Synchronizing Applications of the Parallel Moves Lemma to Formalize Confluence of Orthogonal TRSs in PVS

Ana Cristina Rocha Oliveira¹, André Luiz Galdino² and Mauricio Ayala-Rincón¹

¹ Grupo de Teoria da Computação, Departamentos de Ciência da Computação e Matemática
Univesidade de Brasília, Brasília D.F., Brazil
² Departamento de Matemática
Universidade Federal de Goiás - Campus Catalão, Goiânia, Brazil
anacrismarie@gmail.com, galdino@unb.br, ayala@unb.br

Abstract

A complete formalization in PVS of the theorem of confluence of orthogonal term rewriting systems is presented. The formalized proof uses the PVS theory trs maintaining its distinguishing feature of remaining close to textbook’s proofs. The proof is based on a formalization of the Parallel Moves Lemma. Auxiliary lemmas are given which use an inductive construction of the crucial positions of a term originating a parallel divergence. Classifying all these positions, by application of the parallel moves lemma to the crucial divergence subterms, the desired common term of joinability is built.

1 Introduction

The formalization of confluence of orthogonal TRSs consists of a theory called orthogonality that imports the PVS theory trs [GAR09], that is available in the NASA LaRC PVS library [trs13], and which includes formalizations of several rewriting results ranging from specification of basic rewriting notions and properties to more elaborated results such as the Critical Pair theorem [GAR10], confluence and modular properties of abstract reduction systems [GAR08] and completeness of first-order unification algorithms [AGdMAR11]. The theory orthogonality specifies notions such as Ambiguous?(E), Left Linear?(E), Orthogonal?(E) and parallel_reduction?(E), all them of interest for dealing with formalization of theorems about orthogonal TRS’s (see [ROAR13]).

Proofs of confluence of orthogonal TRSs have been known at least since Rosen’s seminal work [Ros73] which is based on the well-known Parallel Moves Lemma (for short, PML). This proof was adapted by Huet in [Hue80], for proving the confluence of left-linear and parallel closed TRSs that admit critical pairs joinable from left to right in a sole step of parallel reduction. To the best of our knowledge, the sole related formalization was developed very recently in Isabelle/HOL in [Thi12], where unlike orthogonality, weak orthogonality, that allows the existence of trivial critical pairs, is assumed. The chapter on orthogonality of [BKdV03] surveys different styles of proofs of confluence of orthogonal TRSs, that are not different in essence.

Our style of proof follows the inductive approach in [BN98] which depends on the analysis of properties of the parallel rewriting relation and the PML. In this analysis, the PML is applied for guaranteeing parallel joinability of each principal redex involved in a parallel divergence from a term s: u ⇔ s ⇔ v. These redices appear at positions π in which on the one side

*Work supported by FAPDF PRONEX 2009/00091-0 grant. First, second and third authors partially supported by a CAPES Ph.D. scholarship, an FAPEG research support grant and a CNPq research fellowship.
one step of rewriting and, on the other side one step of parallel reduction are applied: either
$u|_\pi \leftarrow t|_\pi \Rightarrow v|_\pi$ or $u|_\pi \leftarrow t|_\pi \rightarrow v|_\pi$, being $t|_\pi$ an instance of the left-hand side (lhs, for short) of
a rule (see Fig. 1). From our point of view this choice is very adequate, because the discipline
of formalization that guided the development of the theory trs, that is also the one desired for
orthogonality, is providing proofs that are as close as possible to textbook’s proofs.

Regarding a previous work in which the general lines of the formalization of this theorem
were presented [ROAR13], here we specifically report on the necessary analysis to
synchronize applications of the PML to terms in order to join the divergence terms in a parallel divergence.
This involves the construction of a sequence of dominating positions in which either the same
rule was applied or on the one side a rewriting rule was applied and on the other side a parallel
reduction was applied. Each term of the parallel divergence is obtained by simple rewriting
steps at sequences of disjunct positions, using associated sequences of substitutions and rules.
The theory is available at www.mat.unb.br/~ayala/publications.html.

