Confluence by Decreasing Diagrams – Formalized

Harald Zankl

Institute of Computer Science, University of Innsbruck, 6020 Innsbruck, Austria

— **Abstract** —————————————————————————————

This paper presents a formalization of decreasing diagrams in the theorem prover Isabelle. It discusses mechanical proofs showing that any locally decreasing abstract rewrite system is confluent. The valley and the conversion version of decreasing diagrams are considered.

1 Introduction

Formalizing confluence criteria has a long history in λ-calculus. Huet [8] proved a stronger variant of the parallel moves lemma in Coq. Isabelle/HOL was used in [11] to prove the Church-Rosser property of β, η, and $\beta\eta$. For β-reduction the standard Tait/Martin-Löf proof as well as Takahashi's proof [23] were formalized. The first mechanically verified proof of the Church-Rosser property of β-reduction was done using the Boyer-Moore theorem prover [20]. The formalization in Twelf [18] was used to formalize the confluence proof of a specific higher-order rewrite system in [22].

Newman's lemma (for abstract rewrite systems) and Knuth and Bendix' critical pair theorem (for first-order rewrite systems) have been proved in [19] using ACL. An alternative proof of the latter in PVS, following the higher-order structure of Huet's proof, is presented in [7]. PVS is also used in the formalization of the lemmas of Newman and Yokouchi in [6]. Knuth and Bendix' criterion has also been formalized in Coq [3] and Isabelle/HOL [25].

Decreasing diagrams [13] are a complete characterization of confluence for abstract rewrite systems whose convertibility classes are countable. As a criterion for abstract rewrite systems, they can easily be applied for first- and higher-order rewriting, including term rewriting and the λ-calculus. Furthermore, decreasing diagrams yield constructive proofs of confluence [16] (in the sense that the joining sequences can be computed based on the divergence). We are not aware of a (complete) formalization of decreasing diagrams in any theorem prover (see remarks in Section 6).

In this paper we discuss a formalization of decreasing diagrams in the theorem prover Isabelle/HOL. (In the sequel we just call it Isabelle.) We closely follow the proofs in [13,15]. For alternative proofs see [1, 10] or [5, 9, 17] where proof orders play an essential role. The main contributions of this paper are (two) mechanical proofs of Theorem 1 in Isabelle.

▶ **Theorem 1** ([13, 15]). *A locally decreasing abstract rewrite system is confluent.* ◀

As a consequence all definitions (lemmata) in this paper have been formalized (proved) in Isabelle. The definitions from the paper are (modulo notation) identical to the ones used in Isabelle. Our formalization (Decreasing_Diagrams.thy, available from [27]) consists of approximately 1600 lines of Isabelle code in the Isar style and contains 31 definitions and 122 lemmata. The valley version [13] amounts to ca. 1000 lines, 22 definitions, and 97 lemmata while the conversion version [15] has additional 600 lines of Isabelle comprising

meaning	set	multiset	sequence/list	[13]
empty	$\{\}$	$\{\#\}$	$[]$	$\emptyset/\epsilon$
singleton	$\{\alpha\}$	$\{\#\alpha\#\}$	$[\alpha]$	$\{\alpha\}/[\alpha]/\alpha$
membership	$\alpha \in S$	$\alpha \in\# M$	$-$	$\in$
union/concatenation	$S \cup T$	$M + N$	$\sigma@\tau$	$\uplus/\sigma\tau$
intersection	$S \cap T$	$M \,\#\cap\, N$	$-$	$\cap$
difference	$S - T$	$M - N$	$-$	$-$
sub(multi)set	$S \subseteq T$	$M \leq N$	$-$	$\subseteq$

Table 1 Predefined Isabelle operators.

9 definitions and 25 lemmata. Our formalization imports the theory Multiset.thy from the Isabelle library and Abstract_Rewriting.thy [21] from the Archive of Formal Proofs. We used Isabelle 2012 and the Archive of Formal Proofs from July 30, 2012.

The remainder of this paper is organized as follows. In the next section we recall helpful preliminaries for our formalization of [13], which is described in Section 3. The conversion version of decreasing diagrams [15] is the topic of Section 4. In Section 5 we highlight changes to (and omissions in) the proofs from [13, 15] before we conclude in Section 6.

2   Preliminaries

We assume familiarity with rewriting [24] and decreasing diagrams [13]. Basic knowledge of Isabelle [12] is not essential but may be helpful.

Given a relation $\to$ we write $\leftarrow$ for its inverse, $\twoheadrightarrow$ for its transitive closure, and $\to^=$ (in pictures also $\overset{=}{\to}$) for its reflexive closure. We write $\leftrightarrow$ for $\to$ or $\leftarrow$ and denote sets by S, T, U, multisets by M, N, I, J, K, Q, single labels by α, β, and γ, and lists of labels by σ, τ, υ, κ, μ, and ρ (possibly primed or indexed).

Table 1 gives an overview of several predefined operators in Isabelle for sets, multisets, and lists (sequences) where we also incorporated the notation from [13] in the rightmost column. In the paper we will use the Isabelle notation, but drop the @ for concatenating sequences and write α instead of $[\alpha]$. In addition to the operators provided by Isabelle, we need the difference (intersection) of a multiset with a set. Here $M -s\ S$ $(M \cap s\ S)$ removes (keeps) all occurrences of elements in M that are in S. Sometimes it will be necessary to convert e.g. a multiset to a set (or a list). In the paper we leave these conversions implicit, since no confusion can arise. We establish the following useful equivalences:

▶ **Lemma 2** (parts of [13, Lemma A.3]).
1. $(M + N) -s\ S = (M -s\ S) + (N -s\ S)$
2. $(M -s\ S) -s\ T = M -s\ (S \cup T)$
3. $M = (M \cap s\ S) + (M -s\ S)$
4. $(M -s\ T) \cap s\ S = (M \cap s\ S) -s\ T$

Proof. By unfolding the definitions of multiset and the operators.   ◀

3   Formalization of Decreasing Diagrams

We assume familiarity with the original proof of decreasing diagrams in [13], upon which our formalization in this section is based. Nevertheless we will recall the important definitions and lemmata. However, we only give proofs if our proof deviates from the original argument.

In addition we state (sometimes small) key results, since an effective collection of lemmata is crucial for completely formal proofs.

The remainder of this section is organized as follows: Section 3.1 describes our results on multisets. Section 3.2 is dedicated to decreasingness (of sequences of labels) and Section 3.3 is concerned with an alternative formulation of local decreasingness. Afterwards, Section 3.4 lifts decreasingness (from labels) to diagrams. Well-foundedness of the measure (on peaks) is proved in Section 3.5, where we also establish the main result.

3.1 Multisets

In the sequel we assume $\prec$ to be a transitive and irreflexive binary relation.

▶ **Definition 3** ([13, Definition 2.5]).
1. The set $\Upsilon\alpha$ is the strict order ideal generated by (or *down-set* of) α, defined by $\Upsilon\alpha = \{\beta \mid \beta \prec \alpha\}$. This is extended to sets $\Upsilon S = \bigcup_{\alpha \in S} \Upsilon\alpha$. We define ΥM and $\Upsilon\sigma$ to be the down-set generated by the set of elements in M and σ, respectively.
2. The *(standard) multiset extension* (denoted by $\prec_{\mathsf{mul}}$) of $\prec$ is defined by

$$M \prec_{\mathsf{mul}} N \text{ if } \exists\ I\ J\ K.\ M = I + K,\ N = I + J,\ K \subseteq \Upsilon J,\ \text{and } J \neq \{\#\}$$

The relation $\preccurlyeq_{\mathsf{mul}}$ is obtained by removing the last condition ($J \neq \{\#\}$). Note that $\preccurlyeq_{\mathsf{mul}}$ is the reflexive closure of $\prec_{\mathsf{mul}}$ (cf. Lemma 39 in Section 5).

The following result is not mentioned in [13]—while [14, Proposition 1.4.8(3)] shows a more general result—but turned out handy for our formalization.

