Non-disjoint Combined Unification and Closure by Equational Paramodulation (Extended Version)

Serdar Erbatur, Andrew M Marshall, Christophe Ringeissen

Non-disjoint Combined Unification and Closure by Equational Paramodulation

(Extended Version)

Serdar Erbatur[1], Andrew M. Marshall[2], and Christophe Ringeissen[3]

[1] University of Texas at Dallas, Richardson, USA
[2] University of Mary Washington, Fredericksburg, USA
[3] Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

Abstract. Closure properties such as forward closure and closure via paramodulation have proven to be very useful in equational logic, especially for the formal analysis of security protocols. In this paper, we consider the non-disjoint unification problem in conjunction with these closure properties. Given a base theory E, we consider classes of theory extensions of E admitting a unification algorithm built in a hierarchical way. In this context, a hierarchical unification procedure is obtained by extending an E-unification algorithm with some additional inference rules to take into account the rest of the theory. We look at hierarchical unification procedures by investigating an appropriate notion of E-constructed theory, defined in terms of E-paramodulation. We show that any E-constructed theory with a finite closure by E-paramodulation admits a terminating hierarchical unification procedure. We present modularity results for the unification problem modulo the union of E-constructed theories sharing only symbols in E. Finally, we also give sufficient conditions for obtaining terminating (combined) hierarchical unification procedures in the case of regular and collapse-free E-constructed theories.

1 Introduction

Unification plays a central role in all logic-based tools using the resolution principle, for instance to perform new deductions using superposition and paramodulation inferences implemented in equational provers. Both superposition and paramodulation aim at deducing a new equality from two equalities that can overlap via (syntactic) unification. In this context, a syntactic unification algorithm computing a most general unifier is ubiquitous. More generally, we may consider equational unification, where the problem is defined modulo an equational theory E, such as the famous example of Associativity-Commutativity. Equational unification, called E-unification, is undecidable in general, but unification algorithms are known for particular classes, like for instance: (1) the class SH of shallow theories [8] defined by axioms whose variables can occur at depth at most 1; (2) the class PC of theories with a finite paramodulation closure [20]; (3) the class FVP of theories defined by convergent term rewrite

systems with the Finite Variant Property [9,16]. FVP and PC can be related since FVP coincides with the class FC of theories with a finite forward closure [6], a particular closure similar to paramodulation closure but dedicated to convergent terms rewrite systems. SH, PC, and FVP are particular classes of syntactic theories (see respectively [8], [20], [11]). When a theory is syntactic [19,24], it is possible to apply a rule-based unification procedure extending the one known for syntactic unification with some additional mutation rules. In general, being syntactic is not a sufficient condition to ensure the termination of this unification procedure. Fortunately, SH, PC, and FVP admit terminating instances of this mutation-based unification procedure (see respectively [8], [20], [11]).

In many practical applications, E is a component in a union of theories, say $F \cup E$. In that case, it is quite natural to solve the $F \cup E$-unification problem in a modular way thanks to the unification algorithms known for F and for E. There are terminating and complete combination procedures when F and E have disjoint signatures [26,3]. These combination procedures can be extended to some non-disjoint unions of theories sharing only constructor symbols, but it is quite difficult to identify particular cases where these procedures terminate [25,10]. A terminating case has been identified in [5] by investigating a notion of *bounded* theory over the constructor symbols. More recently, a hierarchical unification approach [12,11,15] has been initiated when $F \cup E$-unification can be considered as a conservative extension of E-unification while some symbols of E may occur as constructors in F. In that scenario, hierarchical unification consists in using an E-unification algorithm plus some mutation-based unification procedure to manage the remaining part of $F \cup E$. In [15], we have shown that the hierarchical unification approach is particularly well-suited to tackle E-convergent term rewrite systems in which all the symbols in E are constructors. In particular, it is possible to get a terminating hierarchical unification procedure when such constructed-based rewrite system has a finite forward closure [11].

In this paper, we investigate the possible use of hierarchical unification for a class of theories defined via an E-paramodulation closure, where E-paramodulation generalizes the classical paramodulation inference by replacing syntactic unification with E-unification. In that direction, we introduce the notion of E-syntacticness, a useful property to study a possible mutation-based unification procedure modulo the base theory E. To obtain a complete hierarchical unification procedure, it is required that the E-unification algorithm is applicable without loss of completeness to solve any $F \cup E$-unification problem expressed over the signature of E. To fulfill this requirement, we introduce the class of E-constructed theories. These theories are defined using E-paramodulation and generalize the E-convergent term rewrite systems for which all the symbols of E are constructors. The class of E-constructed theories is particularly interesting in the context of non-disjoint combination. Actually, a union of E-constructed theories sharing only E is a union of non-disjoint theories without any overlap between the component theories. We study two classes of E-constructed theories: (i) a class of regular collapse-free E-constructed theories F such that $F \cup E$ ad-

