Formalized Ground Completion*

Aart Middeldorp and Christian Sternagel

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

Abstract

Completion is the process of turning a set of equations into an equivalent confluent and terminating set of rewrite rules. It is known that completion will always succeed if the input equations are ground and the employed reduction order is total on (equivalent) ground terms. Moreover, every reduced ground rewrite system can be obtained by completion from any equivalent set of ground equations. We present the first formalized correctness proofs of these results.

1 Introduction

We assume familiarity with term rewriting [1] but recall the inference rules of abstract completion.

Definition 1. *The inference system KB of abstract (Knuth-Bendix) completion operates on pairs $\mathcal{E}, \mathcal{R}$ of equations $\mathcal{E}$ and rules $\mathcal{R}$. It consists of the following inference rules:*

deduce	$\dfrac{\mathcal{E}, \mathcal{R}}{\mathcal{E} \cup \{s \approx t\}, \mathcal{R}}$	*if* $s \mathrel{{}_{\mathcal{R}}\!\leftarrow} \cdot \rightarrow_{\mathcal{R}} t$	*compose*	$\dfrac{\mathcal{E}, \mathcal{R} \uplus \{s \to t\}}{\mathcal{E}, \mathcal{R} \cup \{s \to u\}}$	*if* $t \rightarrow_{\mathcal{R}} u$
orient	$\dfrac{\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}}{\mathcal{E}, \mathcal{R} \cup \{s \to t\}}$	*if* $s > t$	*simplify*	$\dfrac{\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}}{\mathcal{E} \cup \{u \approx t\}, \mathcal{R}}$	*if* $s \rightarrow_{\mathcal{R}} u$
	$\dfrac{\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}}{\mathcal{E}, \mathcal{R} \cup \{t \to s\}}$	*if* $t > s$		$\dfrac{\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}}{\mathcal{E} \cup \{s \approx u\}, \mathcal{R}}$	*if* $t \rightarrow_{\mathcal{R}} u$
delete	$\dfrac{\mathcal{E} \uplus \{s \approx s\}, \mathcal{R}}{\mathcal{E}, \mathcal{R}}$		*collapse*	$\dfrac{\mathcal{E}, \mathcal{R} \uplus \{t \to s\}}{\mathcal{E} \cup \{u \approx s\}, \mathcal{R}}$	*if* $t \rightarrow_{\mathcal{R}} u$

Here $>$ is an arbitrary but fixed reduction order. The inference system KB^- consists of the inference rules of KB except for deduce.

Snyder [8] proved that ground sets of equations (also called equational systems or ESs for short) can always be completed by KB^-. In the next section we present a proof of this result that we formalized in Isabelle/HOL [5]. Snyder further proved that every reduced ground rewrite system is canonical and can be obtained by completion from any equivalent set of ground equations, our formalization of which is the topic of Section 3.

Our formalization is part of IsaFoR [9][1] version 2.31 where it is located in the file `thys/Abstract_Completion/Ground_Completion.thy`. Furthermore all definitions, theorems, and lemmas in the PDF version of this manuscript are active hyperlinks to a (human readable) HTML presentation of our formalization.

We conclude this introduction with an example illustrating the inference system KB^- on a set of ground equations.

*This work is supported by the Austrian Science Fund (FWF): projects P27502 and P27528.

[1] `http://cl-informatik.uibk.ac.at/isafor`

Example 1. *Consider the ES $\mathcal{E}$ consisting of the ground equations*

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

As reduction order we take LPO induced by the total precedence $\mathsf{a} > \mathsf{b} > \mathsf{c} > \mathsf{f}$. We start by applying orient *to the last two equations:*

$$\mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{a}))) \approx \mathsf{f}(\mathsf{b}) \qquad \mathsf{f}(\mathsf{f}(\mathsf{b})) \approx \mathsf{c} \qquad \mathsf{f}(\mathsf{c}) \leftarrow \mathsf{a} \qquad \mathsf{f}(\mathsf{a}) \rightarrow \mathsf{f}(\mathsf{f}(\mathsf{b}))$$