▶ **Lemma 4.** $\Upsilon(\Upsilon S) \subseteq \Upsilon S$

Proof. Assume $x \in \Upsilon(\Upsilon S)$. By Definition 3 there must be a $y \in \Upsilon S$ with $x \prec y$. From $y \in \Upsilon S$ we obtain a $z \in S$ with $y \prec z$. Then $x \prec z$ by transitivity of $\prec$ and hence $x \in \Upsilon S$. ◀

The multiset extension inherits some properties of the base relation, which we will implicitly use in the sequel.

▶ **Lemma 5.** *Let $\prec$ be a transitive and well-founded relation. Then $\prec_{mul}$ is transitive and well-founded, and $\preccurlyeq_{mul}$ is reflexive and transitive.*

Proof. By Lemmata 38 and 39 in combination with existing results in Multiset.thy. ◀

We can now establish the following properties.

▶ **Lemma 6** ([13, Lemma 2.6]).
1. $\Upsilon(S \cup T) = \Upsilon S \cup \Upsilon T$ *and* $\Upsilon(\sigma\tau) = \Upsilon\sigma \cup \Upsilon\tau$ *and* $\Upsilon(M -s\ S) \supseteq \Upsilon M -s\ \Upsilon S$
2. $M \leq N \Rightarrow M \preccurlyeq_{mul} N \Rightarrow \Upsilon M \subseteq \Upsilon N$
3. $M \preccurlyeq_{mul} N \Rightarrow \exists\ I\ J\ K.\ M = I + K \wedge N = I + J \wedge K \subseteq \Upsilon J \wedge J \#\cap K = \{\#\}$
4. $N \neq \{\#\} \wedge M \subseteq \Upsilon N \Rightarrow M \prec_{mul} N$
5. $M \preccurlyeq_{mul} N \Rightarrow M -s\ \Upsilon S \preccurlyeq_{mul} N -s\ \Upsilon S$
6. $M \preccurlyeq_{mul} N \Leftrightarrow Q + M \preccurlyeq_{mul} Q + N$
7. $Q \subseteq \Upsilon N - \Upsilon M \wedge M \preccurlyeq_{mul} N \Rightarrow Q + M \preccurlyeq_{mul} N$
8. $S \subseteq T \Rightarrow M -s\ T \preccurlyeq_{mul} M -s\ S$
9. $M \prec_{mul} N \Rightarrow Q + M \prec_{mul} Q + N$

Note that statements (5) and (6) slightly differ from [13, Lemma 2.6](5,6), but are easier to apply. The (easy) the statements of (8) and (9) are not mentioned in [13], which we required for [13, Lemmata 3.5 and 3.6].

(a) Decreasing diagram.   **(b)** Locally decreasing diagram.
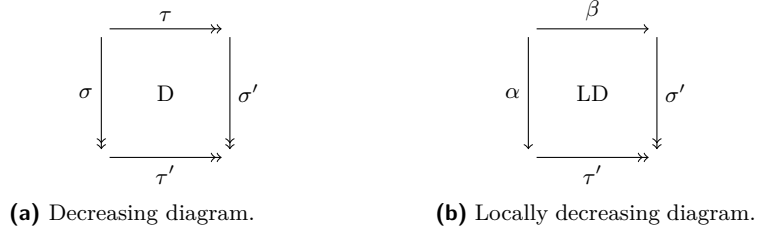
🟨 **Figure 1** Diagrams.

3.2 Decreasingness

We define the *lexicographic maximum* measure, which maps lists to multisets, inductively.

▶ **Definition 7** ([13, Definition 3.2]).

▬ $|[\,]| = \{\#\}$

▬ $|\alpha\sigma| = \{\#\alpha\#\} + (|\sigma| -s \Upsilon\alpha)$

The next lemma establishes properties of the lexicographic maximum measure.

▶ **Lemma 8** ([13, Lemma 3.2]).

1. $\Upsilon|\sigma| = \Upsilon\sigma$

2. $\Upsilon|\sigma\tau| = |\sigma| + (|\tau| -s \Upsilon\sigma)$

Proof.

1. By induction on σ. The base case is trivial. Using Lemma 6(1) the inductive step amounts to $\Upsilon\alpha\cup\Upsilon(|\sigma| -s \Upsilon\alpha) = \Upsilon\alpha\cup\Upsilon\sigma$. The inclusion from left to right follows from the induction hypothesis. For the inclusion from right to left we proceed by case analysis. If $x \in \Upsilon\alpha$ then the result immediately follows. If $x \notin \Upsilon\alpha$ then $x \in \Upsilon\sigma$ and from the induction hypothesis $x \in \Upsilon|\sigma|$. Furthermore $x \notin \Upsilon\alpha$ using Lemma 4 also yields $x \notin \Upsilon(\Upsilon\alpha)$. Hence $x \in \Upsilon|\sigma| -s \Upsilon(\Upsilon\alpha)$ and from Lemma 6(1) we obtain $x \in \Upsilon(|\sigma| -s \Upsilon\alpha)$, from which the result follows.

2. By induction on σ, see [13].   ◀

Decreasingness is defined on quadruples (of sequences of labels).

▶ **Definition 9** ([13, Definition 3.3] for labels). The quadruple of labels $(\tau, \sigma, \sigma', \tau')$ is *decreasing* (D) if $|\sigma\tau'| \preccurlyeq_{\mathsf{mul}} |\tau|+|\sigma|$ and $|\tau\sigma'| \preccurlyeq_{\mathsf{mul}} |\tau|+|\sigma|$. For a visualization see Figure 1a.[1]

We write D into a diagram to indicate that its labels are decreasing.
Decreasingness can also be stated differently.

▶ **Lemma 10** ([13, Definition 3.3]). *The following two statements are equivalent:*

1. $|\sigma\tau'| \preccurlyeq_{mul} |\tau| + |\sigma|$ *and* $|\tau\sigma'| \preccurlyeq_{mul} |\tau| + |\sigma|$

2. $|\tau'| -s \Upsilon\sigma \preccurlyeq_{mul} |\tau|$ *and* $|\sigma'| -s \Upsilon\tau \preccurlyeq_{mul} |\sigma|$

**Proof.** By Lemma 8(2) and Lemma 6(6).   ◀

We have followed the (involved) proofs in [13] that pasting preserves decreasingness (Lemma 11) and that pasting is hypothesis decreasing (Lemma 12) without big changes.

---

[1] Although the results in Sections 3.2 and 3.3 are on labels only for visualization we already use diagrams.

(a) Lemma 11.   **(b)** Lemma 12.
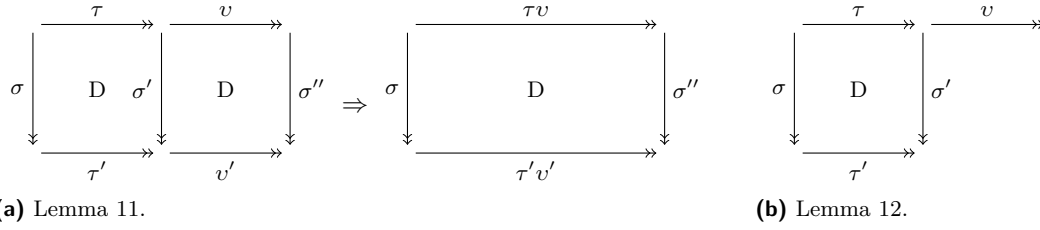
■ **Figure 2** Pasting preserves decreasingness and is hypothesis decreasing.
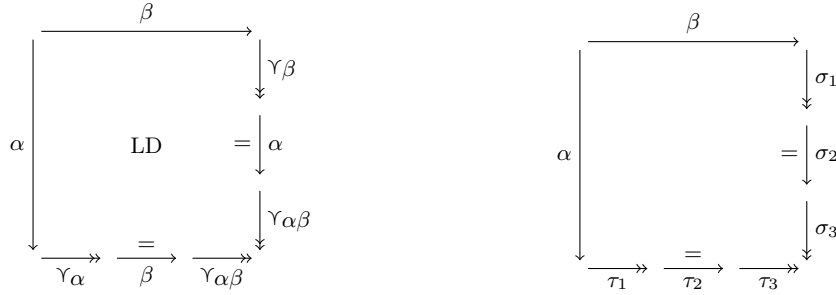
(a) Alternative formulation of local decreasingness.   **(b)** Giving names to the joining sequences.