2 Basic Notions and Definitions

Familiarity with rewriting notations and notions is assumed (c.f. [BN98, BKdV03]). Terms,
built from a given signature and a set of enumerable variables, are represented as trees and
positions of a term $t$ as sequences of naturals. For a position $\pi$ of a term $t$,
$\pi|_t$ denotes the subterm at position $\pi$ and parallel positions $\pi$ and $\pi'$ are sequences such that neither $\pi$
is a prefix of $\pi'$ nor $\pi'$ is a prefix of $\pi$. Given a TRS $R$, the rewriting relation is denoted as $\rightarrow_R$.

The inverse of $\rightarrow$ is denoted by $\leftarrow$ and syntactic equality by $\equiv$. The reflexive closure
of the relation $\rightarrow$ is denoted as $\rightarrow^=$ and the reflexive transitive closure as $\rightarrow^\ast$. Similarly,
$\ast\leftarrow$ will denote the reflexive transitive closure of $\leftarrow$. The relations of local divergence,
divergence and joinability are given by $\leftarrow \ast \rightarrow$, $\ast \leftarrow \ast \rightarrow$ and $\ast \rightarrow \ast \leftarrow$, respectively.

One says that $\rightarrow$ is confluent if $(\ast\leftarrow \ast\rightarrow) \subseteq (\rightarrow^\ast \ast\rightarrow)$; and that it has the
diamond property if $(\leftarrow \ast \rightarrow) \subseteq (\rightarrow \ast \leftarrow)$.

A rule $e = (l, r)$ is a pair of terms such that the lhs cannot be a variable and the variables
occurring in its right-hand side (rhs, for short) should appear in the lhs. A TRS is
given as a set of rules. The reduction relation $\rightarrow_E$ induced by a TRS $E$ is built as follows:
a term $s$ reduces to $t$, denoted as $s \rightarrow t$, if $s = s[\pi \leftarrow \text{lhs}(e)\sigma] \rightarrow_E s[\pi \leftarrow \text{rhs}(e)\sigma] = t$,
where, in general, $u[\pi \leftarrow v]$ denotes the term obtained from $u$ by replacing the subterm at
position $\pi$ of $u$ by the term $v$.

Another crucial relation is parallel reduction: one says that $s$ reduces in parallel to $t$, denoted
as $s \parallel t$, if there exist finite sequences of the same length $n \geq 0$, $\Pi := \pi_1, \ldots, \pi_n$; $\Sigma :=
\sigma_1, \ldots, \sigma_n$ and $\Gamma := \epsilon_1, \ldots, \epsilon_n$ of parallel positions of $s$, substitutions and rules, respectively,
such that: $\forall 1 \leq i \leq n : s|_{\pi_i} = \text{lhs}(\epsilon_i)\sigma_i$, and $t$ is obtained from $s$, by replacing all subterms
at positions in \( \Pi \) by \( t|_{\pi_i} = \text{rhs}(e_i)\sigma_i \). All this is summarized by the following notation:

\[
s \overset{\pi_1 \ldots \pi_n}{\xrightarrow{\sigma_1 \ldots \sigma_n}} t, \quad \text{where}, \quad \sigma_i = \text{rhs}(e_i), \quad \text{for} \quad 1 \leq i \leq n.
\]

For short, notation \( s \overset{\Pi}{\xrightarrow{\Sigma}} t \), where \( \Pi \) is a sequence of parallel positions of \( s \), rules and substitutions, respectively, as in the definition of parallel reduction.

By simple analysis one has that \( \rightarrow \subseteq \Rightarrow \subseteq \rightarrow^* \). Thus, \( \rightarrow^* = \Rightarrow^* \), from which proving the diamond property for \( \Rightarrow \) will provide a proof of confluence of \( \rightarrow \). Thus, the crucial result to be formalized is the theorem below.

**Theorem 2.1 (Orthogonality implies diamond property).** Let \( R \) be a TRS orthogonal. Then, the relation \( \Rightarrow \) has the diamond property.

Orthogonal TRSs have no critical pairs and are left-linear. The PML (see Fig. 1) states that for all instances of rules of an orthogonal system, say \( (l, r) \), if \( l\sigma \Rightarrow s \), then there exists a \( t \) such that \( r\sigma \Rightarrow t \leftarrow s \).