An application of collapse *produces*

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

Next we orient the second equation:

$$\mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{a}))) \approx \mathsf{f}(\mathsf{b}) \qquad \mathsf{f}(\mathsf{f}(\mathsf{b})) \rightarrow \mathsf{c} \qquad \mathsf{f}(\mathsf{c}) \leftarrow \mathsf{a} \qquad \mathsf{f}(\mathsf{f}(\mathsf{c})) \approx \mathsf{f}(\mathsf{f}(\mathsf{b}))$$

Two applications of simplify *produce*

$$\mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{c}))) \approx \mathsf{f}(\mathsf{b}) \qquad \mathsf{f}(\mathsf{f}(\mathsf{b})) \rightarrow \mathsf{c} \qquad \mathsf{f}(\mathsf{c}) \leftarrow \mathsf{a} \qquad \mathsf{f}(\mathsf{f}(\mathsf{c})) \approx \mathsf{c}$$

We continue by orienting the last equation:

$$\mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{c}))) \approx \mathsf{f}(\mathsf{b}) \qquad \mathsf{f}(\mathsf{f}(\mathsf{b})) \rightarrow \mathsf{c} \qquad \mathsf{f}(\mathsf{c}) \leftarrow \mathsf{a} \qquad \mathsf{f}(\mathsf{f}(\mathsf{c})) \rightarrow \mathsf{c}$$

Two applications of simplify *produce*

$$\mathsf{c} \approx \mathsf{f}(\mathsf{b}) \qquad \mathsf{f}(\mathsf{f}(\mathsf{b})) \rightarrow \mathsf{c} \qquad \mathsf{f}(\mathsf{c}) \leftarrow \mathsf{a} \qquad \mathsf{f}(\mathsf{f}(\mathsf{c})) \rightarrow \mathsf{c}$$

Orienting the remaining equation followed by a collapse step produces

$$\mathsf{c} \leftarrow \mathsf{f}(\mathsf{b}) \qquad \mathsf{f}(\mathsf{c}) \approx \mathsf{c} \qquad \mathsf{f}(\mathsf{c}) \leftarrow \mathsf{a} \qquad \mathsf{f}(\mathsf{f}(\mathsf{c})) \rightarrow \mathsf{c}$$

Finally, we orient the only remaining equation and collapse*,* compose*,* simplify*, and* delete *exhaustively, thereby obtaining the TRS $\mathcal{R}$*

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

which constitutes a canonical presentation of $\mathcal{E}$.

2 Correctness

The absence of deduce from KB^- does not hurt for ground systems. If $s \leftarrow \cdot \rightarrow t$ and the two contracted redexes are at parallel positions then trivially $s \rightarrow \cdot \leftarrow t$. If the steps are identical then $s = t$. In the remaining case one of the contracted redexes is a subterm of the other contracted redex, and the effect of deduce is achieved by the collapse inference rule.

On the contrary, the absence of deduce is crucial to conclude that KB^- derivations are always finite.

Lemma 1. *There are no infinite sequences $\mathcal{E}_0, \varnothing \vdash_{\mathsf{KB}^-} \mathcal{E}_1, \mathcal{R}_1 \vdash_{\mathsf{KB}^-} \cdots$ for finite ground ESs $\mathcal{E}_0$.*

Proof. Let $\succ$ denote the lexicographic combination of the multiset extension $>_{\mathsf{mul}}$ of the reduction order $>$ with the standard order on natural numbers $>_{\mathbb{N}}$. Furthermore let $M(\mathcal{E},\mathcal{R})$ denote the (finite) multiset of left-hand sides and right-hand sides occurring in $\mathcal{E}$ and $\mathcal{R}$

$$M(\mathcal{E},\mathcal{R}) = \bigcup\{\{s,t\} \mid (s,t) \in \mathcal{E}\} \cup \bigcup\{\{s,t\} \mid (s,t) \in \mathcal{R}\}$$

and consider the function P that maps the pair $(\mathcal{E},\mathcal{R})$ to $(M(\mathcal{E},\mathcal{R}), |\mathcal{E}|)$. Now it is straightforward to verify that any infinite $\vdash_{\mathsf{KB}^-}$-sequence would give rise to an infinite sequence $P(\mathcal{E}_0,\varnothing) \succ P(\mathcal{E}_1,\mathcal{R}_1) \succ \cdots$, contradicting the well-foundedness of $\succ$. □

The formalization of the following preliminary result is covered by previous work [2].