■ **Figure 3** Local diagrams.

▶ **Lemma 11** ([13, Lemma 3.5] for labels)**.** *If $(\tau, \sigma, \sigma', \tau')$ and $(\upsilon, \sigma', \sigma'', \upsilon')$ are decreasing, then $(\tau\upsilon, \sigma, \sigma'', \tau'\upsilon')$ is decreasing (see Figure 2a).*

Proof. As in [13] but we show $(|\upsilon'| -s \curlyvee\sigma\tau') -s \curlyvee\tau \preccurlyeq_{\mathsf{mul}} (|\upsilon'| -s \curlyvee\sigma') -s \curlyvee\tau$ (instead of $\subseteq$) where we needed Lemma 6(8) (in the last sequence in [13, Proof of Lemma 3.5]).   ◀

▶ **Lemma 12** ([13, Lemma 3.6] for labels)**.** *If τ is non-empty and we have that $(\tau, \sigma, \sigma', \tau')$ is decreasing (see Figure 2b) then $|\sigma'| + |\upsilon| \prec_{\mathsf{mul}} |\sigma| + |\tau\upsilon|$.*

Proof. As in [13] using Lemma 6(9) in the second step.   ◀

3.3   Local Decreasingness

Labels $(\beta, \alpha, \sigma', \tau')$ are *locally decreasing* (LD) if they are decreasing and both α and β consist of exactly one label (see Figure 1b). Now, LD can also be formulated differently:

▶ **Lemma 13** ([13, Prop. 3.4])**.** *The form of locally decreasing labels is specified in Figure 3a.*

To show Lemma 13 we give names to the joining sequences as in Figure 3b. Then the condition of Figure 3a can be expressed as:[2]

$$\mathsf{LD}' := \sigma_1 \subseteq \curlyvee\beta \wedge \mathsf{length}\ \sigma_2 \le 1 \wedge \sigma_2 \subseteq \{\alpha\} \wedge \sigma_3 \subseteq \curlyvee\alpha\beta \wedge$$
$$\tau_1 \subseteq \curlyvee\alpha \wedge \mathsf{length}\ \tau_2 \le 1 \wedge \tau_2 \subseteq \{\beta\} \wedge \tau_3 \subseteq \curlyvee\alpha\beta$$

---

[2] Here length computes the length of a list.

Local decreasingness of the labels in the diagram of Figure 3a (using Lemma 10) yields

$$\text{LD} := |\sigma'| - s\, \Upsilon\beta \preccurlyeq_{\mathsf{mul}} |\alpha| \wedge |\tau'| - s\, \Upsilon\alpha \preccurlyeq_{\mathsf{mul}} |\beta|$$

Hence Lemma 13 states that LD' if and only if LD. This means that

(i) if a local diagram satisfies the conditions in Figure 3a, i.e. LD', then it is decreasing and

(ii) local decreasingness implies that the joining sequences τ' and σ' in Figure 1b can be decomposed into $\tau_1\tau_2\tau_3$ and $\sigma_1\sigma_2\sigma_3$ such that the properties of the local diagram in Figure 3a, i.e. LD', are satisfied.

Lemma 15 will be the key result for (i), but first we establish a useful lemma.

▶ **Lemma 14.** $|\sigma| \le \sigma$

Proof. By induction on σ. The base case is trivial. The step case amounts to

$$|\alpha\sigma| \;=\; \{\#\alpha\#\} + (|\sigma| - s\, \Upsilon\alpha) \;\le\; \{\#\alpha\#\} + (\sigma - s\, \Upsilon\alpha) \;\le\; \alpha\sigma$$

using Definition 7 in the first step and the induction hypothesis in the second step. ◀

In the sequel we will view $|\sigma|$ and σ as sets and use $|\sigma| \subseteq \sigma$. Now we can prove the following key result to establish (i).

▶ **Lemma 15.** $\sigma_1 \subseteq \Upsilon\beta \wedge \mathit{length}\ \sigma_2 \le 1 \wedge \sigma_2 \subseteq \{\alpha\} \wedge \sigma_3 \subseteq \Upsilon\alpha\beta \Rightarrow |\sigma_1\sigma_2\sigma_3| - s\, \Upsilon\beta \preccurlyeq_{\mathit{mul}} |\alpha|$

Proof. We show

$$(|\sigma_1| - s\, \Upsilon\beta) + ((|\sigma_2| - s\, \Upsilon\sigma_1) - s\, \Upsilon\beta) + (((|\sigma_3| - s\, \Upsilon\sigma_2) - s\, \Upsilon\sigma_1) - s\, \Upsilon\beta) \preccurlyeq_{\mathsf{mul}} \{\#\alpha\#\} \ \ (\star)$$

which is equivalent to the conclusion by Lemmata 8(2), 2(1) and Definition 7. The hypothesis contains $\sigma_1 \subseteq \Upsilon\beta$, which together with Lemma 14 yields $|\sigma_1| \subseteq \Upsilon\beta$ and hence

$$|\sigma_1| - s\, \Upsilon\beta = \{\#\} \tag{1}$$

Similarly from $\sigma_3 \subseteq \Upsilon\alpha\beta$ we get $|\sigma_3| - s\, (\Upsilon\alpha \cup \Upsilon\beta) = \{\#\}$ and hence

$$|\sigma_3| - s\, (\Upsilon\sigma_2 \cup \Upsilon\sigma_1 \cup \Upsilon\alpha \cup \Upsilon\beta) = \{\#\} \tag{3}$$

Using $\mathsf{length}\ \sigma_2 \le 1 \wedge \sigma_2 \subseteq \{\alpha\}$ from the hypothesis we have two cases to consider for σ_2.

▬ If $\sigma_2 = [\,]$ then

$$(|\sigma_2| - s\, \Upsilon\sigma_1) - s\, \Upsilon\beta = \{\#\} \tag{2}$$

and from (3) we have

$$((|\sigma_3| - s\, \Upsilon\sigma_2) - s\, \Upsilon\sigma_1) - s\, \Upsilon\beta \preccurlyeq_{\mathsf{mul}} \{\#\alpha\#\} \tag{3'}$$

using Lemma 2(2). Then $(\star)$ follows immediately from (1), (2), and (3').

▬ If $\sigma_2 = [\alpha]$ then we get (2')

$$\begin{aligned}
(|\sigma_2| - s\, \Upsilon\sigma_1) - s\, \Upsilon\beta &= |\sigma_2| - s\, (\Upsilon\sigma_1 \cup \Upsilon\beta) && \text{Lemma 2(2)} \\
&= \{\#\alpha\#\} - s\, (\Upsilon\sigma_1 \cup \Upsilon\beta) && \sigma_2 = [\alpha]\ \text{with Definition 7} \\
&\preccurlyeq_{\mathsf{mul}} \{\#\alpha\#\} && \text{Lemma 6(8)}
\end{aligned}$$

and (because $\Upsilon\sigma_2 = \Upsilon\alpha$), similar as in the other case from (3) we get

$$((|\sigma_3| - s\, \Upsilon\sigma_2) - s\, \Upsilon\sigma_1) - s\, \Upsilon\beta = \{\#\} \tag{3''}$$

From (1), (2'), and (3'') we conclude $(\star)$. ◀

Next we prepare for the key lemma to establish (ii), i.e., Lemma 17, after establishing useful intermediate results. Note that Lemma 16(2) can be seen as an inverse of Lemma 14.

