A New and Formalized Proof of Abstract Completion*

Nao Hirokawa[1], Aart Middeldorp[2], and Christian Sternagel[2]

[1] JAIST, Japan hirokawa@jaist.ac.jp
[2] University of Innsbruck, Austria
{aart.middeldorp|christian.sternagel}@uibk.ac.at

Abstract. Completion is one of the most studied techniques in term rewriting. We present a new proof of the correctness of abstract completion that is based on peak decreasingness, a special case of decreasing diagrams. Peak decreasingness replaces Newman's Lemma and allows us to avoid proof orders in the correctness proof of completion. As a result, our proof is simpler than the one presented in textbooks, which is confirmed by our Isabelle/HOL formalization. Furthermore, we show that critical pair criteria are easily incorporated in our setting.

1 Introduction

Knuth and Bendix' completion procedure [11] is a landmark result in term rewriting. Given an equational system $\mathcal{E}$ and a reduction order, the completion procedure aims to construct a complete (terminating and confluent) term rewrite system that is equivalent to $\mathcal{E}$, thereby providing a general solution to the validity problem. Completion has had significant impact on various areas of computer science, in particular automated theorem proving.

The completion process is non-trivial and showing its correctness is a challenge [8]. Bachmair, Dershowitz, and Hsiang [4] introduced abstract inference rules that capture the essence of completion and introduced a new proof technique based on proof orders and persistent sets. This became the de facto standard and has been adopted in textbooks on term rewriting [1,17]. Very recently, this proof was further simplified for finite runs and formalized in Isabelle/HOL by Sternagel and Thiemann [16]. Still, we do not hesitate to point to the intricacy of these proofs, especially when practical critical pair criteria [2,3] are incorporated in completion.

Contribution. In this paper we present a new and formalized correctness proof of abstract completion for finite runs. We introduce a new confluence criterion for abstract rewriting, which we name peak decreasingness, allowing us to abstract from proof orders in order to obtain a simple and elementary proof of the

* Supported by JSPS KAKENHI Grant Number 25730004 and the Austrian Science Fund (FWF) projects I963 and J3202.

correctness of completion. Moreover the proof incorporates a critical pair criterion: it suffices to consider prime critical pairs. Our formalization was conducted using Isabelle/HOL [12].

Formalization. Our formalization is available as part of IsaFoR (an Isabelle/HOL formalization of rewriting) version 2.14.[3] To have a look at the actual formalization visit IsaFoR's website and follow the link *Mercurial repository* under *Downloads.* Alternatively you can download the provided `*.tgz` file. Either way, all the relevant theory files are to be found in the subdirectory `IsaFoR/`. The content of this paper comprises the following theory files: `Renaming` formalizes permutations and permutation types, and proves useful facts about them; `Renaming_Interpretations` gives permutation type instances for terms, rules, substitutions, TRSs, etc., i.e., allows us to apply permutations to them; `Peak_Decreasingness` defines labeled conversions and peak decreasingness, and contains the proof that the latter implies confluence; `CP` defines overlaps, critical peaks, and critical pairs, and proves the critical pair lemma as well as the fact that for finite TRSs only finitely many representatives of critical pairs have to be considered; `Prime_Critical_Pairs` defines prime critical pairs and proves an important result about peaks that allows us to restrict to prime critical pairs for fairness; `Abstract_Completion` defines the inference rules of abstract completion, and proves their soundness; finally `Completion_Fairness` proves soundness of abstract completion when restricting fairness to prime critical pairs. For the benefit of a general audience we present all the proofs in the following on a high level and using standard mathematical notation. Nevertheless the proofs are exactly along the lines of our formalization and from time to time we sprinkle the text with comments directed at Isabelle initiates. But those are not essential for understanding.

Organization. The remainder of the paper is organized as follows. In the next section we recall some rewriting preliminaries. In Section 3 we discuss our formalization of variable renamings. Peak decreasingness is introduced in Section 4. The critical pair lemma, or rather: a formalized critical peak lemma, is the subject of Section 5. Our new correctness proof for abstract completion is presented in full detail in Section 6. Related work is discussed in Section 7 before we conclude in Section 8.

2 Preliminaries

We assume familiarity with term rewriting and all that (e.g., [1]) and only shortly recall notions that are used in the following. An *abstract rewrite system* (ARS for short) $\mathcal{A}$ is a set A, also called the carrier, equipped with a binary relation $\to$. Sometimes we partition the binary relation into parts according to a set I of indices (or labels). Then we write $\mathcal{A} = \langle A, \{\to_\alpha\}_{\alpha\in I}\rangle$ where we denote the part of the relation with label α by $\to_\alpha$, i.e., $\to = \bigcup_{\alpha\in I} \to_\alpha$. In our formalization

[3] http://cl-informatik.uibk.ac.at/software/ceta

ARSs are just relations which are represented by sets of pairs in Isabelle/HOL, i.e., of type $(\alpha \times \alpha)$ *set*, and their carrier is given implicitly by the type α.

Terms are defined inductively as follows: a *term* is either a variable x from the set $\mathcal{V}$ or is constructed by applying a function symbol $f \in \mathcal{F}$ to a list of argument terms $f(t_1, \ldots, t_n)$. Here $\mathcal{F}$ is called the *signature*. The set of all terms built over $\mathcal{F}$ and $\mathcal{V}$ is denoted by $\mathcal{T}(\mathcal{F}, \mathcal{V})$. In our formalization terms are represented by the datatype

datatype *(α, β) term = Var β | Fun α ((α, β) term list)*

that is, the signature as well as the set of variables is given implicitly by the type parameters α and β, respectively. The *set of variables* of a term t is denoted by $\mathcal{V}\mathsf{ar}(t)$ (this is easily extended to rules, term rewrite systems, etc.). *Positions* are finite lists of positive natural numbers where the empty position (or *root position*) is denoted by ϵ. The set of positions of a term t is denoted by $\mathcal{P}\mathsf{os}(t)$ and partitioned into *function positions* $\mathcal{P}\mathsf{os}_{\mathcal{F}}$ and *variable positions* $\mathcal{P}\mathsf{os}_{\mathcal{V}}$. Positions are partially ordered by the prefix order, i.e., $p \leqslant q$ if p is a prefix of q (we also say that p is above q). Two positions p and q for which neither $p \leqslant q$ nor $q \leqslant p$ are called *parallel*, denoted by $p \parallel q$. Whenever $p \leqslant q$, by $q \setminus p$ we denote position q without its prefix p. The subterm of t at position p is denoted by $t|_p$ and replacing this term by s is denoted by $t[s]_p$.

A *substitution* is a mapping σ from variables to terms such that its domain $\{x \in \mathcal{V} \mid \sigma(x) \neq x\}$ is finite. Applying a substitution to a term is written $t\sigma$.

A pair of terms (s, t) is sometimes considered an *equation*, then we write $s \approx t$, and sometimes a *(rewrite) rule*, then we write $s \to t$. In the latter case we assume that the left-hand side is not a variable and that the variables of the right-hand side t are all contained in the left-hand side s. This assumption we call the *variable condition*.

