Formalizing Soundness and Completeness of Unravelings*

Sarah Winkler and René Thiemann

Institute of Computer Science, University of Innsbruck, 6020 Innsbruck, Austria
{sarah.winkler, rene.thiemann}@uibk.ac.at

Abstract. Unravelings constitute a class of program transformations to model conditional rewrite systems as standard term rewrite systems. Key properties of unravelings are soundness and completeness with respect to reductions, in the sense that rewrite sequences in the unraveled system correspond to rewrite sequences in the conditional system and vice versa. While the latter is easily satisfied, the former holds only under certain conditions and is notoriously difficult to prove. This paper describes an Isabelle formalization of both properties. The soundness proof is based on the approach by Nishida, Sakai, and Sakabe (2012) but we also contribute to the theory by showing it applicable to a larger class of unravelings. Based on our formalization we developed the first certifier to check output of conditional rewrite tools. In particular, quasi-decreasingness proofs by AProVE and conditional confluence proofs by ConCon can be certified.

1 Introduction

Conditional term rewriting is a natural extension of standard rewriting in that it allows to specify conditions for rules to be applied. This is useful in many applications, for instance to reason about logic programs [14, 16]. However, the addition of conditions severely complicates the analysis of various properties. This led to the development of transformations that convert conditional rewrite systems (CTRSs) into standard rewrite systems (TRSs). Provided certain requirements are fulfilled, one can then employ criteria for standard rewrite systems to infer e.g. termination and confluence of the conditional system. Unravelings are the most widely considered class of such transformations [2, 7, 11, 14].

Tools to analyze CTRSs often exploit unravelings. For example, the conditional confluence tool ConCon [17] may unravel a given CTRS R into a TRS R'. It then invokes a confluence tool for TRSs to get a confluence proof P for R', in order to eventually conclude confluence of R. Similarly, AProVE [3] generates operational termination proofs for CTRSs by first applying an unraveling and then trying to prove termination of the resulting TRSs.

Like all tools for program analysis, rewrite tools are inherently complex and error-prone. In the following we describe our IsaFoR/CeTA [18]-based certifica-

* This research was supported by the Austrian Science Fund (FWF) projects I963 and Y757.

tion approach to validate confluence and termination proofs for CTRSs, which combines three different systems: an analyzer, a certifier, and a proof assistant.

1. A proof certificate is generated by an automatic analysis tool like AProVE or CorCon. The certificate consists of a CTRS R, an unraveled TRS R', and the termination (or confluence) proof P.
2. Our certifier CeTA can then be invoked on (R, R', P) to validate the certificate. To this end, CeTA first checks that $R' = U(R)$ for some unraveling U. Next, it verifies that P is a valid termination (or confluence) proof for R', for which it has a variety of techniques at its disposal [9, 18]. Finally, it checks whether U satisfies certain syntactic criteria which ensure that termination (or confluence) of R' also implies termination (or confluence) of R.
3. Soundness of CeTA is guaranteed as it is based on the Isabelle [10] framework IsaFoR (Isabelle Formalization of Rewriting). To that end we formalized[1] two properties in IsaFoR: (a) if U satisfies the syntactic requirements then termination (or confluence) of R' implies termination (or confluence) of R; and (b) CeTA, a functional program written within Isabelle, is sound.

To the best of our knowledge, our contribution constitutes the first work on certified program verification for conditional rewriting. This paper describes the formalization done for task (3), giving rise to a certifier for task (2). Here the vast amount of effort goes into part (3a), after which (3b) can be achieved by applying Isabelle's code generator.

In the remainder of this paper we thus focus on (3a), primarily on formalizing two properties of an unraveling U which are of crucial importance: (i) every rewrite sequence admitted by the transformed TRS $U(R)$ (among terms over the original signature) should be possible with the CTRS R, and (ii) every rewrite sequence allowed by R should be preserved in $U(R)$. These properties are known as soundness and completeness with respect to reductions. While completeness imposes only mild restrictions on such a transformation, soundness is much harder to satisfy, and the respective proofs in the literature are involved and technical.

The remainder of this paper is structured as follows. We first recall some background on TRSs and CTRSs in § 2. In § 3 we describe our formalization of basic results on conditional rewriting, before we introduce unravelings in § 4. The formalization of completeness results of unravelings in combination with the certifier for termination proofs for CTRSs is the topic of § 5. In § 6 we describe the formalized soundness proof, covering a large class of unravelings. Building upon these results, in § 7 we outline a result connecting confluence of the unraveled system with confluence of the original system. Finally, in § 8 we conclude and shortly mention the experimental results.

The full formalization and the certifier (IsaFoR and CeTA) as well as details on the experiments are available on the following website:

`http://cl-informatik.uibk.ac.at/software/ceta/experiments/unravelings/`

For each lemma, theorem, and definition in this paper, the website also contains a link to our Isabelle formulation (and proof) of that lemma, etc.

[1] Here, the notion *formalized* always refers to a machine checked proof in Isabelle.

2 Preliminaries

We refer to [1] for the basics on term rewriting. In the sequel, letters $\ell, r, s, t, \ldots$ are used for terms, $f, g, \ldots$ for symbols, σ, θ for substitutions, and C for contexts. The set of terms over signature $\mathcal{F}$ and variables $\mathcal{V}$ is $\mathcal{T}(\mathcal{F},\mathcal{V})$, and $\mathcal{S}\mathsf{ub}(\mathcal{F},\mathcal{V})$ denotes the set of substitutions of type $\mathcal{V} \to \mathcal{T}(\mathcal{F},\mathcal{V})$. The set of variables in a term t is denoted by $\mathcal{V}\mathsf{ar}(t)$. We write $\rhd$ for the strict subterm relation. The rewrite relation for some TRS R is denoted by $\to_R$, and the parallel rewrite relation is $\rightrightarrows_R$, where sometimes R is omitted if it is clear from the context. Rewrite relations may be restricted by positions, such as root steps ($\to_\epsilon$) or parallel rewriting where all steps are below the root ($\rightrightarrows_{>\epsilon}$). Given a binary relation $\to$, the reflexive transitive closure, the transitive closure, and the n-fold composition of the relation are denoted by $\to^*$, $\to^+$, and $\to^n$, respectively. A relation $\to$ is *confluent on A* if for all $y \in A$ and all x and z, whenever $x \;{}^*\!\!\leftarrow y \to^* z$, there is some u such that $x \to^* u \;{}^*\!\!\leftarrow z$; and $\to$ is *confluent* if it is confluent on the set of all elements. A TRS R is confluent if its rewrite relation $\to_R$ is confluent. A rewrite rule $\ell \to r$ is *left-linear* if no variable occurs more than once in ℓ, and a TRS is left-linear if so are all its rules.

An (oriented) conditional rewrite rule ρ over signature $\mathcal{F}$ is of the form $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ where $\ell, r, s_1, t_1, \ldots, s_k, t_k \in \mathcal{T}(\mathcal{F},\mathcal{V})$. The condition $s_1 \to t_1, \ldots, s_k \to t_k$ is sometimes abbreviated by c. Every standard rewrite rule $\ell \to r$ can be considered a conditional rewrite rule where $k = 0$. A CTRS over $\mathcal{F}$ is a set R of conditional rules over $\mathcal{F}$.

Definition 1 (Conditional rewriting [15, Def. 7.1.4]). *Let R be a CTRS. The unconditional TRSs R_n and the rewrite relation $\to_R$ are defined as follows.*

$$\begin{aligned} R_0 &= \varnothing \\ R_{n+1} &= \{(\ell\sigma, r\sigma) \mid \ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k \in R,\ \forall i.\ s_i\sigma \to^*_{R_n} t_i\sigma\} \\ \to_R &= \bigcup_{n \in \mathbb{N}} \to_{R_n} \end{aligned}$$

A CTRS R is of *type 3* if every rule $\ell \to r \Leftarrow c$ in R satisfies $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(\ell) \cup \mathcal{V}\mathsf{ar}(c)$. A CTRS of type 3 is *deterministic* if for every rule $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k \in R$ and every $1 \leqslant i \leqslant k$ it holds that $\mathcal{V}\mathsf{ar}(s_i) \subseteq \mathcal{V}\mathsf{ar}(\ell) \cup \bigcup_{j=1}^{i-1} \mathcal{V}\mathsf{ar}(t_j)$. In the sequel, we will only deal with deterministic CTRSs of type 3 (abbreviated 3DCTRSs).