Lemma 2. *If* $(\mathcal{E},\mathcal{R}) \vdash^*_{\mathsf{KB}} (\mathcal{E}',\mathcal{R}')$ *then* $\xleftrightarrow[\mathcal{E}\cup\mathcal{R}]{*} = \xleftrightarrow[\mathcal{E}'\cup\mathcal{R}']{*}$. □

Theorem 1. *If* $>$ *is total on* $\mathcal{E}$*-equivalent ground terms then every maximal* KB^- *run produces an equivalent canonical presentation for ground ES* $\mathcal{E}$*.*

Proof. Consider a maximal KB^- run $\mathcal{E}_0,\varnothing \vdash \mathcal{E}_1,\mathcal{R}_1 \vdash \cdots \vdash \mathcal{E}_n,\mathcal{R}_n$ where $\mathcal{E}_0 = \mathcal{E}$ is a ground ES. Because the run is maximal, no inference rule of KB^- is applicable to the final pair $(\mathcal{E}_n,\mathcal{R}_n)$. In particular, compose and collapse are not applicable and hence the final TRS $\mathcal{R}_n$ is reduced. Since $\mathcal{R}_n$ is also ground, it is canonical. From Lemma 2 and the inclusion $\mathsf{KB}^- \subseteq \mathsf{KB}$ we infer that $\mathcal{E}$ and $\mathcal{E}_n \cup \mathcal{R}_n$ are equivalent. It follows that $>$ is total on $\mathcal{E}_n$-equivalent ground terms and thus $\mathcal{E}_n = \varnothing$, for otherwise the run could be extended with an application of delete or simplify. Hence $\mathcal{R}_n$ and $\mathcal{E}$ are equivalent. □

The restriction on the reduction order $>$ in the above correctness theorem is easy to satisfy. In particular, it holds for any LPO or KBO based on a total precedence.

3 Completeness

The final result of this note states the completeness of ground completion. The proof makes use of the following preliminary results. The formalization of the first one is detailed in previous work [3].

Theorem 2 (Métivier [4])**.** *Let* $\mathcal{R}$ *and* $\mathcal{S}$ *be equivalent canonical TRSs. If* $\mathcal{R}$ *and* $\mathcal{S}$ *are compatible with the same reduction order then* $\mathcal{R} \doteq \mathcal{S}$*.* □

Here $\mathcal{R} \doteq \mathcal{S}$ denotes that $\mathcal{R}$ and $\mathcal{S}$ are identical modulo renaming of variables (that is, each rule of $\mathcal{R}$ has a variant in $\mathcal{S}$ and vice versa). The next concept is useful in the analysis of rewrite strategies [7]. It generalizes a number of earlier concepts, including the property $\leftarrow \cdot \rightarrow \subseteq \rightarrow \cdot \leftarrow \cup =$ which is known as WCR^1 and true for left-reduced ground TRSs.

Definition 2. *A TRS* $\mathcal{R}$ *has* random descent *if for every conversion* $a \leftrightarrow^* b$ *with normal form* b *we have* $a \rightarrow^n b$ *with* $n + l = r$*. Here* l *(*r*) denotes the number of* $\leftarrow$ *(*$\rightarrow$*) steps in the conversion* $a \leftrightarrow^* b$*.*

Theorem 3 (van Oostrom [6])**.** *Let* $\mathcal{R}$ *be a TRS with random descent. If* $a \leftrightarrow^* b$ *with normal form* b *then* a *is complete and all rewrite sequences from* a *to* b *have the same length.*

The short and direct proof given below has been formalized.