A set $\mathcal{E}$ of equations is called an *equational system* (ES for short) and a set $\mathcal{R}$ of rules a *term rewrite system* (TRS for short). In the following we assume the variable condition for all rules of a TRS. Sets of pairs of terms induce a *rewrite relation* by closing their components under contexts and substitutions. More precisely the rewrite relation of $\mathcal{R}$, denoted by $\to_{\mathcal{R}}$, is defined inductively by $s \to_{\mathcal{R}} t$ whenever there are a rule $\ell \to r \in \mathcal{R}$, a position p, and a substitution σ such that $s|_p = \ell\sigma$ and $t = s[r\sigma]_p$. In the following we sometimes drop $\mathcal{R}$ in $\to_{\mathcal{R}}$ if it is clear from the context. Moreover, individual steps are sometimes annotated with additional information (the employed rule, the corresponding position, etc.).

A binary relation $\to$ is well-founded (or *terminating*) if it does not admit any infinite descending sequence $a_1 \to a_2 \to a_3 \to \cdots$. A well-founded order that is closed under contexts and substitutions is called a *reduction order*. Thus a reduction order that strictly orients all rules of a TRS establishes termination of the induced rewrite relation.

3 Renaming Variables

This section is not essential for understanding the remainder of the paper. However, it addresses a typical problem that arises when formalizing proofs involving variable renaming. Thus it is mostly interesting for users of proof assistants.

One thing that is often neglected or treated implicitly in paper proofs is renaming of variables, which is often necessary to make sure that two given objects do not contain any common variables. While on the one hand, this is clearly not good enough for a formalization using a proof assistant; on the other hand, a thorough treatment quickly leads to tedious reasoning (which is typically left as an exercise in textbooks; see for example the proof of the statement that two most general unifiers only differ by a renaming in [17, Chapter 2] and [1, Chapter 4]).

We aim for a setup that allows us to argue along the lines of a paper proof also in its formalization. The advantage of doing so is that not only the result is certified to be correct, but also the proof itself. Moreover, simulating the implicit reasoning used in a paper proof should be as painless as possible.

To this end it turns out that a slight modification of a previous Isabelle/HOL formalization of permutations and permutation types by Urban *et al.* [9,18] is very useful. Here a permutation (also called renaming) is just a bijective function f such that $\{x \mid f(x) \neq x\}$ is finite, and a *permutation type* is a type whose elements support applying a permutation to them. The mentioned modification consists in parameterizing permutation types over the type of atoms (which we call variables in the following) in addition to the type of elements (which may be terms, substitutions, rules, TRSs, etc.) To make this possible we have to switch from Isabelle's type classes to locales and therefore to reformalize a theory of permutations (thankfully, most proofs are not much different from the type class version). Moreover many useful results only hold under the assumption that we have an infinite set of variables, e.g., that we can always rename the variables of two finite objects apart. This we express in Isabelle by demanding that the type of variables is in the type class *infinite* (whose only assumption says that the universe of all values of the corresponding type be infinite). Permutation types are expressed as follows in Isabelle (see theory `Renaming`):

locale *pt* =
  fixes $\cdot$ :: *(*α :: *infinite) perm* $\Rightarrow$ β $\Rightarrow$ β
  assumes $id \cdot x = x$ ***and*** $(\pi_1 \circ \pi_2) \cdot x = \pi_1 \cdot (\pi_2 \cdot x)$

where id is the empty permutation, $\circ$ denotes function composition, and $\pi \cdot x$ denotes applying the renaming π to the element x. Also note that α :: *infinite* requires the type α to contain infinitely many elements. Associated with each permutation type is the notion of *support*. Since we will not give any more details about permutation types, suffice it to say that for permutation types whose elements have finite support, this notion corresponds to the set of free variables.

The most important result about finitely supported permutation types for our purposes is that we can always find a permutation π which makes the support

of x disjoint from a given finite set of variables. Intuitively, this means that we can always rename variables apart.

After a general theory of renamings we have to create concrete instances for terms, rules, substitutions, TRSs, etc. (see theory `Renaming_Interpretations`). Using this machinery we have formalized the following results (the interested reader is referred to the formalization for proofs).

Lemma 1. *Let σ and τ be substitutions.*[4]

1. *If σ' and τ' are substitutions with $\sigma\sigma' = \tau$ and $\tau\tau' = \sigma$ then there is a renaming π such that $\pi \cdot \sigma = \tau$.*
2. *If σ and τ are two most general unifiers of a set of equations, then they are variants of each other.*

In the remainder, whenever we say that a term t is a *variant* of a term u, what we formally mean is that there is a permutation π such that $\pi \cdot t = u$. Of course, this also works for rules, substitutions, TRSs, etc.

4 Peak Decreasingness

In this section we present the abstract result that replaces Newman's Lemma in the proof of the correctness of abstract completion.

Definition 2. *An ARS $\mathcal{A} = \langle A, \{\to_\alpha\}_{\alpha\in I}\rangle$ is* peak decreasing *if there exists a well-founded order $>$ on I such that for all $\alpha, \beta \in I$ the inclusion*

$$ {}_\alpha\!\leftarrow \cdot \to_\beta \;\subseteq\; \overset{*}{\underset{\vee\alpha\beta}{\longleftrightarrow}} $$

holds. Here $\vee\alpha\beta$ denotes the set $\{\gamma \in I \mid \alpha > \gamma \text{ or } \beta > \gamma\}$ and if $J \subseteq I$ then $\underset{J}{\to}$ denotes the union of all $\underset{\gamma}{\to}$ with $\gamma \in J$ and $\overset{*}{\underset{J}{\leftrightarrow}}$ denotes a conversion consisting of $\underset{J}{\to}$ steps.

Peak decreasingness is a special case of decreasing diagrams [13], which is known as a powerful confluence criterion. Correctness of decreasing diagrams has been formally verified in Isabelle/HOL by Zankl [20] and it should in principle be possible to obtain our results on peak decreasingness as a special case. However, for the sake of simplicity we present its easy direct proof (which we also formalized in order to verify its correctness). We denote by $\mathcal{M}(J)$ the set of all multisets over a set J.

Lemma 3. *Every peak decreasing ARS is confluent.*

Proof. Let $>$ be a well-founded order on I which shows that the ARS $\mathcal{A} = \langle A, \{\to_\alpha\}_{\alpha\in I}\rangle$ is peak decreasing. With every conversion C in $\mathcal{A}$ we associate the multiset M_C consisting of the labels of its steps. These multisets are compared by the multiset extension $>_{\mathsf{mul}}$ of $>$, which is a well-founded order on $\mathcal{M}(I)$.

[4] Finiteness of substitution domains is used (only) for this lemma (in this paper).