Example 2. Let $\mathcal{F}$ be the signature consisting of constants $\mathsf{0}, \mathsf{T}, \mathsf{F}, []$, unary symbols s, qs, and binary symbols $\leqslant, :, @, \langle\cdot,\cdot\rangle, \mathsf{split}$. The following 3DCTRS R_1 over $\mathcal{F}$ encodes quicksort [15]:

$$\begin{array}{ccc} \mathsf{0} \leqslant x \to \mathsf{T} & \mathsf{s}(x) \leqslant \mathsf{0} \to \mathsf{F} & \mathsf{s}(x) \leqslant \mathsf{s}(y) \to x \leqslant y \\ [] \mathbin{@} x \to x & (x : xs) \mathbin{@} ys \to x : (xs \mathbin{@} ys) & \mathsf{split}(x, []) \to \langle [], [] \rangle \\ \mathsf{qs}([]) \to [] & & \end{array}$$

$$\begin{aligned} \mathsf{split}(x, y : ys) &\to \langle xs, y : zs \rangle \Leftarrow \mathsf{split}(x, ys) \to \langle xs, zs \rangle,\ x \leqslant y \to \mathsf{T} \\ \mathsf{split}(x, y : ys) &\to \langle y : xs, zs \rangle \Leftarrow \mathsf{split}(x, ys) \to \langle xs, zs \rangle,\ x \leqslant y \to \mathsf{F} \\ \mathsf{qs}(x : xs) &\to \mathsf{qs}(ys) \mathbin{@} (x : \mathsf{qs}(zs)) \Leftarrow \mathsf{split}(x, xs) \to \langle ys, zs \rangle \end{aligned}$$

3 Formalizing Conditional Rewriting

Instead of Def. 1, IsaFoR defines conditional rewriting as introduced in [12], where intermediate rewrite relations are used rather than auxiliary unconditional TRSs.

Definition 3 (Conditional rewriting [12]). *Let R be a CTRS. The rewrite relation $\to_R$ is defined as follows.*

$$\xrightarrow{0}_R = \varnothing$$

$$\xrightarrow{n+1}_R = \{(C[\ell\sigma], C[r\sigma]) \mid \ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k \in R,\ \forall i.\ s_i\sigma \xrightarrow{n}{}^*_R t_i\sigma\}$$

$$\to_R = \bigcup_{n \in \mathbb{N}} \xrightarrow{n}_R$$

It is easy to see that $\xrightarrow{n}_R = \to_{R_n}$, and therefore $\to_R$ is the same relation in both Def. 1 and Def. 3.

In IsaFoR we used Def. 3 since it constitutes a stand-alone inductive definition, whereas Def. 1 additionally requires the notion of unconditional rewriting. The use of Def. 3 thus simplified proofs in that it avoided auxiliary results involving standard rewriting. In particular, every rewrite step according to Def. 1 is associated with a rule, a context, and *two substitutions*, where the first substitution originates from the definition of the unconditional TRS R_{n+1}, and the second one stems from the rewrite relation $\to_{R_{n+1}}$ of this unconditional TRS. In contrast, a rewrite step according to Def. 3 involves only one substitution.

Besides the definition of $\to_R$, based on $\xrightarrow{n}_R$ defined as a recursive function on n, we also added several basic results on $\to_R$ to IsaFoR, which were mainly established by first proving them component-wise for $\xrightarrow{n}_R$ by induction on n. For instance, $\xrightarrow{n}_R$ is closed under contexts and substitutions, $\xrightarrow{n}_R \subseteq \xrightarrow{m}_R$ for $n \leqslant m$, etc., and these properties are then easily transferred to $\to_R$. Moreover, we added some extraction results, e.g., for finite derivations $s \to_R^* t$ one can always find a suitable n such that $s \xrightarrow{n}{}^*_R t$. This made it easy to switch between the full relation $\to_R$ and some approximation $\xrightarrow{n}_R$ in proofs.

Recall that the notion of termination is not as important for CTRSs as it is for TRSs. For a CTRS R one is rather interested in operational termination [6], where in addition to strong normalization of $\to_R$ one ensures that there will be no infinite recursion required when evaluating conditions. For example, the CTRS $R = \{\mathsf{f}(x) \to \mathsf{f}(x) \Leftarrow \mathsf{f}(\mathsf{f}(x)) \to \mathsf{f}(x)\}$ terminates as it satisfies $\to_R = \varnothing$, but it is not operationally terminating.

We formalized the following two sufficient criteria for operational termination.

Definition 4 (Quasi-Reductive). *A CTRS R is* quasi-reductive for $\succ$ *if $\succ$ is a strongly normalizing partial order which is closed under contexts, and for every $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ in R, every σ, and $0 \leqslant i < k$ it holds that*

- *if $s_j\sigma \succeq t_j\sigma$ for every $1 \leqslant j \leqslant i$, then $l\sigma\ (\succ \cup \rhd)^+\ s_{i+1}\sigma$, and*
- *if $s_j\sigma \succeq t_j\sigma$ for every $1 \leqslant j \leqslant k$, then $l\sigma \succ r\sigma$.*

A CTRS R is quasi-reductive if it is quasi-reductive for some $\succ$.

Definition 5 (Quasi-Decreasing). *A CTRS R is* quasi-decreasing *for $\succ$ if $\succ$ is a strongly normalizing partial order, $\rightarrow_R \cup \rhd \subseteq \succ$, and for every $\ell \rightarrow r \Leftarrow s_1 \rightarrow t_1, \ldots, s_k \rightarrow t_k$ in R, every substitution σ, and $0 \leqslant i < k$ it holds that if $s_j\sigma \rightarrow_R^* t_j\sigma$ for every $1 \leqslant j \leqslant i$ then $l\sigma \succ s_{i+1}\sigma$. A CTRS R is quasi-decreasing if there exists some $\succ$ such that R is quasi-decreasing for $\succ$.*

Definitions 4 and 5 are exactly the same as Definitions 7.2.36 and 7.2.39 in [15], respectively, except that our definitions do not mention signatures. This deviation is motivated by the fact that neither the conditional rewrite relation nor the unconditional rewrite relation in IsaFoR take signatures into account.

IsaFoR further includes the crucial proof of [15, Lemma 7.2.40], namely that whenever R is quasi-reductive for $\succ$, then R is also quasi-decreasing for $(\succ \cup \rhd)^+$. And since a 3DCTRS is quasi-decreasing if and only if it is operational terminating [6, Thms. 2 and 3], we provide a criterion for operational termination.

4 Unravelings

An unraveling is a computable transformation U which maps a CTRS R over some signature $\mathcal{F}$ to a TRS $U(R)$ over some signature $\mathcal{F}' \supseteq \mathcal{F}$.[2] An unraveling U is *sound with respect to reductions* for R if $s \rightarrow_{U(R)}^* t$ implies $s \rightarrow_R^* t$ for all terms $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. It is *complete with respect to reductions* for R if $s \rightarrow_R^* t$ implies $s \rightarrow_{U(R)}^* t$ for all $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. In order to be independent of concrete unravelings used by tools, our certifier is based on the following more flexible notion of *standard* unravelings.

To that end, two conditional rules $\ell \rightarrow r \Leftarrow s_1 \rightarrow t_1, \ldots, s_k \rightarrow t_k$ and $\ell' \rightarrow r' \Leftarrow s'_1 \rightarrow t'_1, \ldots, s'_{k'} \rightarrow t'_{k'}$ are called *prefix equivalent* up to m if $m \leqslant k$, $m \leqslant k'$, and there is a variable renaming τ such that $\ell\tau = \ell'$, $s_i\tau = s'_i$ for all $1 \leqslant i \leqslant m$, and $t_i\tau = t'_i$ for all $1 \leqslant i < m$. For instance, the first two conditional rules in Ex. 2 are prefix equivalent up to 2, with τ being the identity. For a finite set of variables $V = \{x_1, \ldots, x_n\}$, let $\overrightarrow{V}$ denote the sequence $x_1, \ldots, x_n$ such that $x_1 < \cdots < x_n$ for some arbitrary but fixed ordering $<$ on $\mathcal{V}$.

Definition 6 (Standard unraveling). *A* standard unraveling *U maps a rule ρ of the form $\ell \rightarrow r \Leftarrow s_1 \rightarrow t_1, \ldots, s_k \rightarrow t_k$ to the set of rules $U(\rho)$ given by*

$$U(\rho) = \left\{ \ell \rightarrow U_1^\rho(s_1, \overrightarrow{Z_1}),\ U_1^\rho(t_1, \overrightarrow{Z_1}) \rightarrow U_2^\rho(s_2, \overrightarrow{Z_2}),\ \ldots,\ U_k^\rho(t_k, \overrightarrow{Z_k}) \rightarrow r \right\}$$

where $X_i = \mathcal{V}\mathsf{ar}(\ell, t_1, \ldots, t_{i-1})$, $Y_i = \mathcal{V}\mathsf{ar}(r, t_i, s_{i+1}, t_{i+1} \ldots, s_k, t_k)$, and Z_i is an arbitrary set of variables satisfying $X_i \cap Y_i \subseteq Z_i$, for all $1 \leqslant i \leqslant k$, and $U_1^\rho, \ldots U_k^\rho \notin \mathcal{F}$. Furthermore, we require that $U_i^\rho = U_j^{\rho'}$ only if $i = j$ and ρ and ρ' are prefix equivalent up to i, for all $\rho, \rho' \in R$.