Essentially, the proof is based on the observation that since instances of lhs's of other rules can only overlap at variable positions of \( l \), then by left-linearity one has that \( s = l\sigma' \) for some substitution \( \sigma' \). Also, for all variables \( x \sigma \Rightarrow x\sigma' \). Thus, one has \( l\sigma \Rightarrow l\sigma' \) and \( r\sigma \Rightarrow r\sigma' \leftarrow l\sigma \).

In order to prove the diamond property of orthogonal TRSs (see Fig. 2), the structure of a parallel divergence should be stratified in such a way that crucial positions are chosen to apply either the PML or non ambiguity (inexistence of CPs). A parallel divergence from a term \( s \) through positions \( \Pi_1 \) and \( \Pi_2 \) correspondingly using \( \Sigma_1 \) and \( \Sigma_2 \)-instances of rules \( \Gamma_1 \) and \( \Gamma_2 \), has the form

\[
t_1 = s[\Pi_1 \leftarrow \text{rhs}(\Gamma_1)\Sigma_1] \Rightarrow s \Rightarrow s[\Pi_2 \leftarrow \text{rhs}(\Gamma_2)\Sigma_2] = t_2,
\]

where \( \Pi_i, \Gamma_i, \Sigma_i \), for \( i = 1, 2 \), are sequences of parallel positions of \( s \), rules and substitutions, respectively, as in the definition of parallel reduction.

To prove theorem 2.1, a term \( u \) should be built such that \( t_1 \Rightarrow u \Leftarrow t_2 \).

### 3 Formalization

The formalization of the Diamond Property of parallel reduction of orthogonal TRSs is done by induction on the length of crucial positions occurring in a parallel divergence. These positions are built through the specification of an inductive operator \( \text{Pos}_\text{Over}(\Pi_1, \Pi_2) \) that builds the
subsequence of positions from \( \Pi_1 \) that are parallel to all positions in \( \Pi_2 \) or that have positions in the sequence \( \Pi_2 \) below them. Thus, the crucial positions of a divergence are given by a sequence \( \Pi \) carefully constructed and corresponding to the sequence \( \text{Pos} \_\text{Over}(\Pi_1, \Pi_2) \cup \text{Pos} \_\text{Over}(\Pi_2, \Pi_1) \cup (\Pi_1 \cap \Pi_2) \), where by \( \cup \) and \( \cap \) of sequences one means the sequence obtained by concatenation and by including only common members, respectively. Intuitively, it is easy to check (see Fig. 2) that exactly the subterms at these positions are the ones modified in the parallel divergence and that joining the subterms at these positions of \( t_1 \) and \( t_2 \) will provide the joinability term \( u \). But synchronizing the one-step-parallel movements from the subterms at these positions of \( t_1 \) and \( t_2 \), that is essentially building the necessary premises to apply the PML, requires a great deal of technical work which corresponds to a significant part of the whole formalization.

To guarantee that these crucial positions \( \Pi \), as mentioned above, are the ones modified when a term \( s \) parallelly diverges to \( t_1 \) and \( t_2 \), the lemma \text{replace}_\text{par}_\text{pos}_\text{dominance} \) was proved. This lemma shows that if \( s \rightrightarrows t_i \) through reductions at positions \( \Pi_i \), for \( i = 1, 2 \) correspondingly, then one is able to write \( t_i \) as \( s[\Pi \leftarrow (t_i|_{\pi})_{\pi \in \Pi}] \). This is possible because for every position \( \pi' \) in \( \Pi_i \), there exists a position \( \pi \) in \( \Pi \) that is (above or) prefix of \( \pi' \), what is satisfied by \( \Pi \) indeed.