We prove $\leftrightarrow^* \subseteq \downarrow$ by well-founded induction on $>_{\mathsf{mul}}$. Consider a conversion C between a and b. We either have $a \downarrow b$ or $a \leftrightarrow^* \cdot \leftarrow \cdot \rightarrow \cdot \leftrightarrow^* b$. In the former case we are done. In the latter case there exist labels $\alpha, \beta \in I$ and multisets $\Gamma_1, \Gamma_2 \in \mathcal{M}(I)$ such that $M_C = \Gamma_1 \uplus \{\alpha, \beta\} \uplus \Gamma_2$. By the peak decreasingness assumption there exists a conversion C' between a and b such that $M_{C'} = \Gamma_1 \uplus \Gamma \uplus \Gamma_2$ with $\Gamma \in \mathcal{M}(\vee\alpha\beta)$. We obviously have $\{\alpha, \beta\} >_{\mathsf{mul}} \Gamma$ and hence $M_C >_{\mathsf{mul}} M_{C'}$. We obtain $a \downarrow b$ from the induction hypothesis. □

What we informally state as *with every conversion we associate the multiset of the labels of its steps* in the proof above is formalized as an inductive predicate $\twoheadleftarrow\!\!\!\!\twoheadrightarrow$ defined by the rules

$$\frac{}{a \twoheadleftarrow\!\!\!\!\twoheadrightarrow_{\{\}} a} \qquad\qquad \frac{\alpha \in I \qquad a \overset{\alpha}{\leftrightarrow} b \qquad b \twoheadleftarrow\!\!\!\!\twoheadrightarrow_M c}{a \twoheadleftarrow\!\!\!\!\twoheadrightarrow_{M \uplus \{\alpha\}} c}$$

together with the fact that for all a and b, we have $a \leftrightarrow^* b$ if and only if there is a multiset M such that $a \twoheadleftarrow\!\!\!\!\twoheadrightarrow_M b$. (This predicate is called *conv* in theory `Peak_Decreasingness`.)

5 Critical Pair Lemma

Completion is based on critical pair analysis. In this section we present a version of the critical pair lemma that incorporates primality. The correctness proof is based on peak decreasingness.

Definition 4. *An overlap of a TRS $\mathcal{R}$ is a triple $\langle \ell_1 \to r_1, p, \ell_2 \to r_2 \rangle$ satisfying the following properties:*

- *there are renamings π_1 and π_2 such that $\pi_1 \cdot (\ell_1 \to r_1), \pi_2 \cdot (\ell_2 \to r_2) \in \mathcal{R}$,*
- *$\mathcal{V}\mathsf{ar}(\ell_1 \to r_1) \cap \mathcal{V}\mathsf{ar}(\ell_2 \to r_2) = \varnothing$,*
- *$p \in \mathcal{P}\mathsf{os}_{\mathcal{F}}(\ell_2)$,*
- *ℓ_1 and $\ell_2|_p$ are unifiable,*
- *if $p = \epsilon$ then $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are not variants.*

In general this definition may lead to an infinite set of overlaps, since there are infinitely many possibilities of taking variable disjoint variants of rules. Fortunately it can be shown (and has been formalized) that overlaps that originate from the same two rules are variants of each other (see theory `CP`). Overlaps give rise to critical peaks and pairs.

Definition 5. *Suppose $\langle \ell_1 \to r_1, p, \ell_2 \to r_2 \rangle$ is an overlap of a TRS $\mathcal{R}$. Let σ be a most general unifier of ℓ_1 and $\ell_2|_p$. The term $\ell_2\sigma[\ell_1\sigma]_p = l_2\sigma$ can be reduced in two different ways:*

$$\begin{array}{ccc} & \ell_2\sigma[\ell_1\sigma]_p = \ell_2\sigma & \\ {\scriptstyle \ell_1 \to r_1,\ p} \swarrow & & \searrow {\scriptstyle \ell_2 \to r_2,\ \epsilon} \\ \ell_2\sigma[r_1\sigma]_p & & r_2\sigma \end{array}$$

We call the quadruple $(\ell_2\sigma[r_1\sigma]_p, p, \ell_2\sigma, r_2\sigma)$ *a* critical peak *and the equation* $\ell_2\sigma[r_1\sigma]_p \approx r_2\sigma$ *a* critical pair *of* $\mathcal{R}$*, obtained from the overlap. The set of all critical pairs of* $\mathcal{R}$ *is denoted by* $\mathsf{CP}(\mathcal{R})$*.*

In our formalization we do not use an arbitrary most general unifier in the above definition. Instead we use *the* most general unifier that is computed by the formalized unification algorithm that is part of IsaFoR (thereby removing one degree of freedom and making it easier to show that only finitely many critical pairs have to be considered for finite TRSs).

A critical peak (t, p, s, u) is usually denoted by $t \overset{p}{\leftarrow} s \overset{\epsilon}{\rightarrow} u$. It can be shown (and has been formalized) that different critical peaks and pairs obtained from two variants of the same overlap are variants of each other. Since rewriting is equivariant under permutations, it is enough to consult finitely many critical pairs or peaks for finite TRSs (one for each pair of rules and each appropriate position) in order to conclude rewriting related properties (like joinability or fairness, see below) for all of them.

We present a variation of the well-known critical pair lemma for critical peaks and its formalized proof. The slightly cumbersome statement is essential to avoid gaps in the proof of Lemma 9 below.

Lemma 6. *Let* $\mathcal{R}$ *be a TRS. If* $t \mathrel{{}_{\mathcal{R}}\!\overset{p_1}{\leftarrow}} s \overset{p_2}{\rightarrow}_{\mathcal{R}} u$ *then one of the following holds:*

(a) $t \downarrow_{\mathcal{R}} u$*,*

(b) $p_2 \leqslant p_1$ *and* $t|_{p_2} \overset{p_1 \setminus p_2}{\leftarrow} s|_{p_2} \overset{\epsilon}{\rightarrow} u|_{p_2}$ *is an instance of a critical peak,*

(c) $p_1 \leqslant p_2$ *and* $u|_{p_1} \overset{p_2 \setminus p_1}{\leftarrow} s|_{p_1} \overset{\epsilon}{\rightarrow} t|_{p_1}$ *is an instance of a critical peak.*

Proof. Consider an arbitrary peak $t \mathrel{{}_{p_1,\ell_1'\to r_1',\sigma_1'}\!\leftarrow} s \mathrel{\rightarrow_{p_2,\ell_2\to r_2,\sigma_2}} u$. If $p_1 \parallel p_2$ then $t \mathrel{\rightarrow_{p_2,\ell_2\to r_2,\sigma_2}} t[r_2\sigma_2]_{p_2} = u[r_1'\sigma_1']_{p_1} \mathrel{{}_{p_1,\ell_1'\to r_1',\sigma_1'}\!\leftarrow} u$. If the positions of the contracted redexes are not parallel then one of them is above the other. Without loss of generality we assume that $p_1 \geqslant p_2$. Let $p = p_1 \setminus p_2$. Moreover, let π be a permutation such that $\ell_1 \to r_1 = \pi \cdot (\ell_1' \to r_1')$ and $\ell_2 \to r_2$ have no variables in common. Such a permutation exists since we only have to avoid the finitely many variables of $\ell_2 \to r_2$ and assume an infinite set of variables. Furthermore, let $\sigma_1 = \pi^{-1} \cdot \sigma_1'$. We have $t = s[r_1\sigma_1]_{p_1} = s[\ell_2\sigma_2[r_1\sigma_1]_p]_{p_2}$ and $u = s[r_2\sigma_2]_{p_2}$. We consider two cases depending on whether $p \in \mathcal{P}\mathsf{os}_{\mathcal{F}}(\ell_2)$ in conjunction with the fact that whenever $p = \epsilon$ then $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are not variants, is true or not.