The definition of U is extended to a CTRS R by setting $U(R) = \bigcup_{\rho \in R} U(\rho)$.

[2] Definitions of unravelings in the literature typically demand that $\rightarrow_R \subseteq \rightarrow_{U(R)}^*$ and $U(R \uplus R') = U(R) \cup R'$ hold for any TRS R'. We do not require this by definition but all considered transformations enjoy these properties.

Note that setting $Z_i = X_i$ yields Ohlebusch's unraveling U_{seq} [13, 15], while by taking $Z_i = X_i \cap Y_i$ one obtains the optimized unraveling U_{opt} [2, 11], both of which are thus standard unravelings in our setting.[3] In addition, we allow—but do not enforce—the reuse of U symbols as proposed for the variant of Ohlebusch's unraveling U_{conf} [4] (and already mentioned in [15, page 213]). The set of symbols $\mathcal{F}'$ denotes the signature which extends $\mathcal{F}$ by all U_ρ^i symbols introduced by U.

Example 7. Let R_2 be $U_{\mathsf{conf}}(R_1)$, where the standard unraveling U_{conf} is applied to the CTRS R_1 from Ex. 2. Then R_2 contains all unconditional rules of R_1, and the following rules which replace the conditional rules of R_1:

$$\begin{aligned}
\mathsf{split}(x, y : ys) &\to U_1(\mathsf{split}(x, ys), x, y, ys)\\
U_1(\langle xs, zs\rangle, x, y, ys) &\to U_2(x \leqslant y, x, y, ys, xs, zs)\\
U_2(\mathsf{T}, x, y, ys, xs, zs) &\to \langle xs, y : zs\rangle\\
U_2(\mathsf{F}, x, y, ys, xs, zs) &\to \langle y : xs, zs\rangle\\
\mathsf{qs}(x : xs) &\to U_3(\mathsf{split}(x, xs), x, xs)\\
U_3(\langle ys, zs\rangle, x, xs) &\to \mathsf{qs}(ys) \mathbin{@} (x : \mathsf{qs}(zs))
\end{aligned}$$

Note that the first four rules can simulate both of the first two conditional rules.

Alternatively, a standard unraveling may produce the TRS R_3 where the conditional rules are transformed into:

$$\begin{aligned}
\mathsf{split}(x, y : ys) &\to U_1(\mathsf{split}(x, ys), x, y) & U_1(\langle xs, zs\rangle, x, y) &\to U_2(x \leqslant y, y, xs, zs)\\
U_2(\mathsf{T}, y, xs, zs) &\to \langle xs, y : zs\rangle & U_2(\mathsf{F}, y, xs, zs) &\to \langle y : xs, zs\rangle\\
\mathsf{qs}(x : xs) &\to U_3(\mathsf{split}(x, xs), x) & U_3(\langle ys, zs\rangle, x) &\to \mathsf{qs}(ys) \mathbin{@} (x : \mathsf{qs}(zs))
\end{aligned}$$

Here, R_3 corresponds to $U_{\mathsf{opt}}(R_1)$, except that U symbols are reused for the two prefix equivalent rules. For both R_2 and R_3, the extended signature is $\mathcal{F}' = \mathcal{F} \cup \{U_1, U_2, U_3\}$.

Reusing U symbols is often essential to obtain confluent unraveled systems, e.g., both $U_{\mathsf{opt}}(R_1)$ and $U_{\mathsf{seq}}(R_1)$ are non-confluent TRSs, whereas the TRSs $R_2 = U_{\mathsf{conf}}(R_1)$ and R_3 in Ex. 7 are orthogonal and hence confluent. Also termination provers can benefit from the repeated use of U symbols since for locally confluent overlay TRSs it suffices to prove innermost termination [5].

5 Completeness of Unravelings

Completeness of an unraveling U demands that derivations of R can be simulated by $U(R)$, i.e., $\to_R^* \subseteq \to_{U(R)}^*$ holds. This result is not hard to prove but has limited applicability. For example, it does not entail that termination of $U(R)$ implies strong normalization of $\to_R$ or quasi-reductiveness of R. Therefore, we first formalized a more general, technical result (Lem. 9) which is helpful to derive many of the other properties that we are interested in.

[3] The unraveling U_{D} proposed by Marchiori [8] differs from U_{seq} in that it admits multiple occurrences of the same variable in $\overrightarrow{Z_i}$. In general, it is hence not a standard unraveling, but U_{D} and U_{seq} coincide in the setting of left-linear unraveled systems.

The notion of a standard unraveling does not cover Marchiori's unraveling U_{D}. In order to cover U_{D} and also to keep our results as widely applicable as possible, we introduce an even more general notion of unravelings: Instead of demanding that the left- and right-hand-sides of unraveled rules are exactly of the form $U_i^\rho(t_i, \overrightarrow{Z_i})$ and $U_i^\rho(s_i, \overrightarrow{Z_i})$, we only assume that they are of the shape $C[t_i]$ and $C[s_i]$ for some context C.

Definition 8 (Generalized unraveling). *A* generalized *unraveling U maps a rule ρ of the form $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ to the set of rules $U(\rho)$ given by*

$$U(\rho) = \{\ell \to C_1^\rho[s_1],\ C_1^\rho[t_1] \to C_2^\rho[s_2]),\ \ldots,\ C_k^\rho[t_k] \to r\}$$

where each C_i^ρ is an arbitrary context. As in Def. 6, $U(R) = \bigcup_{\rho \in R} U(\rho)$.

In the remainder of this section, we assume that U is a generalized unraveling.

Lemma 9. *Let $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ be a rule in R, and $1 \leqslant i \leqslant k+1$. For $i = k+1$, define $s_{k+1} := r$ and $C_{k+1}^\rho = \Box$. If $s_j\sigma \to_{U(R)}^* t_j\sigma$ for all $1 \leqslant j < i$, then $\ell\sigma \to_{U(R)}^+ C_i^\rho[s_i]\sigma$.* $\Box$

Proof. $\ell\sigma \to_{U(R)} C_1^\rho[s_1]\sigma \to_{U(R)}^* C_1^\rho[t_1]\sigma \to_{U(R)} C_2^\rho[s_2]\sigma \to_{U(R)}^* \cdots \to_{U(R)}^* C_{i-1}^\rho[t_{i-1}]\sigma \to_{U(R)} C_i^\rho[s_i]\sigma$. $\Box$

Theorem 10 (Completeness). $\to_R \subseteq \to_{U(R)}^+$

Proof. We prove $\xrightarrow{n}_R \subseteq \to_{U(R)}^+$ by induction on n. The base case is trivial. So let $s \xrightarrow{n+1}_R t$, i.e., there is some $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ in R where $s = C[\ell\sigma]$, $t = C[r\sigma]$ and $s_i\sigma \xrightarrow{n}_R^* t_i\sigma$ for all $1 \leqslant i \leqslant k$. By the induction hypothesis, we conclude $s_i\sigma \to_{U(R)}^* t_i\sigma$ for all i. Hence, $\ell\sigma \to_{U(R)}^+ r\sigma$ by applying Lem. 9 for $i := k+1$. But then $s = C[\ell\sigma] \to_{U(R)}^+ C[r\sigma] = t$ immediately follows. $\Box$

Theorem 11 (Termination implies quasi-reductiveness). *If $U(R)$ is terminating then R is quasi-reductive for $\succ := \to_{U(R)}^+$.*

Proof. From termination of $U(R)$ we conclude that $\succ$ is a strongly normalizing partial order, which is obviously also closed under contexts. Let $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ be a rule in R, let i satisfy $0 \leqslant i \leqslant k$, and let $s_j\sigma \succeq t_j\sigma$ for every $1 \leqslant j \leqslant i$. By definition of $\succ$, the preconditions can be reformulated as $1 \leqslant i+1 \leqslant k+1$ and $s_j\sigma \to_{U(R)}^* t_j\sigma$ for all $1 \leqslant j < i+1$. Hence, by Lem. 9 we get $\ell\sigma \to_{U(R)}^+ C_{i+1}^\rho[s_{i+1}\sigma]$, i.e., $\ell\sigma \succ C_{i+1}^\rho[s_{i+1}\sigma]$ where in case $i = k$ we have $C_{i+1}^\rho = \Box$ and $s_{i+1} = r$. Thus, for $i < k$ we obtain $\ell\sigma \succ C_{i+1}^\rho[s_{i+1}\sigma] \trianglerighteq s_{i+1}\sigma$, and for $i = k$ we get $\ell\sigma \succ C_{i+1}^\rho[s_{i+1}\sigma] = r\sigma$, so all conditions of Def. 4 hold. $\Box$

To model generalized unravelings within IsaFoR, we assume U to be given as a function which takes a conditional rule ρ and an index i, and returns the context C_i^ρ. All proofs have been formalized as described above, with only a small overhead: for example, in becoming explicit in the "$\cdots$" within the statement and the proof of Lem. 9 (via quantifiers and inductive), or in manually providing the required substitutions and contexts when performing conditional rewriting.

