Non-Disjoint Combination with Forward-Closed Theories
Serdar Erbatur, Andrew M. Marshall, Christophe Ringeissen

To cite this version:
Serdar Erbatur, Andrew M. Marshall, Christophe Ringeissen. Non-Disjoint Combination with Forward-Closed Theories. 31th International Workshop on Unification, UNIF 2017, Adrià Gascón; Christopher Lynch, Sep 2017, Oxford, United Kingdom. hal-01590782

HAL Id: hal-01590782
https://inria.hal.science/hal-01590782
Submitted on 20 Sep 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.
1 Introduction

Equational unification is the problem of solving equations in structures of terms modulo an equational theory. In general, equational unification is undecidable, but specialized techniques have been developed to solve the problem for particular classes of equational theories.

When the equational theory has the Finite Variant Property (FVP) \cite{4}, equational unification reduces to syntactic unification via the computation of finitely many variants of terms. Nowadays, equational theories with the FVP have attracted a considerable interest, especially for their applications in the analysis of security protocols \cite{2,5,10}.

When the equational theory is given by a convergent term rewrite system, the concept of narrowing is a generalization of rewriting, where the matching process is replaced by some (syntactic) unification problem. Narrowing is complete for equational unification, but it terminates only in some very particular cases. Hence, a particular narrowing strategy, called folding variant narrowing, is complete and terminating for any equational theory with the FVP \cite{10}.

When the equational theory is syntactic, it is possible to apply a mutation-based unification procedure \cite{11}. However, being syntactic is not a sufficient condition for a theory to admit a terminating mutation-based unification procedure. In the particular case of shallow theories, there exists a terminating mutation-based unification procedure \cite{3}.

Another important scenario is given by an equational theory defined as a union of component theories. To solve this case, it’s natural to proceed in a modular way and there are terminating and complete combination procedures for disjoint unions of theories \cite{16}. These combination procedures can be extended to some particular non-disjoint unions of theories, but it is difficult to identify cases where these procedures terminate \cite{6,15}.

In this paper we investigate the unification problem in equational theories involving forward-closed convergent term rewrite systems \cite{2}. In the class of forward-closed theories, unification is decidable and finitary since any convergent term rewrite system has a finite forward closure if and only if it has the FVP \cite{2}. Furthermore, forward-closed theories are syntactic theories admitting a terminating mutation-based unification procedure. We first demonstrate this result by showing that a mutation-based unification algorithm, originally developed for equational theories saturated by paramodulation \cite{13}, remains sound and complete for forward-closed theories. Building on this result we use the new mutation-based algorithm to develop an algorithm that solves the unification problem in unions of forward-closed theories with non-disjoint theories. The resulting algorithm can be viewed as a terminating instance of a procedure initiated for hierarchical combination \cite{7}.
2 Preliminaries

We assume the reader is familiar with equational unification and term rewriting systems [1]. An axiom $l = r$ is regular (also called variable-preserving) if $\text{Var}(l) = \text{Var}(r)$. An axiom $l = r$ is linear (resp., collapse-free) if $l$ and $r$ are linear (resp. non-variable terms). An equational theory is regular (resp., linear/collapse-free) if all its axioms are regular (resp., linear/collapse-free).

A theory $E$ is syntactic if it has a finite resolvent presentation $S$, that is a presentation $S$ such that each equality $t =_E u$ has an equational proof $t \leftrightarrow^*_S u$ with at most one step $\leftrightarrow_S$ applied at the root position. In the following, we often use tuples of terms, say $u = (u_1, \ldots, u_n)$.

An $E$-unification problem is a set of $\Sigma$-equations, $G = \{s_1 =^? t_1, \ldots, s_n =^? t_n\}$, or equivalently a conjunction of $\Sigma$-equations. The set of variables in $G$ is denoted by $\text{Var}(G)$. A solution to $G$, called an $E$-unifier, is a substitution $\sigma$ such that $s_i \sigma =_E t_i \sigma$ for all $1 \leq i \leq n$. A substitution $\sigma$ is more general modulo $E$ than $\theta$ on a set of variables $V$, denoted as $\sigma \leq^E \theta$, if there is a substitution $\tau$ such that $x \sigma \tau =_E x \theta$ for all $x \in V$. A Complete Set of $E$-Unifiers of $G$ is a set of substitutions denoted by $\text{CSU}_E(G)$ such that each $\sigma \in \text{CSU}_E(G)$ is an $E$-unifier of $G$, and for each $E$-unifier $\theta$ of $G$, there exists $\sigma \in \text{CSU}_E(G)$ such that $\sigma \leq^E \theta$.