- Suppose $p \in \mathcal{P}\mathsf{os}_{\mathcal{F}}(\ell_2)$ and $p = \epsilon$ implies that $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are not variants. Let $\sigma'(x) = \sigma_1(x)$ for $x \in \mathcal{V}\mathsf{ar}(\ell_1 \to r_1)$ and $\sigma'(x) = \sigma_2(x)$, otherwise. The substitution σ' is a unifier of $\ell_2|_p$ and ℓ_1: $(\ell_2|_p)\sigma' = (\ell_2\sigma_2)|_p = \ell_1\sigma_1 = \ell_1\sigma'$. Then $\langle \ell_1 \to r_1, p, \ell_2 \to r_2 \rangle$ is an overlap. Let σ be a most general unifier of $\ell_2|_p$ and ℓ_1. Hence $\ell_2\sigma[r_1\sigma]_p \overset{p}{\leftarrow} \ell_2\sigma \overset{\epsilon}{\rightarrow} r_2\sigma$ is a critical peak and there exists a substitution τ such that $\sigma' = \sigma\tau$. Therefore

$$\ell_2\sigma_2[r_1\sigma_1]_p = (\ell_2\sigma[r_1\sigma]_p)\tau \overset{p}{\leftarrow} (\ell_2\sigma)\tau \overset{\epsilon}{\rightarrow} (r_2\sigma)\tau = r_2\sigma_2$$

  and thus (b) is obtained.

– Otherwise, either $p = \epsilon$ and $\ell_1 \to r_1$, $\ell_2 \to r_2$ are variants, or $p \notin \mathcal{P}\mathsf{os}_{\mathcal{F}}(\ell_2)$. In the former case it is easy to show that $r_1\sigma_1 = r_2\sigma_2$ and hence $t = u$. In the latter case, there exist positions q_1, q_2 such that $p = q_1q_2$ and $q_1 \in \mathcal{P}\mathsf{os}_{\mathcal{V}}(\ell_2)$. Let $\ell_2|_{q_1}$ be the variable x. We have $\sigma_2(x)|_{q_2} = \ell_1\sigma_1$. Define the substitution σ_2' as follows:

$$\sigma_2'(y) = \begin{cases} \sigma_2(y)[r_1\sigma_1]_{q_2} & \text{if } y = x \\ \sigma_2(y) & \text{if } y \neq x \end{cases}$$

Clearly $\sigma_2(x) \to_{\mathcal{R}} \sigma_2'(x)$, and thus $r_2\sigma_2 \to^* r_2\sigma_2'$. We also have

$$\ell_2\sigma_2[r_1\sigma_1]_p = \ell_2\sigma_2[\sigma_2'(x)]_{q_1} \to^* \ell_2\sigma_2' \to r_2\sigma_2'$$

Consequently, $t \to^* s[r_2\sigma_2']_{p_2}\ {}^*\!\leftarrow u$. Hence, (c) is concluded. □

An easy consequence of the above lemma is that for every peak $t \mathrel{\mathcal{R}\!\leftarrow} s \to_{\mathcal{R}} u$ we have $t \downarrow_{\mathcal{R}} u$ or $t \leftrightarrow_{\mathsf{CP}(\mathcal{R})} u$. It might be interesting to note that in our formalization of the above proof we do actually not need the fact that left-hand sides of rules are not variables.

Definition 7. *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. A critical pair is called prime if it is derived from a prime critical peak. We write $\mathsf{PCP}(\mathcal{R})$ to denote the set of all prime critical pairs of a TRS $\mathcal{R}$.*

Below we prove that non-prime critical pairs need not be computed. In the proof we use a new ternary relation on terms. It expresses the condition under which a conversion between two terms is considered harmless (when it comes to proving confluence of terminating TRSs). This relation is also used in the new correctness proof of abstract completion that we present in the next section.

Definition 8. *Given a TRS $\mathcal{R}$ and terms s, t, and u, we write $t \mathrel{\triangledown_s} u$ if $s \to_{\mathcal{R}}^+ t$, $s \to_{\mathcal{R}}^+ u$, and $t \downarrow_{\mathcal{R}} u$ or $t \leftrightarrow_{\mathsf{PCP}(\mathcal{R})} u$.*

Lemma 9. *Let $\mathcal{R}$ be a TRS. If $t \overset{p}{\leftarrow} s \overset{\epsilon}{\to} u$ is a critical peak then $t \mathrel{\triangledown_s^2} u$.*

Proof. First suppose that all proper subterms of $s|_p$ are in normal form. Then $t \approx u \in \mathsf{PCP}(\mathcal{R})$ and thus $t \mathrel{\triangledown_s} u$. Since also $u \mathrel{\triangledown_s} u$, we obtain the desired $t \mathrel{\triangledown_s^2} u$. This leaves us with the case that there is a proper subterm of $s|_p$ that is not in normal form. By considering an innermost redex in $s|_p$ we obtain a position $q > p$ and a term v such that $s \overset{q}{\to} v$ and all proper subterms of $s|_q$ are in normal form. Now, if $v \overset{q}{\leftarrow} s \overset{\epsilon}{\to} u$ is an instance of a critical peak then $v \to_{\mathsf{PCP}(\mathcal{R})} u$. Otherwise, $v \downarrow_{\mathcal{R}} u$ by Lemma 6, since $q \not\leqslant \epsilon$. In both cases we obtain $v \mathrel{\triangledown_s} u$. Finally, we analyze the peak $t \overset{p}{\leftarrow} s \overset{q}{\to} v$ by another application of Lemma 6.

1. If $t \downarrow_{\mathcal{R}} v$, we obtain $t \mathrel{\triangledown_s} v$ and thus $t \mathrel{\triangledown_s^2} u$, since also $v \mathrel{\triangledown_s} u$.
2. Since $p < q$, only the case that $v|_p \overset{q\backslash p}{\longleftarrow} s|_p \overset{\epsilon}{\to} t|_p$ is an instance of a critical peak remains. Moreover, all proper subterms of $s|_q$ are in normal form and thus we have an instance of a prime critical peak. Hence $t \leftrightarrow_{\mathsf{PCP}(\mathcal{R})} v$ and together with $v \mathrel{\triangledown_s} u$ we conclude $t \mathrel{\triangledown_s^2} u$. □

Corollary 10. *Let $\mathcal{R}$ be a TRS. If $t \mathrel{{}_{\mathcal{R}}\!\leftarrow} s \to_{\mathcal{R}} u$ then $t \mathrel{\nabla_s^2} u$.*

Proof. From Lemma 6, either $t \downarrow_{\mathcal{R}} u$ and we are done, or $t \mathrel{{}_{\mathcal{R}}\!\leftarrow} s \to_{\mathcal{R}} u$ contains a (possibly reversed) instance of a critical peak. By Lemma 9 we conclude the proof, since rewriting is closed under substitutions and contexts. □

The following result is due to Kapur *et al.* [10, Corollary 4].

Corollary 11. *A terminating TRS is confluent if and only if all its prime critical pairs are joinable.*

Proof. Let $\mathcal{R}$ be a terminating TRS such that $\mathsf{PCP}(\mathcal{R}) \subseteq \downarrow_{\mathcal{R}}$. We label rewrite steps by their starting term and we claim that $\mathcal{R}$ is peak decreasing. As well-founded order we take $> = \to_{\mathcal{R}}^+$. Consider an arbitrary peak $t \mathrel{{}_{\mathcal{R}}\!\leftarrow} s \to_{\mathcal{R}} u$. Lemma 10 yields a term v such that $t \mathrel{\nabla_s} v \mathrel{\nabla_s} u$. From the assumption $\mathsf{PCP}(\mathcal{R}) \subseteq \downarrow_{\mathcal{R}}$ we obtain $t \downarrow_{\mathcal{R}} v \downarrow_{\mathcal{R}} u$. Since $s \to_{\mathcal{R}}^+ v$, all steps in the conversion $t \downarrow_{\mathcal{R}} v \downarrow_{\mathcal{R}} u$ are labeled with a term that is smaller than s. Since the two steps in the peak receive the same label s, peak decreasingness is established and hence we obtain the confluence of $\mathcal{R}$ from Lemma 3. The reverse direction is trivial. □

Note that unlike for ordinary critical pairs, joinability of prime critical pairs does not imply local confluence.