▶ **Lemma 16.**
1. $\alpha \in\# |\sigma| \Rightarrow \exists \sigma_1 \sigma_3.\ \sigma = \sigma_1 \alpha \sigma_3 \wedge \alpha \notin \Upsilon \sigma_1$
2. $|\sigma| \subseteq \Upsilon S \Rightarrow \sigma \subseteq \Upsilon S$
3. $S \subseteq \Upsilon T \Rightarrow \Upsilon S \subseteq \Upsilon T$

Proof.
1. By induction on σ. The base case is trivial. In the step case we can assume that $\alpha \in\# |\beta\sigma|$. We proceed by case analysis.
   - If $\alpha = \beta$ then we are done with $\sigma_1 = [\,]$ and $\sigma_3 = \sigma$.
   - In the other case we have $\alpha \in\# |\sigma|$ and $\alpha \notin \Upsilon\beta$ from Definition 7. The induction hypothesis yields σ_1' and σ_3' with $\sigma = \sigma_1'\alpha\sigma_3'$ such that $\alpha \notin \Upsilon\sigma_1'$. Because $\alpha \notin \Upsilon\beta$ we can conclude with $\sigma_1 = \beta\sigma_1'$ and $\sigma_3 = \sigma_3'$ using Lemma 6(1).
2. Assume $\alpha \in \sigma$. If $\alpha \in\# |\sigma|$ then we are done by the hypothesis. In the other case there must be a $\beta \in |\sigma|$ (easy induction on σ) with $\alpha \prec \beta$. From the hypothesis we get that $\beta \in \Upsilon S$ and by transitivity also $\alpha \in \Upsilon S$, which finishes the proof.
3. By monotonicity of Υ ([14, Proposition 1.4.8(2)]) the assumption yields $\Upsilon S \subseteq \Upsilon(\Upsilon T)$. Lemma 4 finishes the proof. ◀

With Lemma 16 we can now prove the following key result to establish (ii):

▶ **Lemma 17.** $|\sigma'| -s \Upsilon\beta \preccurlyeq_{mul} \{\#\alpha\#\} \Rightarrow \exists \sigma_1 \sigma_2 \sigma_3.\ \sigma' = \sigma_1 \sigma_2 \sigma_3 \wedge \sigma_1 \subseteq \Upsilon\beta \wedge \textit{length } \sigma_2 \leq 1 \wedge \sigma_2 \subseteq \{\alpha\} \wedge \sigma_3 \subseteq \Upsilon\alpha\beta$

Proof. To show the result we perform a case analysis.
- If $\alpha \in\# |\sigma'| -s \Upsilon\beta$ then Lemma 16(1) yields σ_1 and σ_3 with $\sigma' = \sigma_1 \alpha \sigma_3$ and $\alpha \notin \Upsilon\sigma_1$. Hence from the hypothesis and Lemma 8(2) we get

$$(|\sigma_1| -s \Upsilon\beta) + \{\#\alpha\#\} + (((|\sigma_3| -s \Upsilon\alpha) -s \Upsilon\sigma_1) -s \Upsilon\beta) \preccurlyeq_{mul} \{\#\alpha\#\}$$

and since $\alpha \notin \Upsilon\sigma_1$ and $\alpha \notin \Upsilon\beta$ it follows that

$$|\sigma_1| -s \Upsilon\beta = \{\#\} \text{ and } ((|\sigma_3| -s \Upsilon\alpha) -s \Upsilon\sigma_1) -s \Upsilon\beta = \{\#\}$$

Now, Lemma 2(2) yields

$$|\sigma_1| \subseteq \Upsilon\beta \text{ and } |\sigma_3| \subseteq \Upsilon\alpha \cup \Upsilon\sigma_1 \cup \Upsilon\beta$$

and from Lemma 16(2) we get

$$\sigma_1 \subseteq \Upsilon\beta \text{ and } \sigma_3 \subseteq \Upsilon\alpha \cup \Upsilon\sigma_1 \cup \Upsilon\beta$$

The latter simplifies to $\sigma_3 \subseteq \Upsilon\alpha\beta$ using $\Upsilon\sigma_1 \subseteq \Upsilon\beta$ (from Lemma 16(3)) and Lemma 6(1). Hence in this case the result follows with $\sigma_2 = [\alpha]$.
- If $\alpha \notin\# |\sigma'| -s \Upsilon\beta$

$$\begin{aligned}
&\Rightarrow |\sigma'| -s \Upsilon\beta \subseteq \Upsilon\alpha && \text{hypothesis} \\
&\Rightarrow |\sigma'| \subseteq \Upsilon\alpha\beta && \text{Lemma 6(1)} \\
&\Rightarrow \sigma' \subseteq \Upsilon\alpha\beta && \text{Lemma 16(2)}
\end{aligned}$$

In this case the result follows with empty σ_1, empty σ_2, and $\sigma' = \sigma_3$. ◀

Now Lemma 13 follows from Lemma 15 ($\text{LD}' \Rightarrow \text{LD}$) and Lemma 17 ($\text{LD} \Rightarrow \text{LD}'$).

3.4 Labeled Rewriting

So far we have only considered sequences of labels. However, for the main result (Section 3.5) we need labeled rewriting. Hence this section sketches how we formalized *labeled* (abstract) rewriting before lifting the results from Section 3.2 from labels to labeled rewriting (a step which is left implicit in [13]). In the theory Abstract_Rewriting.thy an *abstract rewrite system* (ARS) is a set of pairs of objects of the same type, i.e., a binary relation. Confluence is also defined in Abstract_Rewriting.thy, but the theory does not provide support for *labeled* abstract rewrite systems. In the sequel we write $\mathcal{A}$ ($\mathcal{B}$) for (labeled) ARSs. A *labeled ARS $\mathcal{B}$* is a ternary relation. We call $(a, \alpha, b) \in \mathcal{B}$ a *(labeled rewrite) step* and write $a \xrightarrow{\alpha} b$. Next we define *(labeled rewrite) sequences* inductively, i.e., for each object a there is the empty sequence $a \xrightarrow{[]} a$ and if $a \xrightarrow{\alpha} b$ is a step and $b \xrightarrow{\sigma} c$ is a sequence then $a \xrightarrow{\alpha\sigma} c$ is a sequence.

▶ **Example 18.** Let $\mathcal{B}$ be the labeled ARS $\{(a, \alpha, b), (b, \beta, c)\}$. Then $a \xrightarrow{\alpha} b \xrightarrow{\beta} c$ (or $a \xrightarrow{\alpha\beta} c$) is a sequence in $\mathcal{B}$. The empty sequence $a \xrightarrow{[]} a$ we also write as a.

We prove useful properties for sequences, i.e., that chopping off a segment of a sequence again yields a sequence and that two sequences can be concatenated (provided the last element of the first sequence coincides with the first element of the second sequence).

▶ **Lemma 19.** *Let $a_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{n-1}} a_n$ and $b_1 \xrightarrow{\beta_1} \cdots \xrightarrow{\beta_{m-1}} b_m$ be sequences.*
1. *Then $a_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{i-1}} a_i$ and $a_i \xrightarrow{\alpha_i} \cdots \xrightarrow{\alpha_{n-1}} a_n$ are sequences for any $1 \leqslant i \leqslant n$.*
2. *If $a_n = b_1$ then $a_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{n-1}} a_n = b_1 \xrightarrow{\beta_1} \cdots \xrightarrow{\beta_{m-1}} b_m$ is a sequence.*

Proof. By induction on $a_1 \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_{n-1}} a_n$.   ◀

As a next step we introduce diagrams.

▶ **Definition 20.** A *diagram* is a quadruple of sequences $(\xrightarrow{\tau}, \xrightarrow{\sigma}, \xrightarrow{\sigma'}, \xrightarrow{\tau'})$ such that the start and endpoints of the sequences satisfy the picture in Figure 1a. A diagram is called *decreasing* if its labels are.

We lift Lemma 11 from labels to diagrams.