Let $E$ be an equational $\Sigma$-theory such that $\Sigma = \Sigma_1 \cup \Sigma_2$ and $\Sigma_1 \cap \Sigma_2 = \emptyset$. $\Sigma_i$-terms (including the variables) and $\Sigma_i$-equations (including the equations between variables) are called $i$-pure. An $E$-unification problem is in separate form if it is a conjunction $G_1 \land G_2$, where $G_i$ is a conjunction of $\Sigma_i$-equations for $i = 1, 2$. A term is called a $\Sigma_i$-rooted term if its root symbol is in $\Sigma_i$. An alien subterm of a $\Sigma_i$-rooted term $t$ is a $\Sigma_j$-rooted subterm $s (i \neq j)$ such that all superterms of $s$ are $\Sigma_i$-rooted. A TRS is $i$-rooted if all its left-hand sides and right-hand sides are $\Sigma_i$-rooted. We define general $E$-unification as the unification problem in the equational theory obtained by extending $E$ with arbitrary free function symbols.

Let us now define the notion of forward-closure [2]. For a given convergent TRS $R$, assume a reduction ordering $< \subset$ such that $r < l$ for any $l \rightarrow r \in R$ and $< \subset$ is total on ground terms. Since (rewrite) rules are multisets of two terms, the multiset extension of $<$ leads to an ordering on rules, also denoted by $<$, which is total on ground instances of rules. A rule $\rho$ is strictly redundant in $R$ if any ground instance $\rho \sigma$ of $\rho$ follows from ground instances of $R$ that are strictly smaller w.r.t $< \subset \rho \sigma$. A rule $\rho$ is redundant in $R$ if $\rho$ is strictly redundant in $R$ or $\rho$ is an instance of some rule in $R$. A TRS $R$ is forward-closed if any Forward inference (cf. Figure 1) with premises in $R$ generates a rule which is redundant in $R$.

\begin{center}
\begin{tabular}{l}
\textbf{Forward} & $g \rightarrow d[l']$ & $l \rightarrow r \vdash (g \rightarrow d[r])\sigma$ & where $\sigma = \text{mgu}(l, l')$ and $l'$ is not a variable.
\end{tabular}
\end{center}

Figure 1: Forward inference

3 Unification in Forward-Closed Rewrite Systems

We present a rule-based unification procedure for any forward-closed TRS. We basically reuse the unification procedure initially developed for any equational theory saturated by paramod-
ulation [13]. This procedure implements Basic Syntactic Mutation (BSM) by extending syntactic unification with some additional mutation rules (rules whose names include Mut in Figures 2 and 3) and cycle breaking rules (rules whose names include Cycle in Figure 3). These additional rules are applied in a don’t know non-deterministic way. Thus, the resulting BSM unification procedure is similar to the mutation-based unification procedures designed for syntactic theories [12, 14]. However, these mutation-based procedures are not terminating, whereas the BSM unification procedure always terminates. To get termination, the BSM rules depicted in Figures 2 and 3 make use of boxed terms. This particular annotation of terms works as follows: Subterms of boxed terms are also boxed, terms boxed in the premises of an inference rule remain boxed in the conclusion, and when the “box” status of a term is not explicitly given in an inference rule, it can be either boxed or unboxed. Given a unification problem G and an R-normalized substitution σ, (G, σ) is said to be R-normalized if tσ is R-normalized whenever t is boxed in G. For a forward-closed convergent TRS R, the set of equalities S used in Figures 2 and 3 is defined as being equal to RHS(R) = R = G = Gσ l → r ∈ R, g → d ∈ R, σ ∈ mgu(r,d), lσ ̸= gσ}, where R = {l → r | l → r ∈ R}.

**Figure 2: BSM rules**

Given an R-unification problem G, the BSM unification procedure works as follows: apply the BSM rules (Figures 2 and 3) on G until reaching normal forms. The procedure then only returns those sets of equations which are in dag solved form.

**Theorem 1.** If R is a forward-closed convergent TRS, then the BSM unification procedure provides an R-unification algorithm.