Example 12. Consider the following TRS $\mathcal{R}$:

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

The set $\mathsf{PCP}(\mathcal{R})$ consists of the pairs $\mathsf{f}(\mathsf{a}) \approx \mathsf{b}$ and $\mathsf{f}(\mathsf{a}) \approx \mathsf{c}$, which are trivially joinable. But $\mathcal{R}$ is not locally confluent because the peak $\mathsf{b} \mathrel{{}_{\mathcal{R}}\!\leftarrow} \mathsf{f}(\mathsf{a}) \to_{\mathcal{R}} \mathsf{c}$ is not joinable.

6 Abstract Completion

The abstract completion procedure for which we give a new and formalized correctness proof is presented in the following definition.

Definition 13. *The inference system KB operates on pairs consisting of an ES $\mathcal{E}$ and a TRS $\mathcal{R}$ over a common signature $\mathcal{F}$. It consists of the following six inference rules:*

$$\textsf{deduce}\ \frac{\mathcal{E}, \mathcal{R}}{\mathcal{E} \cup \{s \approx t\}, \mathcal{R}}\ \textit{if } s \mathrel{{}_{\mathcal{R}}\!\leftarrow} \cdot \to_{\mathcal{R}} t \qquad \textsf{compose}\ \frac{\mathcal{E}, \mathcal{R} \uplus \{s \to t\}}{\mathcal{E}, \mathcal{R} \cup \{s \to u\}}\ \textit{if } t \to_{\mathcal{R}} u$$

$$\textsf{orient}\ \frac{\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}}{\mathcal{E}, \mathcal{R} \cup \{s \to t\}}\ \textit{if } s > t \quad \frac{\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}}{\mathcal{E}, \mathcal{R} \cup \{t \to s\}}\ \textit{if } t > s \qquad \textsf{simplify}\ \frac{\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}}{\mathcal{E} \cup \{u \approx t\}, \mathcal{R}}\ \textit{if } s \to_{\mathcal{R}} u \quad \frac{\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}}{\mathcal{E} \cup \{s \approx u\}, \mathcal{R}}\ \textit{if } t \to_{\mathcal{R}} u$$

$$\textsf{delete}\ \frac{\mathcal{E} \uplus \{s \approx s\}, \mathcal{R}}{\mathcal{E}, \mathcal{R}} \qquad \textsf{collapse}\ \frac{\mathcal{E}, \mathcal{R} \uplus \{t \to s\}}{\mathcal{E} \cup \{u \approx s\}, \mathcal{R}}\ \textit{if } t \to_{\mathcal{R}} u$$

Here $>$ is a fixed reduction order on $\mathcal{T}(\mathcal{F},\mathcal{V})$.

Inference rules for completion were introduced by Bachmair, Dershowitz, and Hsiang in [4]. The version above differs from most of the inference systems in the literature (e.g. [2,3]) in that we do not impose any encompassment restriction in collapse. The reason is that only *finite* runs will be considered here (cf. [16]).

We write $(\mathcal{E},\mathcal{R})$ for the pair $\mathcal{E},\mathcal{R}$ when it increases readability. We write $(\mathcal{E},\mathcal{R}) \vdash_{\mathsf{KB}} (\mathcal{E}',\mathcal{R}')$ if $(\mathcal{E}',\mathcal{R}')$ can be obtained from $(\mathcal{E},\mathcal{R})$ by applying one of the inference rules of Definition 13.

According to the following lemma the equational theory induced by $\mathcal{E}\cup\mathcal{R}$ is not affected by application of the inference rules of KB. This is well-known, but our formulation is new and paves the way for a simple correctness proof.

Lemma 14. *Suppose $(\mathcal{E},\mathcal{R}) \vdash_{\mathsf{KB}} (\mathcal{E}',\mathcal{R}')$.*

1. *If $s \xrightarrow[\mathcal{E}\cup\mathcal{R}]{} t$ then $s \xrightarrow[\mathcal{R}']{=} \cdot \xrightarrow[\mathcal{E}'\cup\mathcal{R}']{=} \cdot \xleftarrow[\mathcal{R}']{=} t$.*
2. *If $s \xrightarrow[\mathcal{E}'\cup\mathcal{R}']{} t$ then $s \xleftarrow[\mathcal{E}\cup\mathcal{R}]{*} t$.*

Proof. By inspecting the inference rules of KB we easily obtain the following inclusions:

deduce			
$\mathcal{E}\cup\mathcal{R}$	$\subseteq \mathcal{E}'\cup\mathcal{R}'$	$\mathcal{E}'\cup\mathcal{R}'$	$\subseteq \mathcal{E}\cup\mathcal{R}\cup \xleftarrow[\mathcal{R}]{}\cdot\xrightarrow[\mathcal{R}]{}$
orient			
$\mathcal{E}\cup\mathcal{R}$	$\subseteq \mathcal{E}'\cup\mathcal{R}'\cup(\mathcal{R}')^{-1}$	$\mathcal{E}'\cup\mathcal{R}'$	$\subseteq \mathcal{E}\cup\mathcal{R}\cup\mathcal{E}^{-1}$
delete			
$\mathcal{E}\cup\mathcal{R}$	$\subseteq \mathcal{E}'\cup\mathcal{R}'\cup=$	$\mathcal{E}'\cup\mathcal{R}'$	$\subseteq \mathcal{E}\cup\mathcal{R}$
compose			
$\mathcal{E}\cup\mathcal{R}$	$\subseteq \mathcal{E}'\cup\mathcal{R}'\cup\xrightarrow[\mathcal{R}']{}\cdot\xleftarrow[\mathcal{R}']{}$	$\mathcal{E}'\cup\mathcal{R}'$	$\subseteq \mathcal{E}\cup\mathcal{R}\cup\xrightarrow[\mathcal{R}]{}\cdot\xrightarrow[\mathcal{R}]{}$
simplify			
$\mathcal{E}\cup\mathcal{R}$	$\subseteq \mathcal{E}'\cup\mathcal{R}'\cup\xrightarrow[\mathcal{R}']{}\cdot\xrightarrow[\mathcal{E}']{}\cup\xrightarrow[\mathcal{E}']{}\cdot\xleftarrow[\mathcal{R}']{}$	$\mathcal{E}'\cup\mathcal{R}'$	$\subseteq \mathcal{E}\cup\mathcal{R}\cup\xleftarrow[\mathcal{R}]{}\cdot\xrightarrow[\mathcal{E}]{}\cup\xrightarrow[\mathcal{E}]{}\cdot\xrightarrow[\mathcal{R}]{}$
collapse			
$\mathcal{E}\cup\mathcal{R}$	$\subseteq \mathcal{E}'\cup\mathcal{R}'\cup\xrightarrow[\mathcal{R}']{}\cdot\xrightarrow[\mathcal{E}']{}$	$\mathcal{E}'\cup\mathcal{R}'$	$\subseteq \mathcal{E}\cup\mathcal{R}\cup\xleftarrow[\mathcal{R}]{}\cdot\xrightarrow[\mathcal{R}]{}$