▶ **Lemma 21** ([13, Lemma 3.5] for decreasing diagrams)**.** *Pasting two decreasing diagrams yields a decreasing diagram. For a picture see Figure 2a.*

Proof. With the help of Lemma 19(2) we show that pasting two diagrams again yields a diagram. That pasting preserves decreasingness follows from Lemma 11.   ◀

3.5 Main Result

We establish that if all local peaks of a labeled ARS $\mathcal{B}$ are decreasing then all peaks of $\mathcal{B}$ are decreasing, following the structure of the proof of [13, Theorem 3.7]. (Changes are discussed in Section 5). Note that only here we need that $\prec$ is well-founded, from which irreflexivity immediately follows (to satisfy our global assumption from Section 2). First we introduce (local) peaks.

▶ **Definition 22.** A *peak* $(\xrightarrow{\tau}, \xrightarrow{\sigma})$ is a pair of labeled rewrite sequences which originate from the same object. A *local peak* is a peak where the sequences consist of a single step.

To prove the main result we introduce a measure on *peaks* (actually on pairs of sequences).
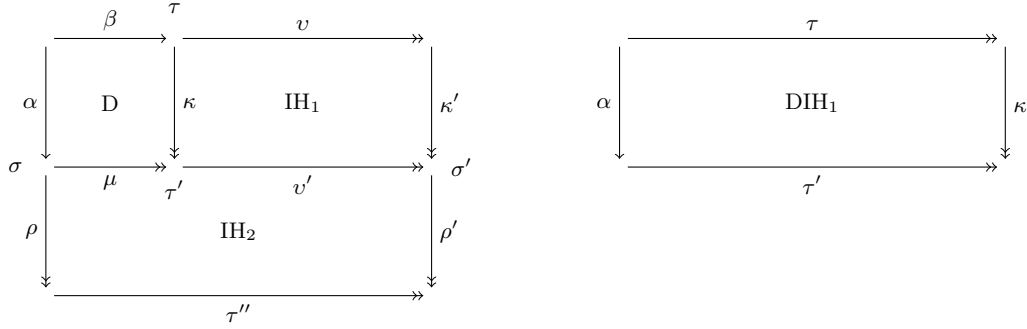
(a) Local decreasingness implies decreasingness.   **(b)** Pasting D and IH_1 into DIH_1.

■ **Figure 4** Lemma 26

▶ **Definition 23.** Let $|(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow})| := |\tau| + |\sigma|$. Then we can lift $\prec$ as a relation on labels to a relation on pairs of sequences $\prec_{\mathsf{peak}}$, i.e., $(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow}) \prec_{\mathsf{peak}} (\overset{\tau'}{\twoheadrightarrow}, \overset{\sigma'}{\twoheadrightarrow})$ if $|(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow})| \prec_{\mathsf{mul}} |(\overset{\tau'}{\twoheadrightarrow}, \overset{\sigma'}{\twoheadrightarrow})|$.

For proofs of induction we establish that $\prec_{\mathsf{peak}}$ is well-founded.

▶ **Lemma 24.** *Let $\prec$ be well-founded. Then $\prec_{peak}$ is well-founded.*

Proof. From [4] we get that $\prec_{\mathsf{mul}}$ is well-founded (this proof is contained in Multiset.thy). We proceed by contraposition. Assume the measure on peaks is not well-founded. Then we obtain an infinite sequence $\cdots \prec_{\mathsf{peak}} (\tau_2, \sigma_2) \prec_{\mathsf{peak}} (\tau_1, \sigma_1)$ which entails an infinite sequence on multisets $\cdots \prec_{\mathsf{mul}} |\tau_2| + |\sigma_2| \prec_{\mathsf{mul}} |\tau_1| + |\sigma_1|$ showing the result. ◀

▶ **Definition 25.** A peak $(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow})$ in a labeled ARS is *decreasing* if it can be completed into a decreasing diagram, i.e., there are $\overset{\sigma'}{\twoheadrightarrow}$ and $\overset{\tau'}{\twoheadrightarrow}$ such that the conditions of Figure 1a are satisfied. A peak is *locally decreasing*, if it is decreasing and a local peak.

▶ **Lemma 26** (similar to [13, Theorem 3.7])**.** *Let $\mathcal{B}$ be a labeled ARS and $\prec$ be a transitive and well-founded relation on the labels. If all local peaks of $\mathcal{B}$ are decreasing, then all peaks of $\mathcal{B}$ are decreasing.*

Proof. To show that all peaks are decreasing we fix a peak $(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow})$ and show that this peak can be completed into a decreasing diagram. The proof is by well-founded induction on $\prec_{\mathsf{peak}}$ and there only is the step case. The interesting situation is when neither τ nor σ are empty, i.e., (using Lemma 19(1) we obtain) $\overset{\tau}{\twoheadrightarrow} = \overset{\beta}{\to} \cdot \overset{\upsilon}{\twoheadrightarrow}$ and $\overset{\sigma}{\twoheadrightarrow} = \overset{\alpha}{\to} \cdot \overset{\rho}{\twoheadrightarrow}$ (see Figure 4a). Hence $(\overset{\beta}{\to}, \overset{\alpha}{\to})$ is a local peak and from the assumption we obtain a decreasing diagram with joining sequences $\overset{\kappa}{\twoheadrightarrow}$ and $\overset{\mu}{\twoheadrightarrow}$. We obtain that $(\overset{\upsilon}{\twoheadrightarrow}, \overset{\kappa}{\twoheadrightarrow})$ is a peak and want to show that the measure of this peak is smaller than that of $(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow})$ (to apply the induction hypothesis). Since β is not empty with Lemma 12 we establish that $|(\overset{\upsilon}{\twoheadrightarrow}, \overset{\kappa}{\twoheadrightarrow})|$ is smaller than $|(\overset{\tau}{\twoheadrightarrow}, \overset{\alpha}{\to})|$ and from $|\alpha| \preccurlyeq_{\mathsf{mul}} |\sigma|$[3] we obtain the desired result. Now, the induction hypothesis yields that IH_1 is a decreasing diagram. Concatenating (using Lemma 19(2)) $\overset{\mu}{\twoheadrightarrow}$ and $\overset{\upsilon'}{\twoheadrightarrow}$ into a sequence $\overset{\tau'}{\twoheadrightarrow}$, using Lemma 21 we can paste the diagrams D and IH_1 into a decreasing diagram (DIH_1, see Figure 4b). The peak $(\overset{\tau'}{\twoheadrightarrow}, \overset{\rho}{\twoheadrightarrow})$ is smaller than the peak $(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow})$ by a mirrored version of

---

[3] This step is not mentioned in [13, 14] but hinted at in [15].

Lemma 12 and hence the induction hypothesis yields the decreasing diagram IH_2. Finally, a mirrored version of Lemma 21 pastes DIH_1 and IH_2 into a decreasing diagram. ◄

We define local decreasingness for ARSs.

▶ **Definition 27** ([13, Definition 3.8])**.** An ARS $\mathcal{A}$ is *locally decreasing* if there exists a transitive and well-founded relation $\prec$ on the labels such that all local peaks are decreasing for (a labeled version of) $\mathcal{A}$.

Finally we arrive at the main result for soundness:

▶ **Corollary 28** ([13, Corollary 3.9])**.** *A locally decreasing ARS is confluent.*

Proof. From local decreasingness we get a transitive and well-founded relation $\prec$ such that all local peaks are decreasing in a labeled version of the ARS. Lemma 26 yields that all peaks are decreasing. The result follows by dropping labels from the labeled rewrite sequences. ◄

4   Formalization of the Conversion Version

In this section we give a formal proof for the main result underlying that local decreasingness with respect to conversions (see [15]) implies confluence. To this end we formally introduce (labeled) conversions, similarly to labeled rewrite sequences. For each object a there is the empty conversion $a \overset{\|}{\leftrightarrow} a$ (also just written a) and if $a \overset{\alpha}{\to} b$ ($a \overset{\alpha}{\leftarrow} b$) is a labeled rewrite step and $b \overset{\sigma}{\leftrightarrow} c$ is a conversion then $a \overset{\alpha}{\to} b \overset{\sigma}{\leftrightarrow} c$ ($a \overset{\alpha}{\leftarrow} b \overset{\sigma}{\leftrightarrow} c$) is a conversion (often written $a \overset{\alpha\sigma}{\leftrightarrow} c$). For conversions we prove similar properties as for sequences (see Lemma 19). In addition we establish that mirroring a conversion again yields a conversion (with the same set of labels) and that every sequence is a conversion.