Proof. Let l (r) be the number of $\leftarrow$ ($\rightarrow$) steps in the conversion from a to b. We have $l \leqslant r$ since $n + l = r$ for some n by random descent. First we prove termination of a. For a proof by contradiction, suppose the existence of an infinite rewrite sequence

$$a = a_0 \rightarrow a_1 \rightarrow a_2 \rightarrow \cdots$$

Clearly, $a \rightarrow^{r-l} a_{r-l}$ and thus there exists a conversion $a_{r-l} \,{}^*\!\leftarrow a \leftrightarrow^* b$ with r backwards and r forwards steps. Hence $a_{r-l} = b$ by another application of random descent and therefore $b \rightarrow a_{r-l+1}$, contradicting the fact that b is a normal form. Next we prove confluence of a. Suppose $c \,{}^*\!\leftarrow a \rightarrow^* d$. We obtain the two conversions $c \leftrightarrow^* b$ and $d \leftrightarrow^* b$, which are transformed into $c \downarrow d$ by two applications of random descent. Finally, assume there are two rewrite sequences $a \rightarrow^m b$ and $a \rightarrow^n b$ from a to b of length m and n. Reversing the first sequence and appending the second one yields a conversion $b \leftrightarrow^* b$ with m backwards and n forwards steps. A final application of random descent yields $b \rightarrow^k b$ for some k with $k + m = n$. Since b is a normal form, $k = 0$ and thus $m = n$ as desired. □

Lemma 3. *Reduced ground TRSs are canonical and have random descent.*

Proof. First we show that every left-reduced ground TRS $\mathcal{R}$ has random descent. To this end let $s \leftrightarrow^* t$ be a conversion between s and the normal form t. Now we proceed by induction on the length of the conversion. If it is empty or the first step is to the right, we are done. Otherwise, we have $s \leftarrow u \leftrightarrow^* t$ where the conversion has l (r) left-steps (right-steps) and obtain $u \rightarrow^k t$ with $k + l = r$ by the induction hypothesis. The remainder of the proof proceeds by induction on k together with the observation that left-reduced ground TRSs enjoy the WCR^1 property.

Moreover, every right-reduced ground TRS $\mathcal{R}$ is terminating. For assuming non-termination there would be a minimal non-terminating term t. This means that after a finite number of non-root steps $t \rightarrow^* u$ there will be a root-step $u \rightarrow v$ such that v is non-terminating. But since $\mathcal{R}$ is right-reduced and ground, v is a ground normal form.

Since all terms are terminating, confluence of $\mathcal{R}$ is an immediate consequence of the definition of random descent. □

Theorem 4. *For every ground ES $\mathcal{E}$ and every equivalent reduced ground TRS $\mathcal{R}$ there exist a reduction order $>$ and a derivation $\mathcal{E}, \varnothing \vdash_{\mathsf{KB}^-} \cdots \vdash_{\mathsf{KB}^-} \varnothing, \mathcal{R}$.*

Proof. Let $>$ be a reduction order that contains $\mathcal{R}$ and is total on $\mathcal{E}$-equivalent ground terms. Consider a maximal KB^- run starting from $\mathcal{E}$ and using $>$. According to Theorem 1, the run produces an equivalent reduced TRS $\mathcal{R}'$. Since $\mathcal{R} \subseteq >$ and $\mathcal{R}' \subseteq >$, we obtain $\mathcal{R} = \mathcal{R}'$ from Theorem 2. It remains to show that $>$ exists. Let $\sqsupset$ be a total precedence and define $s > t$ if and only if $s \leftrightarrow^*_{\mathcal{E}} t$ and either $d_{\mathcal{R}}(s) > d_{\mathcal{R}}(t)$ or both $d_{\mathcal{R}}(s) = d_{\mathcal{R}}(t)$ and $s \sqsupset_{\mathsf{lpo}} t$.[2] Here $d_{\mathcal{R}}(u)$ is the number of rewrite steps in $\mathcal{R}$ to normalize the term u, which is well-defined since all normalizing sequences in a reduced ground TRS have the same length as a consequence of Lemma 3 and Theorem 3. It is easy to show that $>$ has the required properties. The only interesting cases are closure under contexts and substitutions. Both are basically handled by the following observation: $d_{\mathcal{R}}(C[t\sigma]) = d_{\mathcal{R}}(C[t{\downarrow}\sigma]) + d_{\mathcal{R}}(t)$ for any term t (which holds due to random descent together with termination). This allows us to lift $d_{\mathcal{R}}(s) = d_{\mathcal{R}}(t)$ and $d_{\mathcal{R}}(s) > d_{\mathcal{R}}(t)$ into arbitrary contexts and substitutions. □

The above result cannot be generalized to left-linear right-ground systems, as shown in the following example due to Dominik Klein (personal communication).