Consider for instance the collapse rule and suppose that $s \approx t \in \mathcal{E}\cup\mathcal{R}$. If $s\approx t\in\mathcal{E}$ then $s\approx t\in\mathcal{E}'$ because $\mathcal{E}\subseteq\mathcal{E}'$. If $s\approx t\in\mathcal{R}$ then either $s\approx t\in\mathcal{R}'$ or $s\to_{\mathcal{R}} u$ with $u\approx t\in\mathcal{E}'$ and thus $s\to_{\mathcal{R}'}\cdot\to_{\mathcal{E}'} t$. This proves the inclusion on the left. For the inclusion on the right the reasoning is similar. Suppose that $s\approx t\in\mathcal{E}'\cup\mathcal{R}'$. If $s\approx t\in\mathcal{R}'$ then $s\approx t\in\mathcal{R}$ because $\mathcal{R}'\subseteq\mathcal{R}$. If $s\approx t\in\mathcal{E}'$ then either $s\approx t\in\mathcal{E}$ or there exists a rule $u\to t\in\mathcal{R}$ with $u\to_{\mathcal{R}} s$ and thus $s\,{}_{\mathcal{R}}\!\leftarrow\cdot\to_{\mathcal{R}} t$.

Since rewrite relations are closed under contexts and substitutions, the inclusions in the right column prove statement (2). Because each inclusion in the left column is a special case of

$$\mathcal{E}\cup\mathcal{R} \subseteq \xrightarrow[\mathcal{R}']{=}\cdot\xrightarrow[\mathcal{E}'\cup\mathcal{R}']{=}\cdot\xleftarrow[\mathcal{R}']{=}$$

also statement (1) follows from the closure under contexts and substitutions of rewrite relations. □

Corollary 15. *If* $(\mathcal{E},\mathcal{R}) \vdash^*_{\mathsf{KB}} (\mathcal{E}',\mathcal{R}')$ *then* $\overset{*}{\underset{\mathcal{E}\cup\mathcal{R}}{\longleftrightarrow}} = \overset{*}{\underset{\mathcal{E}'\cup\mathcal{R}'}{\longleftrightarrow}}$. □

The next lemma states that termination of $\mathcal{R}$ is preserved by applications of the inference rules of KB. It is the final result in this section whose proof refers to the inference rules.

Lemma 16. *If* $(\mathcal{E},\mathcal{R}) \vdash^*_{\mathsf{KB}} (\mathcal{E}',\mathcal{R}')$ *and* $\mathcal{R} \subseteq >$ *then* $\mathcal{R}' \subseteq >$.

Proof. We consider a single step $(\mathcal{E},\mathcal{R}) \vdash_{\mathsf{KB}} (\mathcal{E}',\mathcal{R}')$. The statement of the lemma follows by a straightforward induction proof. Observe that deduce, delete, and simplify do not change the set of rewrite rules and hence $\mathcal{R}' = \mathcal{R} \subseteq >$. For collapse we have $\mathcal{R}' \subsetneq \mathcal{R} \subseteq >$. In the case of orient we have $\mathcal{R}' = \mathcal{R} \cup \{s \to t\}$ with $s > t$ and hence $\mathcal{R}' \subseteq >$ follows from the assumption $\mathcal{R} \subseteq >$. Finally, consider an application of compose. So $\mathcal{R} = \mathcal{R}'' \uplus \{s \to t\}$ and $\mathcal{R}' = \mathcal{R}'' \cup \{s \to u\}$ with $t \to_{\mathcal{R}} u$. We obtain $s > t$ from the assumption $\mathcal{R} \subseteq >$. Since $>$ is a reduction order, $t > u$ follows from $t \to_{\mathcal{R}} u$. Transitivity of $>$ yields $s > u$ and hence $\mathcal{R}' \subseteq >$ as desired. □

To guarantee that the result of a finite KB derivation is a complete TRS equivalent to the initial $\mathcal{E}$, KB derivations must satisfy the fairness condition defined below. Fairness requires that prime critical pairs of the final TRS $\mathcal{R}_n$ which were not considered during the run are joinable in $\mathcal{R}_n$.

Definition 17. *A* run *for a given ES* $\mathcal{E}$ *is a finite sequence*

$$\mathcal{E}_0,\mathcal{R}_0 \;\vdash_{\mathsf{KB}}\; \mathcal{E}_1,\mathcal{R}_1 \;\vdash_{\mathsf{KB}}\; \cdots \;\vdash_{\mathsf{KB}}\; \mathcal{E}_n,\mathcal{R}_n$$

such that $\mathcal{E}_0 = \mathcal{E}$ *and* $\mathcal{R}_0 = \varnothing$. *The run* fails *if* $\mathcal{E}_n \neq \varnothing$. *The run is* fair *if*

$$\mathsf{PCP}(\mathcal{R}_n) \;\subseteq\; \downarrow_{\mathcal{R}_n} \cup \bigcup_{i=0}^{n} \leftrightarrow_{\mathcal{E}_i}$$

The reason for writing $\leftrightarrow_{\mathcal{E}_i}$ instead of $\mathcal{E}_i$ in the definition of fairness is that critical pairs are ordered, so in a fair run a (prime) critical pair $s \approx t$ of $\mathcal{R}_n$ may be ignored by deduce if $t \approx s$ was generated, or more generally, if $s \leftrightarrow_{\mathcal{E}_i} t$ holds at some point in the run. Non-prime critical pairs can always be ignored.

According to the main result of this section (Theorem 20), a completion procedure that produces fair runs is correct. The challenge is the confluence proof of $\mathcal{R}_n$. We show that $\mathcal{R}_n$ is peak decreasing by labeling rewrite steps (not only in $\mathcal{R}_n$) with multisets of terms. As well-founded order on these multisets we take the multiset extension of $>$.

Definition 18. *Let* $\to$ *be a rewrite relation and* M *a finite multiset of terms. We write* $s \xrightarrow{M} t$ *if* $s \to t$ *and there exist terms* $s', t' \in M$ *such that* $s' \geqslant s$ *and* $t' \geqslant t$. *Here* $\geqslant$ *denotes the reflexive closure of the given reduction order* $>$.

Lemma 19. *Let* $(\mathcal{E},\mathcal{R}) \vdash_{\mathsf{KB}} (\mathcal{E}',\mathcal{R}')$. *If* $s \overset{M}{\underset{\mathcal{E}\cup\mathcal{R}}{\longleftrightarrow}}{}^* t$ *and* $\mathcal{R}' \subseteq >$ *then* $s \overset{M}{\underset{\mathcal{E}'\cup\mathcal{R}'}{\longleftrightarrow}}{}^* t$.