▶ **Lemma 29.** *Let* $a_1 \overset{\alpha_1}{\leftrightarrow} \cdots \overset{\alpha_{n-1}}{\leftrightarrow} a_n$ *and* $b_1 \overset{\beta_1}{\leftrightarrow} \cdots \overset{\beta_{m-1}}{\leftrightarrow} b_m$ *be conversions.*
1. *Then* $a_1 \overset{\alpha_1}{\leftrightarrow} \cdots \overset{\alpha_{i-1}}{\leftrightarrow} a_i$ *and* $a_i \overset{\alpha_i}{\leftrightarrow} \cdots \overset{\alpha_{n-1}}{\leftrightarrow} a_n$ *are conversions for any* $1 \leqslant i \leqslant n$.
2. *If* $a_n = b_1$ *then* $a_1 \overset{\alpha_1}{\leftrightarrow} \cdots \overset{\alpha_{n-1}}{\leftrightarrow} a_n = b_1 \overset{\beta_1}{\leftrightarrow} \cdots \overset{\beta_{m-1}}{\leftrightarrow} b_m$ *is a conversion.*
3. *Then* $a_n \overset{\alpha_{n-1}}{\leftrightarrow} \cdots \overset{\alpha_1}{\leftrightarrow} a_1$ *is a conversion and* $\{\alpha_1, \ldots, \alpha_n\} = \{\alpha_n, \ldots, \alpha_1\}$.
4. *If* $c_1 \overset{\gamma_1}{\to} \cdots \overset{\gamma_{n-1}}{\to} c_n$ *is a sequence then* $c_1 \overset{\gamma_1}{\leftrightarrow} \cdots \overset{\gamma_{n-1}}{\leftrightarrow} c_n$ *is a conversion.*

Proof. Items (1)-(3) are proved by induction on the first conversion, item (4) is proved by induction on the sequence. ◄

We will also use the following easy lemma being a direct consequence of Definition 3.

▶ **Lemma 30.** *If* $M \preccurlyeq_{mul} N$ *and* $N \subseteq \Upsilon S$ *then* $M \subseteq \Upsilon S$. ◄

The following result (stated as observation in [15]) follows from Lemma 30.

▶ **Lemma 31.** *If* $(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow}, \overset{\sigma'}{\twoheadrightarrow}, \overset{\tau'}{\twoheadrightarrow})$ *is a decreasing diagram and* $|(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow})| \subseteq \Upsilon M$ *then also* $|(\overset{\sigma'}{\twoheadrightarrow}, \overset{\tau'}{\twoheadrightarrow})| \subseteq \Upsilon M$. ◄

A local peak $(\overset{\beta}{\to}, \overset{\alpha}{\to})$ is *decreasing with respect to conversions*[4] if there exist conversions such that the constraints from Figure 5a are satisfied. Now we can state the main result underlying soundness of the conversion version of decreasing diagrams.

---

[4] Please note the asymmetry to the definition of local decreasingness (Definition 25).
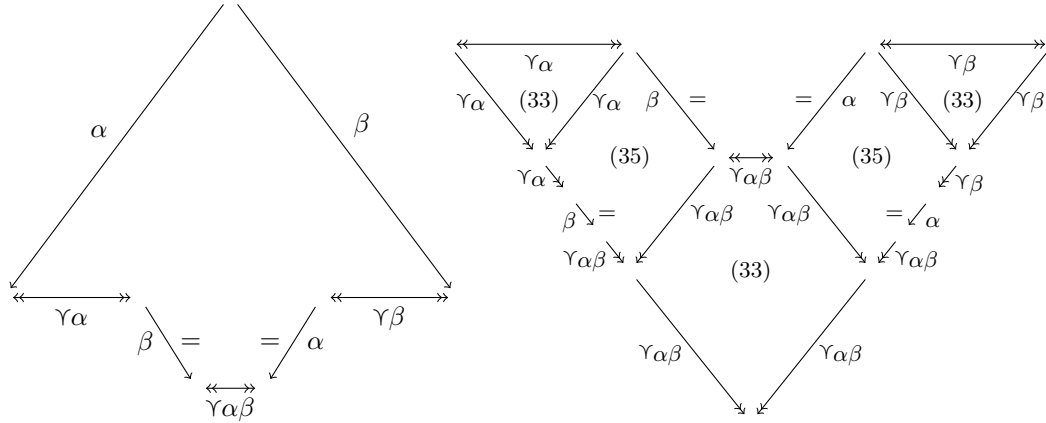
(a) Local decreasingness wrt. conversions.   **(b)** Closing the conversion into a valley.

■ **Figure 5** Conversion version of decreasing diagrams.
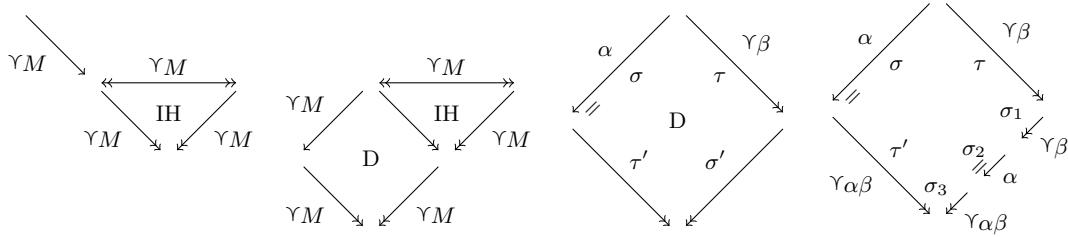
(a) Lemma 33 (case $\to$).   **(b)** Lemma 33 (case $\leftarrow$).   **(c)** Lemma 35.   **(d)** Lemma 35.

■ **Figure 6** Lemmata 33 and 35.

▶ **Lemma 32.** *Let $\mathcal{B}$ be a labeled ARS and $\prec$ be a transitive and well-founded relation on the labels. If all local peaks of $\mathcal{B}$ are decreasing with respect to conversions, then all peaks of $\mathcal{B}$ are decreasing (with respect to valleys).*

Proof. Similar to [15] we follow the proof of the valley version (see Lemma 26). In contrast to Lemma 26 we do not get decreasingness of the local peak $(\xrightarrow{\beta}, \xrightarrow{\alpha})$ (in Figure 4a) by assumption. Instead our assumption yields local decreasingness with respect to conversions, i.e., as depicted in Figure 5a. We close the conversion into a valley as outlined in Figure 5b. To this end we use Lemmata 33 and 35 (see below) and conclude the valleys as shown in Figure 5b. Note that for the final application of Lemma 33 we apply Lemma 29 first, to combine the sequences and conversions into a single conversion. Lemma 13 (lifted to rewriting sequences) then shows decreasingness of the diagram. ◀

The main structure of our proof follows the one from [15]. However, there the proofs of two key results are sketchy and informal. We identified the statements as Lemmata 33 and 35 and provide formal proofs. Note that to establish these properties we can use the induction hypothesis (from the proof of Lemma 32), e.g., peaks whose measure is smaller than $|(\xrightarrow{\beta}, \xrightarrow{\alpha})|$ can be completed into a decreasing diagram.

▶ **Lemma 33.** *Let all peaks smaller than* $|(\xrightarrow{\beta}, \xrightarrow{\alpha})|$ *have a decreasing diagram. Then for any* M *with* $M \prec_{mul} \{\#\alpha, \beta\#\}$ *we have* $\overset{\Upsilon M}{\longleftrightarrow} \subseteq \overset{\Upsilon M}{\twoheadrightarrow} \cdot \overset{\Upsilon M}{\twoheadleftarrow}$.