Example 12. The TRS R_3 from Ex. 7 is terminating. According to Thm. 11, R_1 is thus quasi-reductive. A corresponding proof is automatically generated by AProVE and certified by CeTA.

6 Soundness of Unravelings

After having formalized simple proofs on unravelings like completeness, in this section we describe the following more challenging soundness result.

Theorem 13 (Soundness of standard unravelings). *Consider a 3DCTRS R and a standard unraveling U such that $U(R)$ is left-linear. Then U is sound with respect to reductions for R.*

Our formalization of this result follows the line of argument pursued in [12, Theorem 4.3]. However, Thm. 13 constitutes an extension in several respects. First, it is not fixed to the unraveling U_{opt}. Instead, it only assumes U to be a standard unraveling, thereby in particular covering U_{seq}, U_{conf}, and U_{opt}. Second, it does not rely on the assumption that R is non-left variable or non-right variable, i.e., that either no left- or no right-hand side of R is a variable. In [12] this restriction is used to simplify the decomposition of $U(R)$-rewrite sequences. Instead, we introduced the notion of partial and complete ρ-step simulations below. Finally, in contrast to the proof of [12, Lemma 4.2], we devised an inductive argument to prove the Key Lemma 18 in its full generality, instead of restricting to rules with only two conditions.

A number of preliminary results were required in order to prove Thm. 13.

Definition 14 (Complete and partial simulation). *Let $\rho = \ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$. A rewrite sequence $s \rightrightarrows^n_{U(R)} t$ contains a* complete ρ-step simulation *if it can be decomposed into a $U(R)$-rewrite sequence*

$$\begin{aligned} s &\rightrightarrows^{n_0} \ell\sigma_1 \to_\epsilon U^\rho_1(s_1, \overrightarrow{Z_1})\sigma_1 \\ &\rightrightarrows^{n_1}_{>\epsilon} U^\rho_1(t_1, \overrightarrow{Z_1})\sigma_2 \to_\epsilon U^\rho_2(s_2, \overrightarrow{Z_2})\sigma_2 \\ &\vdots \\ &\rightrightarrows^{n_k}_{>\epsilon} U^\rho_k(t_k, \overrightarrow{Z_k})\sigma_{k+1} \to_\epsilon r\sigma_{k+1} \rightrightarrows^{n_{k+1}} t \end{aligned} \tag{1}$$

for some $n_0, \ldots, n_{k+1}$ and substitutions $\sigma_1, \ldots, \sigma_{k+1}$ such that $n = n_{k+1} + \sum_{i=0}^{k}(n_i + 1)$. Moreover, $s \rightrightarrows^n_{U(R)} t$ contains a partial ρ-step simulation up to m *if it can be decomposed as*

$$\begin{aligned} s &\rightrightarrows^{n_0} \ell\sigma_1 \to_\epsilon U^\rho_1(s_1, \overrightarrow{Z_1})\sigma_1 \\ &\rightrightarrows^{n_1}_{>\epsilon} U^\rho_1(t_1, \overrightarrow{Z_1})\sigma_2 \to_\epsilon U^\rho_2(s_2, \overrightarrow{Z_2})\sigma_2 \\ &\vdots \\ &\rightrightarrows^{n_{m-1}}_{>\epsilon} U^\rho_{m-1}(t_{m-1}, \overrightarrow{Z_{m-1}})\sigma_m \to_\epsilon U^\rho_m(s_m, \overrightarrow{Z_m})\sigma_m \rightrightarrows^{n_m}_{>\epsilon} t \end{aligned} \tag{2}$$

for some $m \leqslant k$ as well as $n_0, \ldots, n_m$ and substitutions $\sigma_1, \ldots, \sigma_m$ such that $n = n_m + \sum_{i=0}^{m-1}(n_i + 1)$.

The proof of the following result is technical but straightforward, applying induction on the length of the rewrite sequence A.

Lemma 15. *Suppose $s \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ admits a rewrite sequence $A\colon s \rightrightarrows^n_{U(R)} t$ which contains a root step. Then A contains a complete or a partial ρ-step simulation for some $\rho \in R$.* $\square$

Lemma 16 ([12, Lemma A.1]). *Consider a 3DCTRS R, a rule $\rho \in R$ of the form $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ such that $U(\rho)$ is left-linear, and substitutions $\theta_1, \ldots, \theta_{k+1}$. If $s_i\theta_i \to^*_R t_i\theta_{i+1}$ and $\overrightarrow{Z_i}\theta_i \to^*_R \overrightarrow{Z_i}\theta_{i+1}$ for all $1 \leqslant i \leqslant k$ then $\ell\theta_1 \to^*_R r\theta_{k+1}$.* $\square$

Here $\overrightarrow{Z_i}\theta_i \to^*_R \overrightarrow{Z_i}\theta_{i+1}$ denotes $z_j\theta_i \to^*_R z_j\theta_{i+1}$ for all $1 \leqslant j \leqslant n$, given $Z_i = \{z_1, \ldots, z_n\}$. The following lemma follows from the properties of 3DCTRSs.

Lemma 17. *A rule $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ in a 3DCTRS satisfies*

1. *$\mathcal{V}\mathsf{ar}(s_{m+1}) \subseteq \mathcal{V}\mathsf{ar}(t_m) \cup (X_m \cap Y_m)$ for all $m < k$, and*
2. *$\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(t_k) \cup (X_k \cap Y_k)$.* $\square$

Lemma 18 (Key Lemma). *Consider a 3DCTRS R and a standard unraveling U such that $U(R)$ is left-linear. Let $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and t be linear such that $s \rightrightarrows^n_{U(R)} t\sigma$ for some substitution $\sigma \in \mathcal{S}\mathsf{ub}(\mathcal{F}', \mathcal{V})$. Then there is some substitution θ such that (i) $s \to^*_R t\theta$, (ii) $x\theta \rightrightarrows^n_{U(R)} x\sigma$ and $x\theta \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ for all $x \in \mathcal{V}\mathsf{ar}(t)$, and (iii) if $t\sigma \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ then $t\theta = t\sigma$.*

Before proving the key lemma, we show that it admits a very short proof of the main soundness result. The lemma will also be used in § 7 to prove confluence.

Proof (Proof of Thm. 13). Consider $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ such that $s \to^*_{U(R)} t$. Let $x \in \mathcal{V}$ and $\sigma := \{x \mapsto t\}$. Hence $s \rightrightarrows^*_{U(R)} x\sigma$ holds, and from Lem. 18 it follows that $s \to^*_R x\sigma = t$. $\square$

The following four pages describe a complete paper proof of the key lemma. We present it for the following reasons: In contrast to the proof of [12, Theorem 3.8], it devises an argument for the general case instead of restricting to two conditions. It is also structured differently, as it makes use of the notion of complete and partial ρ-step simulations and prefix equivalence. The latter differences in particular allowed us to show a more general result. And finally, the paper proof served as a detailed and human-readable proof plan for the proof within IsaFoR: the formalized proof contains even more details and is over 800 lines long.

At this point we want to emphasize the advantage of having a formalized proof within a proof assistant like Isabelle: in order to verify the proof's correctness, one can simply check whether the statement of the key lemma from the paper corresponds to the one in the formalization, because the (even more detailed) formalized proof is validated automatically.

Proof (of key lemma). The proof is by induction on (n, s), compared lexicographically by $>$ and $\rhd$. If $n = 0$ then $s = t\sigma \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, and one can set $\theta = \sigma$. The remainder of the proof performs a case analysis on a rewrite sequence

$$s \rightrightarrows^{n+1}_{U(R)} t\sigma \tag{3}$$

To enhance readability, the subscript in $\rightrightarrows_{U(R)}$ will be omitted; all steps denoted $\rightrightarrows$ and $\to_\epsilon$ are in $U(R)$.