Proof. We consider a single $(\mathcal{E} \cup \mathcal{R})$-step from s to t. The statement of the lemma follows then by induction on the length of the conversion between s and t. According to Lemma 14(1) there exist terms u and v such that

$$s \xrightarrow[\mathcal{R}']{=} u \xrightarrow[\mathcal{E}' \cup \mathcal{R}']{=} v \xleftarrow[\mathcal{R}']{=} t$$

We claim that the (non-empty) steps can be labeled by M. There exist terms $s', t' \in M$ with $s' \geqslant s$ and $t' \geqslant t$. Since $\mathcal{R}' \subseteq >$, $s \geqslant u$ and $t \geqslant v$ and thus also $s' \geqslant u$ and $t' \geqslant v$. Hence

$$s \xrightarrow[\mathcal{R}']{M} = u \xrightarrow[\mathcal{E}' \cup \mathcal{R}']{M} = v = \xleftarrow[\mathcal{R}']{M} t$$

and thus also $s \xleftrightarrow[\mathcal{E}' \cup \mathcal{R}']{M}{}^* t$. □

After these preliminaries we are ready for the main result of this section. A TRS $\mathcal{R}$ is called a *representation* of an ES $\mathcal{E}$ if $\leftrightarrow^*_{\mathcal{R}}$ and $\leftrightarrow^*_{\mathcal{E}}$ coincide.

Theorem 20. *For every fair non-failing run γ*

$$\mathcal{E}_0, \mathcal{R}_0 \vdash_{\mathsf{KB}} \mathcal{E}_1, \mathcal{R}_1 \vdash_{\mathsf{KB}} \cdots \vdash_{\mathsf{KB}} \mathcal{E}_n, \mathcal{R}_n$$

the TRS $\mathcal{R}_n$ is a complete representation of $\mathcal{E}$.

Proof. We have $\mathcal{E}_n = \varnothing$. From Corollary 15 we know that $\leftrightarrow^*_{\mathcal{E}} = \leftrightarrow^*_{\mathcal{R}_n}$. Lemma 16 yields $\mathcal{R}_n \subseteq >$ and hence $\mathcal{R}_n$ is terminating. It remains to prove that $\mathcal{R}_n$ is confluent. Let

$$t \xleftarrow[\mathcal{R}_n]{M_1} s \xrightarrow[\mathcal{R}_n]{M_2} u$$

From Lemma 10 we obtain $t \mathrel{\nabla_s^2} u$. Let $v \mathrel{\nabla_s} w$ appear in this sequence (so $t = v$ or $w = u$). We obtain

$$(v, w) \in {\downarrow_{\mathcal{R}_n}} \cup \bigcup_{i=0}^{n} {\leftrightarrow_{\mathcal{E}_i}}$$

from the definition of ∇_s and fairness of γ. We label all steps between v and w with the multiset $\{v, w\}$. Because $s > v$ and $s > w$ we have $M_1 >_{\mathsf{mul}} \{v, w\}$ and $M_2 >_{\mathsf{mul}} \{v, w\}$. Hence by repeated applications of Lemma 19 we obtain a conversion in $\mathcal{R}_n$ between v and w in which each step is labeled with a multiset that is smaller than both M_1 and M_2. It follows that $\mathcal{R}_n$ is peak decreasing. □

A completion procedure is a program that generates KB runs. In order to ensure that the final outcome $\mathcal{R}_n$ is a complete representation of the initial ES, fair runs should be produced. Fairness requires that prime critical pairs of $\mathcal{R}_n$ are considered during the run. Of course, $\mathcal{R}_n$ is not known during the run, so to be on the safe side, prime critical pairs of any $\mathcal{R}$ that appears during the run should be generated by deduce. (If a critical pair is generated from a rewrite rule that disappears at a later stage, it can be safely deleted from the run.) In particular, there is no need to deduce equations that are not prime critical pairs. So we may strengthen the condition $s \mathrel{\mathcal{R}\!\leftarrow} \cdot \rightarrow_{\mathcal{R}} t$ of deduce to $s \approx t \in \mathsf{PCP}(\mathcal{R})$ without affecting Theorem 20.

7 Related Work

Formalizations of the Critical Pair Lemma. There is previous work on formalizing the Critical Pair Lemma. The first such formalization that we are aware of is by Ruiz-Reina *et al.* in ACL2 [15]. Details of the formalization are not presented in the paper, however, the authors state the following:

> *The main proof effort was done to handle noncritical (or variable) overlaps. It is interesting to point out that in most textbooks and surveys this case is proved pictorially. Nevertheless, in our mechanical proof [it] turns out to be the most difficult part and it even requires the design of an induction scheme not discovered by the heuristics of the prover.*

In contrast our proof of Lemma 6 handles the variable overlap case rigorously but still without excessive complexity (also in the formalization).

Another formalization of the Critical Pair Lemma was conducted by Galdino and Ayala-Rincón in PVS [7]. Here renamings are handled as substitutions satisfying further restrictions. While this was also our first approach in our own formalization, it leads to rather cumbersome proof obligations where basically the same kind of proofs have to be done for every object that we want to permute, i.e., terms, rules, substitutions, TRSs, etc. Most of those obligations can be handled in the abstract setting of permutation types once and for all and thus freely carry over to any concrete instance. Moreover the obtained set of critical pairs is infinite but there is no formalized proof that it suffices to look at only finitely many representatives for finite TRSs.

The latest formalization of the Critical Pair Lemma we are aware of is by Sternagel and Thiemann in Isabelle/HOL [16]. It consists of a rather involved proof. Moreover, it is restricted to *string*s and relies on concrete renaming functions. Thus it is not so convenient to use in an abstract setting. A big advantage, however, is that this formalization is executable and the obtained set of critical pairs is finite (for finite TRSs) by construction. The good news is that it should be possible to prove the soundness of the same executable function also via our abstract formalization, which would combine the advantages of executability and an abstract theory.

Soundness of Completion. Bachmair *et al.* [4] consider an infinite fair run to characterize the output system as the pair $(\mathcal{E}_\infty, \mathcal{R}_\infty)$ of the *persistent sets*:

$$\mathcal{E}_\infty = \bigcup_{i \geqslant 0} \bigcap_{j \geqslant i} \mathcal{E}_i \qquad\qquad \mathcal{R}_\infty = \bigcup_{i \geqslant 0} \bigcap_{j \geqslant i} \mathcal{R}_i$$

When proving confluence of $\mathcal{R}_\infty$, conversions $s_1 \leftrightarrow \cdots \leftrightarrow s_n$ in $\mathcal{E}_\infty \cup \mathcal{R}_\infty$ are compared by comparing the corresponding multisets $\{\mathsf{cost}(s_i, s_{i+1}) \mid i < n\}$ using the *proof order* given by $\big((>_{\mathsf{mul}}, \rhd, >)_{\mathsf{lex}}\big)_{\mathsf{mul}}$. Here the function cost is defined as

$$\mathsf{cost}(s,t) = \begin{cases} (\{s,t\}, -, -) & \text{if } s \leftrightarrow_{\mathcal{E}_\infty} t \\ (\{s\}, \ell, t) & \text{if } s \to_{\mathcal{R}_\infty} t \\ (\{t\}, \ell, s) & \text{if } t \to_{\mathcal{R}_\infty} s \end{cases}$$

Table 1. Comparison between existing Isabelle/HOL formalizations

	∼ LoI new	∼ LoI [16]
renaming (+ interpretations)	2000	–
peak decreasingness	400	–
critical peak/pair lemma	300	300
soundness of completion	600	1600
longest proof	80	900
soundness with PCPs	120	–

where – is an arbitrary fixed element. Whenever a conversion contains a local peak, one can find a conversion that is smaller in the proof order. In this way confluence is obtained.