Regarding joinability of subterms at positions \( \pi \) in \( \Pi \) of \( t_1 \) and \( t_2 \), two cases are to be analyzed. Firstly, the subterms of \( t_1 \) and \( t_2 \) at a position \( \pi \) in \( \Pi_1 \cap \Pi_2 \) are easily joined in one step of parallel reduction because these subterms are identical since there are no critical pairs in an orthogonal TRS. Secondly, the lemma \text{divergence}_\text{in}_\text{Pos}_\text{Over} \) shows explicitly how the divergence in the subterms of \( s, t_1 \) and \( t_2 \) at a position \( \pi \) in \( \text{Pos} \_\text{Over}(\Pi_1, \Pi_2) \cup \text{Pos} \_\text{Over}(\Pi_2, \Pi_1) \) satisfies the conditions required by the PML. So subterms \( t_1|_{\pi} \) and \( t_2|_{\pi} \) are joinable in one step of parallel reduction too (see Fig 1).

So, by the discussion in the last paragraph, for all \( \pi \) in the sequence of crucial positions \( \Pi \), there exists \( u_\pi \) such that \( t_1|_{\pi} \rightrightarrows u_\pi \rightrightarrows t_2|_{\pi} \) whenever \( t_1 \rightrightarrows s \rightrightarrows t_2 \) through reductions at positions \( \Pi_1 \) and \( \Pi_2 \). A sequence of terms \( U := (u_\pi)_{\pi \in \Pi} \) is built such that replacing subterms of \( s \) at these positions gives the required term of parallel joinability: \( u = s[\Pi \leftarrow U] \). At this point it is necessary to stress that a great deal of effort was necessary to formalize the synchronization the positions, rules and substitutions of \( \Pi_i, \Gamma_i \) and \( \Sigma_i \), for \( i = 1, 2 \), involved in the construction of the terms \( u_\pi \) and in general in the construction of the joinability term \( u \).

Another important lemma to conclude the proof of diamond property of parallel reduction is \text{parallel}_\text{reduction}_\text{context} \), which was necessary because one cannot guarantee directly that, if \( t_1|_{\pi} \rightrightarrows u_\pi, \ \forall \pi \in \Pi \), then \( t_1 \rightrightarrows u \). The formalization of this lemma uses induction on the length of the sequence of crucial positions \( \Pi \) and, through it, is possible to conclude that \( t_1 = s[\Pi \leftarrow (t_1|_{\pi})_{\pi \in \Pi}] \rightrightarrows s[\Pi \leftarrow U] = u \rightrightarrows s[\Pi \leftarrow (t_2|_{\pi})_{\pi \in \Pi}] = t_2 \).

Excluding all these technical details necessary to adequately apply the PML, the formalization of confluence of orthogonal TRSs follows the sketch of proof presented in Section 6.4 of [BN98]. In its current status, the PVS \text{theory}_\text{orthogonality} \) has about 53000 lines of proofs and 770 lines of specification. It is worth mentioning that the proof file includes also typing information that substantially increases over the part strictly related with the formalization.

### 4 Related work and Conclusions

The PVS \text{theory}_\text{orthogonality} \) includes a complete formalization of the theorem of confluence of orthogonal TRSs which is based on the PML. Although the formalization follows the lines of textbook’s proofs such as the one given in [BN98], its development required a great deal of invisible effort that was necessary to adequately apply the PML. Several additional lemmas were formalized in order to prove that a parallel divergence can be structured as an ordered
sequence of crucial divergences from subterms of the term of divergence, from which instances of the hypotheses of the PML are detected. Then, applying the PML to these subterms one builds a general term of joinability in parallel. The formalization of the PML was finished obtaining in this way a complete formalization of the theorem of confluence of orthogonal TRSs.

Future developments and extensions are related with the usability of this formalization to check automatically confluence of functional specifications that follow the discipline of orthogonality. Also, an interesting investigation is related with formalization of confluence of several variants such as weak orthogonal TRSs and Church-Rosser theorems for variants of the \( \lambda \)-calculus. Adaptation of the proof style used here to the alternative definition of parallel reduction used in the short proof of confluence for variants of the \( \lambda \)-calculus in [Tak95], and extensible for orthogonal TRSs as it is done in the chapter on orthogonality in [BKdV03], is also of great interest. Other technologies of proof surveyed in [BKdV03] as the one based on developments [vO97] as well as strengthening the current result to the permutation equivalence [HL91], that were pertinently pointed out by the reviewers, deserve formalizations, but although parts of the current formalization can be reused, they will require formalization developments substantially different from the current one.

References