Proof. By induction on the conversion $\overset{\Upsilon M}{\longleftrightarrow}$. The base case is trivial. In the step case we have $\overset{\Upsilon M}{\longleftrightarrow} \cdot \overset{\Upsilon M}{\longleftrightarrow}$. The induction hypothesis yields $\overset{\Upsilon M}{\longleftrightarrow} \cdot \overset{\Upsilon M}{\twoheadrightarrow} \cdot \overset{\Upsilon M}{\twoheadleftarrow}$. We consider two cases. If the first step is from left to right, i.e., $\overset{\Upsilon M}{\longrightarrow}$ then the result follows from Lemma 29(2) (see Figure 6a). In the other case we have $\overset{\Upsilon M}{\longleftarrow} \cdot \overset{\Upsilon M}{\twoheadrightarrow} \cdot \overset{\Upsilon M}{\twoheadleftarrow}$. Since the peak $\overset{\Upsilon M}{\longleftarrow} \cdot \overset{\Upsilon M}{\twoheadrightarrow}$ has a smaller measure than $(\xrightarrow{\beta}, \xrightarrow{\alpha})$ it can be completed into a decreasing diagram and Lemma 31 in combination with Lemma 29(2) yields the result (see Figure 6b). ◀

To show the second key result we establish a useful decomposition result on sequences.

▶ **Lemma 34.** *Let* $\overset{\sigma}{\twoheadrightarrow}$ *be a sequence and* $\sigma = \sigma_1 \sigma_2$. *Then there are sequences* $\overset{\sigma_1}{\twoheadrightarrow}$ *and* $\overset{\sigma_2}{\twoheadrightarrow}$ *such that* $\overset{\sigma}{\twoheadrightarrow} = \overset{\sigma_1}{\twoheadrightarrow} \cdot \overset{\sigma_2}{\twoheadrightarrow}$.

Proof. By induction on the sequence $\overset{\sigma}{\twoheadrightarrow}$. ◀

Below $\overset{\alpha}{\longrightarrow}^=$ stands for $\overset{\alpha}{\longrightarrow}$ (one step) or $\overset{[]}{\twoheadrightarrow}$ (zero steps). Please note the similarity of the following result to the explicit characterization of local decreasingness (cf. Figure 3a).

▶ **Lemma 35.** *Let all peaks smaller than* $|(\xrightarrow{\beta}, \xrightarrow{\alpha})|$ *have a decreasing diagram. Then the peak* $(\overset{\Upsilon\beta}{\twoheadrightarrow}, \overset{\alpha}{\longrightarrow}^=)$ *can be closed by* $\overset{\Upsilon\alpha\beta}{\twoheadrightarrow} \cdot \overset{\Upsilon\alpha\beta}{\twoheadleftarrow} \cdot \overset{\alpha}{\longleftarrow}^= \cdot \overset{\Upsilon\beta}{\twoheadleftarrow}$ *(see Figure 6d).*

Proof. Since $|(\overset{\Upsilon\beta}{\twoheadrightarrow}, \overset{\alpha}{\longrightarrow}^=)|$ is smaller than $|(\xrightarrow{\beta}, \xrightarrow{\alpha})|$, it can be completed into a decreasing diagram $(\overset{\tau}{\twoheadrightarrow}, \overset{\sigma}{\twoheadrightarrow}, \overset{\sigma'}{\twoheadrightarrow}, \overset{\tau'}{\twoheadrightarrow})$ (see Figure 6c). First we show $\tau' \subseteq \Upsilon\alpha\beta$. From decreasingness and Lemma 10 we get $|\tau'| -s \Upsilon\sigma \preccurlyeq_{mul} |\tau|$. The assumption $\tau \subseteq \Upsilon\beta$ and Lemma 14 yields $|\tau| \subseteq \Upsilon\beta$. Using Lemma 30 we obtain $|\tau'| -s \Upsilon\sigma \subseteq \Upsilon\beta$, i.e. $|\tau'| \subseteq \Upsilon\beta \cup \Upsilon\sigma$. The assumption $\sigma \subseteq \alpha$ yields $\Upsilon\sigma \subseteq \Upsilon\alpha$ and hence we conclude by Lemmata 6(1) and 16(2).

Next we show that $\overset{\sigma'}{\twoheadrightarrow}$ can be decomposed into $\overset{\sigma_1}{\twoheadrightarrow}, \overset{\sigma_2}{\twoheadrightarrow}^=$, and $\overset{\sigma_3}{\twoheadrightarrow}$ with $\sigma_1 \subseteq \Upsilon\beta$, $\sigma_2 \subseteq \{\alpha\}$, length $\sigma_2 \leq 1$, and $\sigma_3 \subseteq \Upsilon\alpha\beta$. To this end we first observe that Lemma 17 also holds if β is not a single label but a sequence (here τ). Then from decreasingness we obtain $\sigma' = \sigma_1 \sigma_2 \sigma_3 \wedge \sigma_1 \subseteq \Upsilon\tau \wedge$ length $\sigma_2 \leq 1 \wedge \sigma_2 \subseteq \{\alpha\} \wedge \sigma_3 \subseteq \Upsilon\alpha\sigma$. Lemma 34 lifts the decomposition of labels to a decomposition of sequences and we can conclude. ◀

An ARS $\mathcal{A}$ is *locally decreasing with respect to conversions* if there exists a transitive and well-founded relation $\prec$ on the labels such that all local peaks are decreasing with respect to conversions for (a labeled version of) $\mathcal{A}$. Finally we arrive at the main result for soundness:

▶ **Corollary 36** ([15, Theorem 3])**.** *A locally decreasing with respect to conversions ARS is confluent.* ◀

5   Meanderings

In this section we discuss differences between our formalization and (proofs from) [13, 15].

Within Isabelle (Abstract_Rewriting.thy) an ARS is a binary relation while in [13] the ARS also contains the domain of the relation. A similar statement holds for labeled ARSs.

General multisets are used in [13], which can represent sets and finite multisets in one go wheres our formalization clearly separates the two concepts. The reason is purely practical, i.e., the Isabelle library already contains the dedicated theories Set.thy and Multiset.thy. The only (negligible) disadvantage we have experienced from this design choice is the need

for multiple definitions of the down-set (for lists, sets, and multisets) and for Lemma 6(1). On the other hand, this saved us from formalizing *general multisets*, which we anticipate as a significant endeavour on its own. Moreover, [13] uses a different multiset extension than Multiset.thy. The latter defines the multiset extension as the transitive closure of the "one-step" multiset extension.

▶ **Definition 37.** The *one-step multiset extension* (denoted by $\prec_{\mathsf{mult1}}$) of $\prec$ is defined by

$$M \prec_{\mathsf{mult1}} N \text{ if } \exists\, a\, I\, K.\ M = I + K,\ N = I + \{\#a\#\},\ \forall\, b \in K.\ b \prec a$$

and the *multiset extension* of $\prec$ (denoted by $\prec_{\mathsf{mult}}$) is the transitive closure of $\prec_{\mathsf{mult1}}$.

Based on the results in Multiset.thy and Definition 3(1) we have proven these two definitions equivalent for any transitive base relation.

▶ **Lemma 38.** *If $\prec$ is transitive then $\prec_{mult}$ and $\prec_{mul}$ coincide.* ◀

Moreover we proved the claim in Definition 3.

▶ **Lemma 39.** *We have that $\preccurlyeq_{mul}$ is the reflexive closure of $\prec_{mul}$.* ◀

Proof. First we show the inclusion from left to right. Let $M \preccurlyeq_{\mathsf{mul}} N$. If $J = \{\#\}$ then $M = N$ and the result follows. If $J \neq \{\#\}$ then $M \prec_{\mathsf{mul}} N$ and we are done.

For the reverse inclusion let (M, N) be in the reflexive closure of $\prec_{\mathsf{mul}}$. If $M = N$ then we finish with $I = M$, $K = J = \{\#\}$. In the other case we get suitable I, J, and K from the definition of $\prec_{\mathsf{mul}}$. ◀

Our formalization is first performed for sequences (of labels) and then lifted to labeled rewrite sequences (conversions), a step which is left implicit in [13]. After introducing labeled rewriting, we proved useful results in Isabelle (Lemmata 19 and 29).