Case (i): The sequence (3) *does not contain a root step.* Then s cannot be a variable so, $s = f(s_1, \dots, s_m)$ for some $f \in \mathcal{F}$. In this case, the result will easily follow from the induction hypothesis. Still, we have to consider two cases.

1. Suppose $t \notin \mathcal{V}$. As (3) does not contain a root step we may write $t = f(t_1, \dots, t_m)$, and have $s_i \rightrightarrows^{n+1} t_i\sigma$ for all $1 \leqslant i \leqslant m$. (Here we employ the fact that $\rightrightarrows^k \subseteq \rightrightarrows^{n+1}$ for all $k \leqslant n+1$, which will be freely used in the sequel of this proof.) For all i such that $1 \leqslant i \leqslant m$, $s_i, t_i \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and t_i is linear. Hence the induction hypothesis yields a substitution θ_i such that $s_i \to^*_R t_i\theta_i$, $x\theta_i \rightrightarrows^{n+1} x\sigma$ and $x\theta_i \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ for all $x \in \mathcal{V}\mathsf{ar}(t_i)$, and $t_i\theta_i = t_i\sigma$ if $t_i\sigma \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. By linearity of t, $\theta := \bigcup_{i=1}^m \theta_i|_{\mathcal{V}\mathsf{ar}(t_i)} \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ is a substitution which satisfies $t_i\theta_i = t_i\theta$ for all i. Hence we obtain
$$s = f(s_1, \dots, s_m) \to^*_R f(t_1, \dots, t_m)\theta = t\theta \rightrightarrows^{n+1} f(t_1, \dots, t_m)\sigma = t\sigma$$
and if $t\sigma \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ then $t_i\sigma \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ implies $t_i\theta = t_i\theta_i = t_i\sigma$, such that $t\theta = t\sigma$.
2. We have $t = x \in \mathcal{V}$, hence $x\sigma = f(t_1, \dots, t_m)$. Let $x_1, \dots, x_m$ be distinct variables and σ' be a substitution such that $x_i\sigma' = t_i$ for all $1 \leqslant i \leqslant m$. As $s = f(s_1, \dots, s_m)$ and (3) does not contain a root step, we have $s_i \rightrightarrows^{n+1} t_i = x_i\sigma'$. For all i such that $1 \leqslant i \leqslant m$, the induction hypothesis yields a substitution θ_i such that $s_i \to^*_R x_i\theta_i$, $x_i\theta_i \rightrightarrows^{n+1} x_i\sigma'$ and $x_i\theta_i \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, where $x_i\theta_i = x_i\sigma'$ if $x_i\sigma' \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. Let $\theta := \{x \mapsto f(x_1\theta_1, \dots, x_m\theta_m)\}$. One thus obtains
$$s = f(s_1, \dots, s_m) \to^*_R f(x_1\theta_1, \dots, x_m\theta_m) = x\theta \rightrightarrows^{n+1} f(x_1, \dots, x_m)\sigma' = x\sigma$$
and if $t\sigma \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ then $t_i = x_i\sigma' \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ implies $x_i\theta_i = x_i\sigma'$, so $t\theta = t\sigma$.

Case (ii): The sequence (3) *contains a root step.* Then according to Lem. 15, (3) contains a partial or a complete ρ-step simulation for some $\rho \in R$ where ρ is of the shape $\ell \to r \Leftarrow s_1 \to t_1, \dots, s_k \to t_k$, and $s \rightrightarrows^{n_0} \ell\sigma_1$ for some $n_0 < n+1$. As $\ell \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ is linear by the assumption of left-linearity, the induction hypothesis yields a substitution θ_1 such that $s \to^*_R \ell\theta_1$, $x\theta_1 \rightrightarrows^{n_0} x\sigma_1$ and $x\theta_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ for all $x \in \mathcal{V}\mathsf{ar}(\ell)$, and if $\ell\sigma_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ then $\ell\theta_1 = \ell\sigma_1$ $(\star)$.

1. Suppose (3) contains a partial ρ-step simulation up to m of the form
$$s \rightrightarrows^{n_0} \ell\sigma_1 \to_\epsilon U_1^\rho(s_1, \overrightarrow{Z_1})\sigma_1 \rightrightarrows^{n_1}_{>\epsilon} \cdots \to_\epsilon U_m^\rho(s_m, \overrightarrow{Z_m})\sigma_m \rightrightarrows^{n_m}_{>\epsilon} t\sigma$$

for $m \leq k$, such that $\mathsf{root}(t\sigma) = U_m$. Since $t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ by assumption it must be the case that $t = x \in \mathcal{V}$. Let $\theta = \{x \mapsto \ell\theta_1\}$. In combination with ($\star$) it follows that $s \to_R^* \ell\theta_1 = x\theta$, $x\theta = \ell\theta_1 \rightrightarrows^{n_0} \ell\sigma_1 \rightrightarrows^{n+1-n_0} t\sigma = x\sigma$ and consequently $x\theta \rightrightarrows^{n+1} x\sigma$, $x\theta = \ell\theta_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and $x\sigma \notin \mathcal{T}(\mathcal{F}, \mathcal{V})$ which shows the claim.

2. Suppose (3) contains a complete ρ-step simulation

$$\begin{aligned} s &\rightrightarrows^{n_0} \ell\sigma_1 \to_\epsilon U_1^\rho(s_1, \overrightarrow{Z_1})\sigma_1 \rightrightarrows_{>\epsilon}^{n_1} U_1^\rho(t_1, \overrightarrow{Z_1})\sigma_2 \to_\epsilon U_2^\rho(s_2, \overrightarrow{Z_2})\sigma_2 \rightrightarrows_{>\epsilon}^{n_2} \cdots \\ &\to_\epsilon U_k^\rho(s_k, \overrightarrow{Z_k})\sigma_k \rightrightarrows_{>\epsilon}^{n_k} U_k^\rho(t_k, \overrightarrow{Z_k})\sigma_{k+1} \\ &\to_\epsilon r\sigma_{k+1} \rightrightarrows^{n_{k+1}} t\sigma \end{aligned} \tag{4}$$

The key step is now to establish existence of a substitution θ' such that

$$s \to_R^+ r\theta', \qquad r\theta' \in \mathcal{T}(\mathcal{F}, \mathcal{V}), \text{ and} \qquad r\theta' \rightrightarrows^n t\sigma \tag{5}$$

First, suppose ρ is an unconditional rule $\ell \to r$. Then one can take $\theta' := \theta_1$: By ($\star$) one has $s \to_R^* \ell\theta_1$, and for all $x \in \mathcal{V}\mathsf{ar}(\ell)$ it holds that $x\theta_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, $x\theta_1 \rightrightarrows^{n_0} x\sigma_1$ and $x\theta_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. Obviously there is also the rewrite sequence $s \to_R^* r\theta_1$. As $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(\ell)$ because R is a DCTRS, the properties of θ_1 imply $r\theta_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. Together with ($\star$), $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(\ell)$ also implies $r\theta_1 \rightrightarrows^{n_0} r\sigma_1$. Combined with the complete simulation, $r\theta_1 \rightrightarrows^n t\sigma$ holds.
Second, in the case of a conditional rule the following claim is used: there are substitutions $\theta_1, \ldots, \theta_{k+1}$ such that θ_1 is as derived in ($\star$), and it holds that