## 4 Forward-Closed Combination

In previous papers [7,8], we have studied a form of non-disjoint combination, called hierarchical combination, which is defined as a convergent TRS R₁ combined with a base theory E₂. The TRS R₁ must satisfy some properties to ensure that E = R₁ ∪ E₂ is a conservative extension of E₂. We are interested in combined theories E where it is possible to reduce any E-equality between two terms (s =ₚ t) into the E₂-equality of their R₁-normal forms (s ↓ R₁ = E₂ t ↓ R₁). Below, we assume that R₁ is forward-closed.
Example 1. Consider \( \Sigma \) equational \( R \)-theory. An FC-combination \( \Sigma \)-collapse-free \( u \) is true. Either, 

Lemma 1. \( \text{Lemma of equalities} S \) does not apply since \( \Sigma S \subset BSM \) We study how the 5 Unification Procedure for Forward-Closed Combination rules in Figures 2 and 3, parameterized by \( E \) and \( f \) are applied only if the input is in separate form, and by matching only \( \Sigma 1 \)-equations.

Lemma 2. Given an \( E \)-unification problem \( G \) as input, the repeated application of \( BSC \) rules always terminates and computes a set of normal forms in separate form denoted by \( BSC(G) \).
Following Lemma 2, the BSC unification procedure works as follows: apply the BSC rules on a given $E$-unification problem $G$ until reaching normal forms, and return all the dag solved forms in $\text{BSC}(G)$. The completeness of the BSC unification procedure relies on the lemma given below. First, we state that an $E_2$-unification algorithm can be reused without loss of completeness to $E$-unify any conjunction of $\Sigma_2$-equations. This is a classical result, already used in hierarchical combination [7], which can be easily lifted to FC-combination.

| VA | $\{s = t[u]\} \cup G \vdash \{s = t[x], x = u\} \cup G$  
where $u$ is an alien subterm of $t$, $x$ is a fresh variable, and $u$ is boxed iff $t[u]$ is boxed.  
| IE | $\{s = t\} \cup G \vdash \{x = s, x = t\} \cup G$  
where $s$ is a non-variable $\Sigma_1$-term, $t$ is a non-variable $\Sigma_2$-term and $x$ is a fresh variable.  
| Solve2 | $G_1 \land G_2 \vdash \bigvee_{\sigma \in \text{CSU}_{E_2}(G_2)} G_1 \land \hat{\sigma}_2$  
if $G_2$ is $E_2$-unifiable and unsolved, and no other rule applies. |

Figure 4: Additional Rules for the combination with $E_2$

**Lemma 3** (Completeness). If $\sigma$ is an $E$-unifier of $G$, $(G, \sigma)$ is $R_1$-normalized, and $G$ is not a separate form in dag solved form, then there exist some $G'$ and a substitution $\sigma'$ such that $G'$ is obtained from $G$ by applying some BSC rule, $\sigma'$ is an $E$-unifier of $G'$, $(G', \sigma')$ is $R_1$-normalized, and $\sigma' \preceq_{E}^{\text{var}(G)} \sigma$.

According to Lemmas 2 and 3, we can conclude that BSC leads to a terminating and complete $E$-unification procedure: given an $E$-unification problem, the set of dag solved forms in $\text{BSC}(G)$ provides a $\text{CSU}_{E}(G)$. Then, this $E$-unification algorithm can be lifted to a general $E$-unification algorithm by assuming that $E_2$ includes the free symbols.

**Theorem 2.** Given any layer-preserving FC-combination $(E_1, E_2)$ and an $E_2$-unification algorithm, BSC provides a general $E_1 \cup E_2$-unification algorithm.

For sake of simplicity, we restrict us in this short paper to layer-preserving FC-combinations, where all conflicts between component theories have no solution just like in disjoint unions of regular and collapse-free theories [17]. The general case of arbitrary FC-combinations, where the TRS $R_1$ may contain non-regular or collapse axioms, will be addressed in a full version [9]. In the general case, we will investigate the possibility of considering a single mutation rule dedicated to equations between a variable and a $\Sigma_1$-rooted term.

## 6 Connection with the Finite Variant Property

The computation of finite variants [4,10] is another way to reduce any unification problem modulo $E = R_1 \cup E_2$ into some $E_2$-unification problems with free function symbols. Thus, there exists an interesting connection between the finite variant property and FC-combinations. It can be shown that a brute force method can be used to solve $E$-unification: compute all the finitely many $R_1$-variants of an input $E$-unification problem, and solve them by general $E_2$-unification, usually implemented by combining $E_2$-unification and syntactic unification. This is a highly non-deterministic method. The brute force approach of computing all variants can be prohibitive due to the possible large number of variants and thus it is desirable to have alternatives to that approach. From our point of view, the approach described in Section 5 provides an interesting alternative where all the non-determinism is managed inside the combination procedure, when mutation rules and Solve2 have to be applied.
References