In addition to the algebraic proof of Lemma 6(3) from [13] our formalization contains an alternative one. Our proof of Lemma 8(1) differs from the informal one in [13]. Also the formal proof of Lemma 13 differs from the sketch given for [13, Proposition 3.4], requiring auxiliary results (Lemmata 14 and 16).

There are some (tiny) differences between [13, Theorem 3.7] and Lemma 26. In [13] a measure on *diagrams* is used. However, since the closing/joining steps of the diagram are just obtained by the induction hypothesis the measure must be on *peaks* (which is used in [15]). Moreover, since in either case the measure is a multiset it is hard to relate arbitrary multisets to a peak. Hence we lifted the order on labels $\prec$ to peaks $\prec_{\mathsf{peak}}$ (Section 3.5) and used well-founded induction on this order. In the formalization of Lemma 26 (Footnote 3) we identified a necessary step to apply the induction hypothesis. Another aspect where our formalization deviates from [13] is that the original work uses families of labeled ARSs whereas our formalization considers a single labeled ARS only. Hence [13, Theorem 3.7] states the main result on families of ARSs whereas our Lemma 26 makes a statement about a single ARS.

Concerning [13] our formal proofs for the alternative formulation of local decreasingness (Lemma 13) differs from the one in [13, 14]. While this alternative formulation of local decreasingness was not needed to obtain the main result underlying the valley version ([13, Main Theorem 3.7], i.e., Lemma 26), it was (in a generalized formulation) essential for the main result underlying the conversion version ([15, Theorem 3], i.e., Lemma 32). Furthermore we gave formal proofs for two (informal) key observations made in the proof of [15, Theorem 3], resulting in Lemmata 33 and 35. Especially the latter has a non-trivial formal proof, since the induction hypothesis yields decreasingness (see Figure 6c) but not

the desired decomposition of the joining sequences (see Figure 6d), in contrast to what the proof in [15] conveys.

6   Conclusion

In this paper we have described a formalization of decreasing diagrams in the theorem prover Isabelle following the original proofs from [13,15]. In Sections 3.3 and 3.4 our formal proofs deviate from the either informal or implicit ones in [13] and we also elaborate on Lemma 35, a result which is implicitly used in [15]. To show the applicability of our formalization we performed a mechanical proof of Newman's lemma using decreasing diagrams (following [13, Corollary 4.4]). Our formalization has few dependencies on existing theories. From Abstract_Rewriting.thy we employ some properties for unlabeled abstract rewriting (and the definition of confluence). The theory Multiset.thy provides standard multiset operations and a well-foundedness proof of the multiset extension of a well-founded relation. Note that some of our results on multisets (a formalized proof of [13, Lemma 2.6(3)], i.e., Lemma 6(3)) might be of interest for a larger community.

In [2] a "point version" of decreasing diagrams is introduced, where objects are labeled instead of steps. It is unknown if the point version is equivalent to the standard one. Parts of [2] have been formalized in Coq but 29 axioms are assumed, i.e., not proven in the theorem prover. Furthermore the more useful alternative representation of local decreasingness (Lemma 13) is not considered in [2]. The same holds for the conversion version. Hence [2] is only a *partial* formalization and essentially different from ours.

We anticipate that our contribution paves the way for future work in several directions. One possibility is the formalization of confluence results that can be proven with decreasing diagrams (e.g. Toyama's theorem [26]). The benefit might be two-fold. On the one hand side the proof by decreasing diagrams might be easier to formalize and furthermore proofs by decreasing diagrams are constructive, cf. [16]. Another idea would be the certification of confluence proofs (based on decreasing diagrams) given by automated confluence provers.[5] Both aims require to lift our formalization from abstract rewriting to term rewriting, which is a natural idea for future work.

Acknowledgments

───── **References** ─────

1   Bezem, M., Klop, J., V. van Oostrom: Diagram techniques for confluence. I&C 141(2), 172–204 (1998)

2   Bognar, M.: A point version of decreasing diagrams. In: Proceedings Accolade 1996. Dutch Graduate School in Logic. pp. 1–14 (1997). The formalization is available from `http://web.archive.org/web/20051226052550/http://www.cs.vu.nl/~mirna/`

3   Contejean, E., Courtieu, P., Forest, J., Pons, O., Urbain, X.: Automated certified proofs with CiME3. In: Proc. 22nd RTA. LIPIcs, vol. 10, pp. 21–30 (2011)

---

[5] Certification is already established in the termination community where it has shown tools as well as termination criteria unsound.

4 Dershowitz, N., Manna, Z.: Proving termination with multiset orderings. Comm. ACM 22(8), 465–476 (1979)

5 Felgenhauer, B.: A proof order for decreasing diagrams. In: Proc. 1st IWC. pp. 7–14 (2012)

6 Galdino, A., Ayala-Rincón, M.: A formalization of Newman's and Yokouchi's lemmas in a higher-order language. JFR 1(1), 39–50 (2008)

7 Galdino, A., Ayala-Rincón, M.: A formalization of the Knuth-Bendix(-Huet) critical pair theorem. JAR 45(3), 301–325 (2010)

8 Huet, G.: Residual theory in lambda-calculus: A formal development. JFP 4(3), 371–394 (1994)

9 Jouannaud, J.P., van Oostrom, V.: Diagrammatic confluence and completion. In: Proc. 36th ICALP. LNCS, vol. 5556, pp. 212–222 (2009)

10 Klop, J., van Oostrom, V., de Vrijer, R.: A geometric proof of confluence by decreasing diagrams. JLP 10(3), 437–460 (2000)

11 Nipkow, T.: More Church-Rosser proofs. JAR 26(1), 51–66 (2001)

12 Nipkow, T., Paulson, L., Wenzel, M.: Isabelle/HOL – A Proof Assistant for Higher-Order Logic. vol. 2283 of LNCS. Springer (2002)

13 van Oostrom, V.: Confluence by decreasing diagrams. TCS 126(2), 259–280 (1994)

14 van Oostrom, V.: Confluence for Abstract and Higher-Order Rewriting. PhD thesis, Vrije Universiteit, Amsterdam (1994)

15 van Oostrom, V.: Confluence by decreasing diagrams – converted. In: Proc. 19th RTA. LNCS, vol. 5117, pp. 306–320 (2008)

16 van Oostrom, V.: Modularity of confluence constructed. In: Proc. 4th IJCAR. LNCS, vol. 5195, pp. 348–363 (2008)

17 van Oostrom, V.: Decreasing proof orders – interpreting conversions in involutive monoids. In: Proc. 1st IWC. pp. 1–4 (2012)

18 Pfenning, F.: A proof of the Church-Rosser theorem and its representation in a logical framework. Technical Report CMU-CS-92-186, School of Computer Science, Carnegie Mellon University (1992)

19 Ruiz-Reina, J.L., Alonso, J.A., Hidalgo, M.J., Martín-Mateos, F.J.: Formal proofs about rewriting using ACL2. AMAI 36(3), 239–262 (2002)

20 Shankar, N.: A mechanical proof of the Church-Rosser theorem. JACM 35(3), 475–522 (1988)

21 Sternagel, C., Thiemann, R.: Abstract rewriting. AFP (2010)

22 Støvring, K.: Extending the extensional lambda calculus with surjective pairing is conservative. LMCS 2(2), 14 pages (2006)

23 Takahashi, M.: Parallel reductions in λ-calculus. I&C 118(1), 120–127 (1995)

24 Terese: Term Rewriting Systems. vol. 55 of Cambridge Tracts in Theoretical Computer Science. Cambridge University Press (2003)

25 Thiemann, R.: Certification of confluence proofs using CeTA. In: Proc. 1st IWC. p. 45 (2012)

26 Toyama, Y.: On the Church-Rosser property for the direct sum of term rewriting systems. JACM 34(1), 128–143 (1987)

27 Zankl, H.: Confluence by decreasing diagrams – formalized. CoRR abs/1210.1100v2, 17 pages (2013)