(a) $s_i\theta_i \to_R^* t_i\theta_{i+1}$ (c) $\theta_j|_{V_j} \in \mathcal{S}\mathsf{ub}(\mathcal{F}, \mathcal{V})$
(b) $\overrightarrow{Z_i}\theta_i \to_R^* \overrightarrow{Z_i}\theta_{i+1}$ (d) $x\theta_{i+1} \rightrightarrows^{N_i} x\sigma_{i+1} \quad \forall x \in \mathcal{V}\mathsf{ar}(t_i) \cup Z_i$

for all $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant k+1$. Here $N_i = \sum_{j=0}^i n_j$, and V_j denotes the variable set defined by $V_1 = \mathcal{V}\mathsf{ar}(\ell)$ and $V_{j+1} = \mathcal{V}\mathsf{ar}(t_j) \cup (X_j \cap Y_j)$ for $j > 0$. We conclude the main proof before showing the claim. In particular, the claim yields substitutions $\theta_1, \ldots, \theta_{k+1}$ with properties (a)–(d). Due to (a), (b), and Lem. 16, there is a rewrite sequence $\ell\theta_1 \to_R^* r\theta_{k+1}$. In combination with ($\star$) it follows that $s \to_R^* \ell\theta_1 \to_R^* r\theta_{k+1}$. According to Lem. 17 (2), $\mathcal{V}\mathsf{ar}(r) \subseteq \mathcal{V}\mathsf{ar}(t_k) \cup (X_k \cap Y_k) = V_{k+1}$, so with (c) it holds that $r\theta_{k+1} \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. Moreover, in combination with (d) and the fact that $X_k \cap Y_k \subseteq Z_k$ one has $x\theta_{k+1} \rightrightarrows^{N_k} x\sigma_{k+1}$ for all $x \in \mathcal{V}\mathsf{ar}(r)$, and hence $r\theta_{k+1} \rightrightarrows^{N_k} r\sigma_{k+1} \rightrightarrows^{n_{k+1}} t\sigma$. Now since $N_k + n_{k+1} \leqslant n$ one has $r\theta_{k+1} \rightrightarrows^n t\sigma$, so the substitution θ_{k+1} satisfies all properties of θ' as demanded in (5).
So suppose there is a substitution θ' which satisfies the properties (5). Applying the induction hypothesis to the rewrite sequence $r\theta' \rightrightarrows^n t\sigma$ yields a substitution θ such that $r\theta' \to_R^* t\theta$ (and hence $s \to_R^* t\theta$), $x\theta \rightrightarrows^n x\sigma$ and $x\theta \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ for all $x \in \mathcal{V}\mathsf{ar}(t)$, and if $t\sigma \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ then $t\theta = t\sigma$. This concludes the case of a complete ρ-step simulation, it only remains to prove the above claim.
Proof of the claim. We perform an inner induction on k. In the base where $k = 0$, the singleton substitution list containing θ_1 vacuously satisfies properties (a), (b), and (d), and (c) holds as $\theta_1|_{V_1} \in \mathcal{S}\mathsf{ub}(\mathcal{F}, \mathcal{V})$ according to ($\star$).

So consider the case for $k = m+1$. From the induction hypothesis one obtains substitutions $\theta_1, \ldots, \theta_k$ which satisfy properties (a)–(d) for all $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant k$. In the sequel, they will be referred to by (a')–(d'). Let θ'_k be defined as follows:

$$\theta'_k(x) = \begin{cases} x\theta_k & \text{if } k = 1 \text{ and } x \in \mathcal{V}\mathsf{ar}(\ell), \text{ or } x \in \mathcal{V}\mathsf{ar}(t_m) \cup Z_m \\ x\sigma_k & \text{otherwise} \end{cases}$$

In the first place

$$s_k\theta'_k \rightrightarrows^{N_m} s_k\sigma_k \quad \text{and} \quad s_k\theta'_k \in \mathcal{T}(\mathcal{F}, \mathcal{V}) \tag{6}$$

is established by means of a case analysis. First, suppose $k = 1$. As R is deterministic, $\mathcal{V}\mathsf{ar}(s_1) \subseteq \mathcal{V}\mathsf{ar}(\ell)$. According to ($\star$), $x\theta_1 \rightrightarrows^{n_0} x\sigma_1$ and $x\theta_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ hold for all $x \in \mathcal{V}\mathsf{ar}(\ell)$. By definition of θ'_1 and $\mathcal{V}\mathsf{ar}(s_1) \subseteq \mathcal{V}\mathsf{ar}(\ell)$ we get $s_1\theta'_1 = s_1\theta_1$. Hence $s_1\theta'_1 \rightrightarrows^{n_0} s_1\sigma_1$ and thus $s_1\theta'_1 \rightrightarrows^{N_0} s_1\sigma_1$, and $s_1\theta'_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. Second, suppose $k > 1$. By Lem. 17 (1) one has $\mathcal{V}\mathsf{ar}(s_k) \subseteq \mathcal{V}\mathsf{ar}(t_m) \cup (X_m \cap Y_m) = V_k$. Due to $X_m \cap Y_m \subseteq Z_m$ it also holds that $\mathcal{V}\mathsf{ar}(s_k) \subseteq \mathcal{V}\mathsf{ar}(t_m) \cup Z_m$. By (d'), $x\theta_k \rightrightarrows^{N_m} x\sigma_k$ and $x\theta_k \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ for all $x \in \mathcal{V}\mathsf{ar}(t_m) \cup Z_m$, such that also $s_k\theta_k \rightrightarrows^{N_m} s_k\sigma_k$ holds. From $\mathcal{V}\mathsf{ar}(s_k) \subseteq \mathcal{V}\mathsf{ar}(t_m) \cup Z_m$ it also follows that $s_k\theta_k = s_k\theta'_k$ such that $s_k\theta'_k \rightrightarrows^{N_m} s_k\sigma_k$ holds. Moreover, $\mathcal{V}\mathsf{ar}(s_k) \subseteq V_k$ and (c') imply $s_k\theta'_k \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, so (6) is satisfied.
According to derivation (4) $s_k\sigma_k \rightrightarrows^{n_k} t_k\sigma_{k+1}$ holds, so with (6) it follows that $s_k\theta'_k \rightrightarrows^{N_k} t_k\sigma_{k+1}$. Now the outer induction hypothesis can be applied to this rewrite sequence: as $U(R)$ is left-linear also t_k must be linear, $s_k\theta'_k, t_k \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, and $N_k < n + 1$ so one obtains a substitution θ_s such that

$$s_k\theta'_k \to_R^* t_k\theta_s, \qquad x\theta_s \rightrightarrows^{N_k} x\sigma_{k+1}, \text{ and} \qquad x\theta_s \in \mathcal{T}(\mathcal{F}, \mathcal{V}) \tag{7}$$

for all $x \in \mathcal{V}\mathsf{ar}(t_k)$.
Next, we show that for every $z \in Z_k$ there is a substitution θ_z such that

$$z\theta'_k \to_R^* z\theta_z, \qquad z\theta_z \rightrightarrows^{N_k} z\sigma_{k+1}, \text{ and} \qquad z(\theta_z|_{V_k}) \in \mathcal{T}(\mathcal{F}, \mathcal{V}). \tag{8}$$

holds, by a case analysis. First, in the case where either $k = 1$ and $z \notin \mathcal{V}\mathsf{ar}(\ell)$, or $k > 1$ and $z \notin \mathcal{V}\mathsf{ar}(t_m) \cup Z_m$, it suffices to take $\theta_z = \{z \mapsto z\theta'_k\} = \{z \mapsto z\sigma_k\}$ as according to derivation (4) one has $z\sigma_k \rightrightarrows^{n_k} z\sigma_{k+1}$ and hence $z\sigma_k \rightrightarrows^{N_k} \sigma_{k+1}$. Both $z(\theta_z|_{V_k}) \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ and $z\theta'_k \to_R^* z\theta_z$ trivially hold, so (8) is satisfied.
Second, if $k = 1$ and $z \in \mathcal{V}\mathsf{ar}(\ell)$, or $k > 1$ and $z \in \mathcal{V}\mathsf{ar}(t_m) \cup Z_m$. Then

$$z\theta'_k \rightrightarrows^{N_m} z\sigma_k \quad \text{and} \quad z(\theta'_k|_{V_k}) \in \mathcal{T}(\mathcal{F}, \mathcal{V}) \tag{9}$$

holds, as can be seen by a case analysis on k. If $k = 1$ and $z \in \mathcal{V}\mathsf{ar}(\ell)$, then by ($\star$) it holds that $z\theta_1 \rightrightarrows^{n_0} z\sigma_1$ and $z\theta_1 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, so also $z\theta_1 \rightrightarrows^{N_0} z\sigma_1$ is satisfied, and $z\theta'_1 = z\theta_1$ holds by definition. If $k > 1$ then $z\theta'_k \rightrightarrows^{N_m} z\sigma_k$ and $z(\theta'_k|_{V_k}) \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ hold according to (c'), (d') and as $z\theta'_k = z\theta_k$.

So in both cases (9) is satisfied. Now the derivation (4) implies $z\sigma_k \rightrightarrows^{n_k} z\sigma_{k+1}$, and together with (9) it holds that $z\theta'_k \rightrightarrows^{N_k} z\sigma_{k+1}$. Applying the outer induction hypothesis to this rewrite sequence yields a substitution θ_z that satisfies (8).