Sternagel and Thiemann [16] observed that the encompassment restriction in the collapse inference rule is unnecessary for finite runs. Based on this observation they simplified the cost function (for runs of length n) to

$$\mathsf{cost}(s,t) = \begin{cases} (\{s,t\}, -) & \text{if } s \leftrightarrow_{\mathcal{E}_\infty} t \\ (\{s\}, n - o(\ell \to r)) & \text{if } s \to_{\ell \to r} t \text{ and } \ell \to r \in \mathcal{R}_\infty \\ (\{t\}, n - o(\ell \to r)) & \text{if } t \to_{\ell \to r} s \text{ and } \ell \to r \in \mathcal{R}_\infty \end{cases}$$

where $o(\ell \to r)$ denotes the highest $i \leqslant n$ such that $\ell \to r \in \mathcal{R}_i$. The proof order is $\big((>_{\mathsf{mul}}, >_{\mathbb{N}})_{\mathsf{lex}}\big)_{\mathsf{mul}}$. In our new proof the second ingredient of the cost is replaced by mathematical induction in Lemma 19, and the proof order is hidden behind the abstract notion of peak decreasingness.

For a more detailed comparison between our current formalization and the one of Sternagel and Thiemann consult Table 1, where we compare *Lines of Isabelle code* (LoI for short). A general theory of renamings (plus special instances for terms, rules, TRSs, etc.) is a big part of our formalization and not present in the previous formalization at all. However this theory should be useful in future proofs. Moreover, its absence restricts the previous work to strings as variables. Peak decreasingness is also exclusive to our formalization. Concerning the critical pair lemma, both formalizations are approximately the same size, but note that our formalization is concerned with critical peaks instead of critical pairs (which is more general and actually needed in later proofs). As for soundness of abstract completion, our new formalization is drastically shorter (both columns include all definitions and intermediate lemmas that are needed for the final soundness result). Another interesting observation might be that in our new formalization of soundness the longest proof (confluence of the final TRS via peak decreasingness) is a mere 80 LoI, whereas the longest proof in the previous formalization is more than 900 LoI long (and concerned with the fact that applying an inference rule strictly decreases the cost). Finally, on top of the previous result the soundness of completion via prime critical pairs is an easy extension.

In the literature (e.g. [2,3]) critical pair criteria (like primality) are formulated as fairness conditions for completion, and correctness proofs are a combination of proof orders and a confluence criterion known as *connected-below* due to Winkler and Buchberger [19]. Our new approach avoids this detour.

8 Conclusion

In this paper we presented a new and formalized correctness proof of abstract completion which is significantly simpler than the existing proofs in the literature. Unlike earlier formalizations of the critical pair lemma and abstract completion, our formalization follows the paper proof included in this paper. This was made possible by extending IsaFoR with an abstract framework for handling variable renamings inspired by and based on a previous formalization for Nominal Isabelle.

Furthermore, our formalization of completion is the first that incorporates critical pair criteria. The key to the simple proof is the notion of peak decreasingness, a very mild version of the decreasing diagrams technique for proving confluence in the absence of termination.

There are several important variations of completion. We anticipate that the presented approach can be adapted for them, in particular ordered completion [5].

Acknowledgments. We want to give special thanks to the team around Sledgehammer and Nitpick [6] two indispensable Isabelle tools, the former increasing productivity while proving by a factor of magnitude, and the latter often pointing out slightly wrong statements that could cost hours, if not days, of a formalization attempt.

References

1. F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.
2. L. Bachmair. *Canonical Equational Proofs*. Birkhäuser, 1991.
3. L. Bachmair and N. Dershowitz. Equational inference, canonical proofs, and proof orderings. *Journal of the ACM*, 41(2):236–276, 1994. doi:10.1145/174652.174655.
4. L. Bachmair, N. Dershowitz, and J. Hsiang. Orderings for equational proofs. In *Proc. 1st IEEE Symposium on Logic in Computer Science*, pages 346–357, 1986.
5. L. Bachmair, N. Dershowitz, and D. A. Plaisted. *Resolution of Equations in Algebraic Structures: Completion without Failure*, volume 2, pages 1–30. Academic Press, 1989.
6. J.C. Blanchette, L. Bulwahn, and T. Nipkow. Automatic proof and disproof in Isabelle/HOL. In *Proc. 8th International Symposium on Frontiers of Combining Systems*, volume 6989 of *Lecture Notes in Computer Science*, pages 12–27, 2011. doi:10.1007/978-3-642-24364-6_2.
7. A.L. Galdino and M. Ayala-Rincón. A formalization of the Knuth-Bendix(-Huet) critical pair theorem. *Journal of Automated Reasoning*, 45(3):301–325, 2010. doi:10.1007/s10817-010-9165-2.

8. G. Huet. A complete proof of correctness of the Knuth-Bendix completion algorithm. *Journal of Computer and System Sciences*, 23(1):11–21, 1981. doi:10.1016/0022-0000(81)90002-7.
9. B. Huffman and C. Urban. A new foundation for Nominal Isabelle. In M. Kaufmann and L.C. Paulson, editors, *Proc. 1st International Conference on Interactive Theorem Proving*, volume 6172 of *Lecture Notes in Computer Science*, pages 35–50. Springer, 2010. doi:10.1007/978-3-642-14052-5_5.
10. D. Kapur, D.R. Musser, and P. 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.
11. D.E. Knuth and P. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. 1970.
12. T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer, 2002. doi:10.1007/3-540-45949-9.
13. V. van Oostrom. Confluence by decreasing diagrams. *Theoretical Computer Science*, 126(2):259–280, 1994. doi:10.1016/0304-3975(92)00023-K.
14. F. van Raamsdonk, editor. *Proc. 24th International Conference on Rewriting Techniques and Applications*, volume 21 of *Leibniz International Proceedings in Informatics*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2013.
15. J.-L. Ruiz-Reina, J.-A. Alonso, M.-J. Hidalgo, and F.-J. Martín-Mateos. Formal proofs about rewriting using ACL2. *Annals of Mathematics and Artificial Intelligence*, 36(3):239–262, 2002. doi:10.1023/A:1016003314081.
16. C. Sternagel and R. Thiemann. Formalizing Knuth-Bendix orders and Knuth-Bendix completion. In van Raamsdonk [14], pages 287–302. doi:10.4230/LIPIcs.RTA.2013.287.
17. Terese. *Term Rewriting Systems*, volume 55 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2003.
18. C. Urban and C. Kaliszyk. General bindings and alpha-equivalence in Nominal Isabelle. *Logical Methods in Computer Science*, 8(2):465–476, 2012. doi:10.2168/LMCS-8(2:14)2012.
19. F. Winkler and B. Buchberger. A criterion for eliminating unnecessary reductions in the Knuth-Bendix algorithm. In *Proc. Colloquium on Algebra, Combinatorics and Logic in Computer Science, Vol. II*, volume 42 of *Colloquia Mathematica Societatis J. Bolyai*, pages 849–869, 1986.
20. H. Zankl. Decreasing diagrams – formalized. In van Raamsdonk [14], pages 352–367. doi:10.4230/LIPIcs.RTA.2013352.