}{\underset{\alpha}{\longleftarrow}} \cdot \overset{*}{\underset{\Upsilon\gamma}{\longleftarrow}}$$

and

$$\vdash\!\!\dashv \cdot \underset{\gamma}{\longrightarrow} \subseteq \overset{*}{\underset{\Upsilon\alpha}{\longrightarrow}} \cdot \overset{*}{\vdash\!\!\dashv} \cdot \overset{*}{\underset{\Upsilon\alpha}{\longleftarrow}} \cdot \overset{=}{\underset{\alpha}{\longleftarrow}}.$$

Proof. Apply Theorem 13 using $\mathcal{L}' = \mathcal{L} \cup \{\bot\}$ with $\alpha \succ \bot$ for all $\alpha \in \mathcal{L}$ as labels, and label all $\vdash\!\!\dashv$ steps by $\bot$. □

As another instance of Theorem 13 we can obtain a key lemma for abstract Church-Rosser modulo from [1]:

Corollary 15 ([1, Lemma 2.1])**.** *Let $(\underset{\alpha}{\longrightarrow})_{\alpha\in\mathcal{L}}$ and $(\underset{\alpha}{\vdash\!\!\dashv})_{\alpha\in\mathcal{L}}$ be families of abstract rewrite relations, where each $\underset{\alpha}{\vdash\!\!\dashv}$ is symmetric. Then $\underset{\mathcal{L}}{\longrightarrow}$ is Church-Rosser modulo $\overset{*}{\underset{\mathcal{L}}{\vdash\!\!\dashv}}$, if for all $\alpha, \gamma \in \mathcal{L}$,*

$$\underset{\alpha}{\longleftarrow} \cdot \underset{\gamma}{\longrightarrow} \subseteq \underset{\Upsilon\alpha,\gamma}{\Longleftrightarrow} \quad \text{and} \quad \underset{\alpha}{\vdash\!\!\dashv} \cdot \underset{\gamma}{\longrightarrow} \subseteq \underset{\Upsilon\alpha,\gamma}{\Longleftrightarrow}.$$

5 A Note on Witnesses for Non-Confluence

In this section we present an example of a *linear*, non-confluent TRS whose critical pairs are nevertheless *deeply joinable*. Two terms s, t are deeply joinable if any reducts $s \to^* s'$, $t \to^* t'$ are joinable. The example shows that when looking for witnesses for non-confluence, it does not suffice to look at reducts of critical pairs alone; some smarter technique is required in general.

Example 4. The TRS $\mathcal{R}$ consists of the rules

$$\begin{array}{llll} \mathsf{f}(\mathsf{u}(\mathsf{O}),\mathsf{u}(y)) \to \mathsf{A} & \mathsf{O} \to \mathsf{u}(\mathsf{O}) & \mathsf{u}(x) \to x & \mathsf{f}(x,y) \to \mathsf{f}(x,\mathsf{u}(y)) \\ \mathsf{f}(\mathsf{v}(x),\mathsf{v}(\mathsf{O})) \to \mathsf{B} & \mathsf{O} \to \mathsf{v}(\mathsf{O}) & \mathsf{v}(x) \to x & \mathsf{f}(x,y) \to \mathsf{f}(\mathsf{v}(x),y) \end{array}$$

This TRS is not confluent since $\mathsf{A} \mathrel{{}^*_{\mathcal{R}}\!\!\leftarrow} \mathsf{f}(\mathsf{O},\mathsf{O}) \to^*_{\mathcal{R}} \mathsf{B}$. There are 12 critical pairs, but they originate from only 4 different sources. We consider each possible source in turn.

1. $\mathsf{f}(\mathsf{u}(\mathsf{O}),\mathsf{u}(y))$ (5 critical pairs). By induction we can show that any term reachable from $\mathsf{f}(\mathsf{u}(\mathsf{O}),\mathsf{u}(y))$ is either equal to A or has shape $\mathsf{f}(\{\mathsf{u},\mathsf{v}\}^*(\mathsf{O}),\mathsf{u}^*(y)\})$, which in turn can be reduced to A. Therefore, all the corresponding critical pairs are deeply joinable.
2. $\mathsf{f}(\mathsf{v}(x),\mathsf{v}(\mathsf{O}))$ (5 critical pairs). This is analogous to the previous case, swapping the arguments of f and the roles of u and v.
3. $\mathsf{f}(x,y)$ (1 critical pair). From this source, we can reach only terms of shape $\mathsf{f}(\mathsf{v}^*(x),\mathsf{u}^*(y))$, which can all be rewritten to $\mathsf{f}(x,y)$.
4. O (1 critical pair). We can rewrite O to $\{\mathsf{u},\mathsf{v}\}^*(\mathsf{O})$, all of which reduce back to O.

Therefore, all critical pairs of $\mathcal{R}$ are deeply joinable as desired.

It has been pointed to the author that $\mathcal{R}$ is E-overlapping [4]. It is an interesting question whether this can be avoided. Note, however, that existence of E-overlaps is undecidable.

Acknowledgments. The author is grateful to the anonymous reviewers for constructive feedback on this paper, to Vincent van Oostrom for sharing and discussing related work on involutive monoids, and to Aart Middeldorp and Harald Zankl for fruitful discussions.

References

[1] T. Aoto and Y. Toyama. A reduction-preserving completion for proving confluence of non-terminating term rewriting systems. *LMCS*, 8(1:31):1–29, 2012.

[2] L. Bachmair and N. Dershowitz. Equational inference, cannonical proofs, and proof orderings. *JACM*, 41(2):236–276, 1994.

[3] M.C.F. Ferreira. *Termination of Term Rewriting: Well-Foundedness, Totality and Transformations.* PhD thesis, Utrecht University, 1995.

[4] H. Gomi, M. Oyamaguchi, and Y. Ohta. On the Church-Rosser property of root-E-overlapping and strongly depth-preserving term rewriting systems. *Trans. IPSJ*, 39(4):992–1005, 1998.

[5] G. Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *JACM*, 27(4):797–821, 1980.

[6] J.-P. Jouannaud and V. van Oostrom. Diagrammatic confluence and completion. In *Proc. 36th ICALP*, volume 5556 of *LNCS*, pages 212–222, 2009.

[7] E. Ohlebusch. Church-Rosser theorems for abstract reduction modulo an equivalence relation. In *Proc. 9th RTA*, volume 1379 of *LNCS*, pages 17–31, 1998.

[8] V. van Oostrom. Confluence by decreasing diagrams – converted. In *Proc. 19th RTA*, volume 5117 of *LNCS*, pages 306–320, 2008.