Since $U(R)$ is left-linear, $\mathcal{V}\mathsf{ar}(t_k)$ and Z_k are disjoint. Therefore, $\theta_{k+1} := \theta_s|_{\mathcal{V}\mathsf{ar}(t_k)} \cup \bigcup_{z\in Z_k}\{z \mapsto z\theta_z\}$ is a well-defined substitution. It can be verified that the sequence of substitutions $\theta_1, \ldots, \theta_m, \theta'_k, \theta_{k+1}$ satisfies all desired properties (a)–(d):
First, note that $\theta_1, \ldots, \theta_m, \theta'_k$ also satisfy the properties corresponding to (a')–(d'): from (a') one has $s_m\theta_m \to_R^* t_m\theta'_k$ because $t_m\theta_k = t_m\theta'_k$; $\overrightarrow{Z}_m\theta_m \to_R^* \overrightarrow{Z}_m\theta'_k$ and $\theta'_k|_{V_k} \in \mathcal{S}\mathsf{ub}(\mathcal{F},\mathcal{V})$ hold by (b'), (c'), and the definition of θ'_k. By the definition of θ'_k, $x\theta'_k = x\theta_k$ for all $x \in \mathcal{V}\mathsf{ar}(t_m) \cup Z_m$, so (d') also holds for $\theta_1, \ldots, \theta_m, \theta'_k$.
In summary, one can conclude

$$\begin{array}{ll} \text{(a) } s_i\theta_i \to_R^* t_i\theta_{i+1} & \text{(c) } \theta_j|_{V_j} \in \mathcal{S}\mathsf{ub}(\mathcal{F},\mathcal{V}) \\ \text{(b) } \overrightarrow{Z_i}\theta_i \to_R^* \overrightarrow{Z_i}\theta_{i+1} & \text{(d) } x\theta_{i+1} \rightrightarrows^{N_i} x\sigma_{i+1} \quad \forall x \in \mathcal{V}\mathsf{ar}(t_i) \cup Z_i \end{array}$$

for all $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant k+1$, where (a) follows from (a') and as $s_k\theta'_k \to_R^* t_k\theta_{k+1}$ follows from (7). Next, (b) holds because of (b') and (8), which entails $\overrightarrow{Z_k}\theta'_k \to_R^* \overrightarrow{Z_k}\theta_{k+1}$ as $z\theta_z = z\theta_{k+1}$ for all $z \in Z_k$. Finally, (7) and (8) imply $\theta_{k+1}|_{V_{k+1}} \in \mathcal{S}\mathsf{ub}(\mathcal{F},\mathcal{V})$ and $x\theta_{k+1} \rightrightarrows^{N_k} x\sigma_{k+1}$ for all $x \in \mathcal{V}\mathsf{ar}(t_k) \cup Z_k$, which together with (c') and (d') induce (c) and (d). □

Thm. 13 and its preliminary lemmas are formalized in IsaFoR as presented in the proofs above. As already mentioned, the notions of partial and complete ρ-step simulations are used to circumvent the restriction to non-left or non-right variable CTRSs (and a respective duplication of the main proof steps). At some places the formalization induces some technical overhead, for instance to construct a substitution by taking the union of a set of domain-disjoint substitutions.

7 Applying Unravelings to Confluence

It is known that confluence of an unraveled system $U(R)$ implies confluence of the conditional system R under certain conditions [4]. In order to verify proof certificates by CoCon, a respective result was added to IsaFoR, and the following paragraphs describe our formalized proof.

We call a standard unraveling *source preserving* if for all rules $\rho \in R$ of the form $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ it holds that $\mathcal{V}\mathsf{ar}(\ell) \subseteq Z_i$ for all $i \leqslant k$. The intuition behind this notion is that then each term $U_i^\rho(t, \overrightarrow{Z_i})\sigma$ completely determines σ on $\mathcal{V}\mathsf{ar}(\ell)$. For instance, R_2 in Ex. 7 is source preserving, but R_3 is not since the information on x gets lost in U_2.

Lemma 19. *Let R be a deterministic, non-left variable 3DCTRS, and let U be a source preserving unraveling such that $U(R)$ is left-linear. Suppose $s, t \in \mathcal{T}(\mathcal{F},\mathcal{V})$*

such that $s \to^*_{U(R)} u \;{}_{U(R)}{}^*\!\!\leftarrow t$ *for some* $u \in \mathcal{T}(\mathcal{F}', \mathcal{V})$*. Then there is some* $v \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ *such that* $s \to^*_R v \;{}_R^*\!\!\leftarrow t$ *holds.*

Proof. By induction on u. If $u \in \mathcal{V}$ then $u \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, so using Thm. 13 one can directly conclude $s \to^*_R u \;{}_R^*\!\!\leftarrow t$.

Otherwise, suppose for a first case that $\mathsf{root}(u) \in \mathcal{F}$, so let $u = f(u_1, \ldots, u_m)$. Let u' be the linear term $f(x_1, \ldots, x_m)$, and $\sigma := \{x_i \mapsto u_i \mid 1 \leqslant i \leqslant m\}$, i.e., $u = u'\sigma$. We have $s \rightrightarrows^{n_s}_{U(R)} u'\sigma$ and $t \rightrightarrows^{n_t}_{U(R)} u'\sigma$ for some n_s and n_t. From Lem. 18 we thus obtain substitutions θ_s and θ_t such that $s \to^*_R u'\theta_s$, $t \to^*_R u'\theta_t$, and $u'\theta_s, u'\theta_t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. Moreover, for all variables $x_i \in \{x_1, \ldots, x_m\}$ we have $x_i\theta_s \to^*_{U(R)} x_i\sigma$ and $x_i\theta_t \to^*_{U(R)} x_i\sigma$; and since $u \rhd x_i\sigma$, we can apply the induction hypothesis to obtain $x_i\theta_s \to^*_R v_i \;{}_R^*\!\!\leftarrow x_i\theta_t$ for some $v_i \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. Joinability of s and t follows because of

$$s \to^*_R u'\theta_s \rightrightarrows^*_R f(v_1, \ldots, v_m) \;{}_R^*\!\!\leftleftarrows u'\theta_t \;{}_R^*\!\!\leftarrow t$$

Second, assume $\mathsf{root}(u) \notin \mathcal{F}$, so by the assumption $u \in \mathcal{T}(\mathcal{F}', \mathcal{V})$ we have $u = U_i^\rho(u_1, \vec{Z}_i\nu)$ for some $\rho \in R$ of the form $\ell \to r \Leftarrow s_1 \to t_1, \ldots, s_k \to t_k$ and $1 \leqslant i \leqslant k$, some term u_i and some substitution ν. Let $x \in \mathcal{V}$ be some variable, so we have $s \rightrightarrows^{n_s}_{U(R)} x\{x \mapsto u\}$ for some n_s. By Lem. 18, there is a substitution θ_s such that $s \to^*_R x\theta_s$, and $x\theta_s \in \mathcal{T}(\mathcal{F}, \mathcal{V})$.

As u is rooted by U_i^ρ an analysis of the proof of Lem. 18 for this case shows the following:[4] The rewrite sequence $s \rightrightarrows^{n_s}_{U(R)} x\{x \mapsto u\}$ contains a partial ρ'-step simulation up to i, for some rule $\rho' \in R$ prefix equivalent to ρ, and there are a substitution σ_0 such that $x\theta_s = \ell\sigma_0$ as well as substitutions $\sigma_1, \ldots, \sigma_i$ such that

1. $z\sigma_0 \rightrightarrows^*_{U(R)} z\sigma_1$ for all $z \in \mathcal{V}\mathsf{ar}(\ell)$,
2. $z\sigma_j \rightrightarrows^*_{U(R)} z\sigma_{j+1}$ for all $z \in Z_j$ and $1 \leqslant j < i$, and
3. $z\sigma_i \rightrightarrows^*_{U(R)} z\nu$ for all $z \in Z_i$.

Consider some variable $z \in \mathcal{V}\mathsf{ar}(\ell)$. Since U is source preserving, $z \in Z_j$ for all $j \leqslant i$. Therefore, the properties of the substitutions σ_j yield a rewrite sequence $z\sigma_0 \rightrightarrows^*_{U(R)} z\nu$.

In the same way the rewrite sequence $t \rightrightarrows^{n_t}_{U(R)} x\{x \mapsto u\}$ gives rise to substitutions θ_t, τ_0 such that $t \to^*_R z\theta_t$, $z\theta_t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, $z\theta_t = \ell\tau_0$, and $z\tau_0 \rightrightarrows^*_{U(R)} z\nu$ holds for all $z \in \mathcal{V}\mathsf{ar}(\ell)$.