[2] In the formalization we actually use $\sqsupset_{\mathsf{kbo}}$ with all weights set to 1, since in contrast to LPO, for KBO ground-totality for total precedences has already been formalized before.

Example 2. *Consider the ES $\mathcal{E}$ consisting of the two equations $\mathsf{f}(x) \approx \mathsf{f}(\mathsf{a})$ and $\mathsf{f}(\mathsf{b}) \approx \mathsf{b}$. Let $>$ be a reduction order. If $\mathsf{f}(\mathsf{b}) > \mathsf{b}$ does not hold, no inference rule of KB is applicable to $(\mathcal{E}, \varnothing)$. If $\mathsf{f}(\mathsf{b}) > \mathsf{b}$ then the second equation can be oriented*

$$(\mathcal{E}, \varnothing) \vdash (\{\mathsf{f}(x) \approx \mathsf{f}(\mathsf{a})\}, \{\mathsf{f}(\mathsf{b}) \to \mathsf{b}\})$$

At this point trivial equations of the shape $\mathsf{f}^n(\mathsf{b}) \approx \mathsf{f}^n(\mathsf{b})$ with $n \geqslant 0$ can be deduced and subsequently deleted. No other possibilities exist and hence completion will fail on $\mathcal{E}$. Nevertheless, the TRS $\mathcal{R}$ consisting of the rewrite rule $\mathsf{f}(x) \to \mathsf{b}$ constitutes a canonical presentation of $\mathcal{E}$.

References

[1] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[2] N. Hirokawa, A. Middeldorp, and C. Sternagel. A new and formalized proof of abstract completion. In *Proc. 5th International Conference on Interactive Theorem Proving*, volume 8558 of *Lecture Notes in Computer Science*, pages 292–307, 2014. doi: 10.1007/978-3-319-08970-6_19.

[3] N. Hirokawa, A. Middeldorp, C. Sternagel, and S. Winkler. Infinite runs in abstract completion. In *Proc. 2nd International Conference on Formal Structures for Computation and Deduction*, volume 84 of *Leibniz International Proceedings in Informatics*, pages 19:1–19:16, 2017. To appear.

[4] Y. Métivier. About the rewriting systems produced by the Knuth-Bendix completion algorithm. *Information Processing Letters*, 16(1):31–34, 1983. doi: 10.1016/0020-0190(83)90009-1.

[5] 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.

[6] V. van Oostrom. Random descent. In *Proc. 18th International Conference on Rewriting Techniques and Applications*, volume 4533 of *Lecture Notes in Computer Science*, pages 314–328, 2007. doi: 10.1007/978-3-540-73449-9_24.

[7] V. van Oostrom and Y. Toyama. Normalisation by random descent. In *Proc. 1st International Conference on Formal Structures for Computation and Deduction*, volume 52 of *Leibniz International Proceedings in Informatics*, pages 32:1–32:18, 2016. doi: 10.4230/LIPIcs.FSCD.2016.32.

[8] W. Snyder. A fast algorithm for generating reduced ground rewriting systems from a set of ground equations. *Journal of Symbolic Computation*, 15(4):415–450, 1993. doi: 10.1006/jsco.1993.1029.

[9] R. Thiemann and C. Sternagel. Certification of termination proofs using CeTA. In *Proc. 22nd International Conference on Theorem Proving in Higher Order Logics*, volume 5674 of *Lecture Notes in Computer Science*, pages 452–468, 2009. doi: 10.1007/978-3-642-03359-9_31.