Consider again some $z \in \mathcal{V}\mathsf{ar}(\ell)$. We have $z\sigma_0 \rightrightarrows^*_{U(R)} z\nu$ and $z\tau_0 \rightrightarrows^*_{U(R)} z\nu$, where $z\sigma_0, z\tau_0 \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. But as we have $u \rhd z\nu$, the induction hypothesis shows $z\sigma_0 \downarrow_R z\tau_0$. Hence $\ell\sigma_0$ and $\ell\tau_0$ are joinable to some common reduct $\ell\nu' \in \mathcal{T}(\mathcal{F}, \mathcal{V})$.

In summary, joinability of s and t follows from the rewrite sequence

$$s \to^*_R x\theta_s = \ell\sigma_0 \rightrightarrows^*_R \ell\nu' \;{}_R^*\!\!\leftleftarrows \ell\tau_0 = x\theta_t \;{}_R^*\!\!\leftarrow t$$

□

Theorem 20 (Confluence). *Let* R *be a non-left variable 3DCTRS over signature* $\mathcal{F}$*, and* U *be a source preserving unraveling such that* $U(R)$ *is left-linear. Then confluence of* $U(R)$ *implies confluence of* R*.*

[4] Within IsaFoR this fact is made explicit by adapting the statement of Lem. 18.

Proof. Consider a peak $s \;{}_R^*\!\!\leftarrow u \to_R^* t$ with $u \in \mathcal{T}(\mathcal{F}, \mathcal{V})$. Then also $s, t \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ since R has signature $\mathcal{F}$. By completeness of U, we also have $s \;{}_{U(R)}^*\!\!\leftarrow u \to_{U(R)}^* t$. Confluence of $U(R)$ yields a join $s \to_{U(R)}^* v' \;{}_{U(R)}^*\!\!\leftarrow t$ for some term $v' \in \mathcal{T}(\mathcal{F}', \mathcal{V})$. By Lem. 19 there is also a term $v \in \mathcal{T}(\mathcal{F}, \mathcal{V})$ such that $s \to_R^* v \;{}_R^*\!\!\leftarrow t$. Hence R is confluent on terms in $\mathcal{T}(\mathcal{F}, \mathcal{V})$. A further technical renaming suffices to prove confluence on all terms u, where we refer to the formalization for details. □

Example 21. The TRS $R_2 = U_{\mathsf{conf}}(R_1)$ from Ex. 7 is confluent since it is orthogonal. According to Thm. 20, R_1 is thus confluent as well. Due to our formalization, the confluence proof generated by ConCon can be certified by CeTA.

The following example shows that U_{conf} is not necessarily an optimal choice when it comes to confluence analysis.

Example 22. Consider the CTRS R_4 consisting of rules

$$\mathsf{a} \to \mathsf{b} \;\Leftarrow\; \mathsf{c} \to x,\; \mathsf{d}_i(x) \to \mathsf{e} \qquad\qquad \mathsf{d}_i(\mathsf{c}) \to \mathsf{e}$$

for $i \in \{1, 2\}$. We obtain the following unraveled TRSs:

$$\begin{array}{rllll}
U_{\mathsf{conf}}: & \mathsf{a} \to U_1(\mathsf{c}) & U_1(x) \to U_2^i(\mathsf{d}_i(x), x) & U_2^i(\mathsf{e}, x) \to \mathsf{b} & \mathsf{d}_i(\mathsf{c}) \to \mathsf{e} \\
U_{\mathsf{opt}}: & \mathsf{a} \to U_1^i(\mathsf{c}) & U_1^i(x) \to U_2^i(\mathsf{d}_i(x)) & U_2^i(\mathsf{e}) \to \mathsf{b} & \mathsf{d}_i(\mathsf{c}) \to \mathsf{e} \\
U_{\mathsf{seq}}: & \mathsf{a} \to U_1^i(\mathsf{c}) & U_1^i(x) \to U_2^i(\mathsf{d}_i(x), x) & U_2^i(\mathsf{e}, x) \to \mathsf{b} & \mathsf{d}_i(\mathsf{c}) \to \mathsf{e}
\end{array}$$

U_{conf} admits the non-joinable peak $U_2^1(\mathsf{d}_1(x), x) \leftarrow U_1(x) \to U_2^2(\mathsf{d}_2(x), x)$, but U_{seq} (as well as U_{opt}) is confluent, so R_4 is confluent by Thm. 20.

8 Conclusion

We presented a formalization of soundness and completeness results of unravelings. We used these results to certify quasi-reductiveness proofs by AProVE [3] and conditional confluence proofs by ConCon [17]. As a test bench we used all 3DCTRSs from Cops (problems 1–438) and TPDB 9.0,[5] duplicates removed. In this way we obtained 85 problems from Cops and 31 problems from TPDB.

AProVE produces termination proofs for 84 input problems, and CeTA could certify these termination proofs for 83 problems. ConCon could prove confluence for 58 problems, and nonconfluence for 28 problems. CeTA could certify 38 confluence proofs. Around 17 % of the confluence proofs of ConCon required sharing of U symbols. All proofs that CeTA could not certify contain some techniques which are not yet formalized. Detailed experimental results are provided on the website.

In summary, we consider our contribution threefold. On the *formalization* side, we provided to the best of our knowledge the first formalization framework for conditional rewriting and unravelings. Besides basic definitions it comprises the crucial soundness and completeness results for the wide class of standard

[5] See `http://cops.uibk.ac.at/` and `http://termination-portal.org/wiki/TPDB`

unravelings. *Theoretically,* we contribute a comprehensive proof for soundness of standard unravelings. It is based on [12, Theorem 3.8], but we could generalize it in several respects. *Practically,* we provide a certifier for CTRSs. It is able to certify quasi-decreasingness for all but one of the proofs generated by AProVE, and it confirms 65% of the examples where ConCon claims confluence.

Potential future work includes the integration of further (non)confluence techniques or termination techniques for CTRSs into IsaFoR.

References

1. F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.
2. F. Durán, S. Lucas, J. Meseguer, C. Marché, and X. Urbain. Proving termination of membership equational programs. In *Proc. PEPM 2004*, pages 147–158, 2004.
3. J. Giesl, M. Brockschmidt, F. Emmes, F. Frohn, C. Fuhs, C. Otto, M. Plücker, P. Schneider-Kamp, T. Ströder, S. Swiderski, and R. Thiemann. Proving termination of programs automatically with AProVE. In *Proc. 7th IJCAR*, volume 8562 of *LNCS*, pages 184–191, 2014.
4. K. Gmeiner, N. Nishida, and B. Gramlich. Proving confluence of conditional term rewriting systems via unravelings. In *Proc. IWC 2013*, pages 35–39, 2013.
5. B. Gramlich. Abstract relations between restricted termination and confluence properties of rewrite systems. *Fundamenta Informaticae*, 24:3–23, 1995.
6. S. Lucas, C. Marché, and J. Meseguer. Operational termination of conditional term rewriting systems. *IPL*, 95(4):446–453, 2005.
7. M. Marchiori. Unravelings and ultra-properties. In *Proc. ICLP 1996*, volume 1139 of *LNCS*, pages 107–121, 1996.
8. M. Marchiori. On deterministic conditional rewriting. Technical Report Computation Structures Group Memo 405, MIT, 1997.
9. J. Nagele and R. Thiemann. Certification of confluence proofs using CeTA. In *Proc. 3rd IWC*, pages 19–23, 2014.
10. T. Nipkow, L.C. Paulson, and M. Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer, 2002.
11. N. Nishida. *Transformational Approach to Inverse Computation in Term Rewriting.* PhD thesis, Nagoya University, 2004.
12. N. Nishida, M. Sakai, and T. Sakabe. Soundness of unravelings for conditional term rewriting systems via ultra-properties related to linearity. *LMCS*, 8(3):1–49, 2012.
13. E. Ohlebusch. Transforming conditional rewrite systems with extra variables into unconditional systems. In *Proc. LPAR 1999*, volume 1705 of *LNCS*, pages 111–130, 1999.
14. E. Ohlebusch. Termination of logic programs: Transformational methods revisited. *AAECC*, 12(1–2):73–116, 2001.
15. E. Ohlebusch. *Advanced Topics in Term Rewriting.* Springer, 2002.
16. E. Ohlebusch, C. Claves, and C. Marché. TALP: A tool for the termination analysis of logic programs. In *Proc. 20th RTA*, volume 1833 of *LNCS*, pages 270–273, 2000.
17. T. Sternagel and A. Middeldorp. Conditional confluence (system description). In *Proc. 25th RTA*, volume 8560 of *LNCS*, 2014.
18. R. Thiemann and C. Sternagel. Certification of termination proofs using CeTA. In *Proc. 22nd TPHOLs*, volume 5674 of *LNCS*, pages 452–468, 2009.