mits a hierarchical unification algorithm; (ii) the class of E-constructed theories closed by E-paramodulation. We show the following modularity result: let $\mathcal{C}$ be any class (i) or (ii), if F_1 and F_2 are two theories in $\mathcal{C}$ sharing only the symbols in E, then $F_1 \cup F_2$ is a theory in $\mathcal{C}$. In both cases, there exists a hierarchical unification algorithm for $F_1 \cup F_2 \cup E$. Compared to [15], we consider equational theories that are not necessarily presented by E-convergent term rewrite systems, and we go beyond the subterm collapse-free assumption of [15]. For example, in the class (i) the combined hierarchical unification algorithm applies without loss of completeness to theories that are assumed to be regular and collapse-free but not necessarily subterm collapse-free. The regularity and the collapse-freeness of a theory is trivially checked by examining its axioms, while the subterm collapse-freeness is a property that can be difficult to check.

Motivating Examples from Security Protocols. Let us consider a theory used in practice to model a group messaging protocol [7]. For this protocol, the theory modeling the intruder can be defined [23] as a combination $R^{=}_{ENC} \cup K$ where $K = \{keyexch(x, pk(x'), y, pk(y')) = keyexch(x', pk(x), y', pk(y))\}$, and

$$R^{=}_{ENC} = \left\{ \begin{array}{rr} adec(aenc(m, pk(sk)), sk) = m & getmsg(sign(m, sk)) = m \\ checksign(sign(m, sk), m, pk(sk)) = ok & sdec(senc(m, k), k) = m \end{array} \right\}$$

The equational theories $R^{=}_{ENC}$ and K share the absolutely free constructor pk and they are both closed by paramodulation. Thanks to a modularity result developed in this paper, we can show that $R^{=}_{ENC} \cup K$ is closed by paramodulation too. Thus, $R^{=}_{ENC} \cup K$ admits a (hierarchical) unification algorithm.

Let us now consider a theory for dealing with member keys in a group of users and an overall group key [21]. Member keys can be kept in a tree like structure with the group key being the root. A *pick* function is included to retrieve the group key. In [21], the group is modeled thanks to a constructor with some equational properties, ideally a set union operator. Here, we consider $E_1 = \{pick(x, tree(y, x \cup m)) = y, add(x, tree(y, m)) = tree(y, x \cup m)\}$ where $\cup$ is an AC-constructor used to build multisets. This theory is closed by AC-paramodulation, and so it admits a hierarchical unification algorithm built over an AC-unification algorithm. To model homomorphic encryption or exponentiation, we can use axioms such as $e(x * y, z) = e(x, z) * e(y, z)$ and $e(e(x, y), z) = e(x, y \circledast z)$, where $\circledast$ is an AC-symbol. In [15], it has been shown that two distributive theories including these axioms admit a hierarchical unification algorithm. These regular and collapse-free theories satisfy the assumptions needed to get a terminating combined unification procedure.

Outline. After this introduction and the next section on preliminaries, the paper is organized as follows. Section 3 presents the E-paramodulation closure and then the E-constructed theories. In Section 4, we introduce the notion of E-syntacticness. In Section 5, a hierarchical unification procedure is given as a rule-based system including some classical purification rules, an E-unification algorithm encapsulated in a solving rule, plus a couple of mutation rules. The

unification problem and the related modularity properties are investigated in Section 6 for the class (i) and in Section 7 for the class (ii).

2 Preliminaries

We use the standard notation of equational unification [4] and term rewriting systems [1]. Given a first-order signature Σ and a (countable) set of variables V, the set of Σ-terms over variables V is defined in the usual way. The set of variables in a term t is denoted by $Var(t)$. A term t is *ground* if $Var(t) = \emptyset$. For any position p in a term t (including the root position ϵ), $t(p)$ is the symbol at position p, $t|_p$ is the subterm of t at position p, and $t[u]_p$ is the term t in which $t|_p$ is replaced by u. A substitution is an endomorphism of the Σ-structure of terms over V such that only finitely many variables are not mapped to themselves, denoted by $\sigma = \{x_1 \mapsto t_1, \ldots, x_m \mapsto t_m\}$, where the domain and the range of σ are respectively $Dom(\sigma) = \{x_1, \ldots, x_m\}$ and $Ran(\sigma) = \{t_1, \ldots, t_m\}$. Application of a substitution σ to t is written $t\sigma$.

Equational Theories. Given a set E of Σ-axioms (i.e., pairs of Σ-terms, denoted by $l = r$), the *equational theory* $=_E$ is the congruence closure of E under the law of substitutivity (by a slight abuse of terminology, E is often called an equational theory). Equivalently, $=_E$ can be defined as the reflexive transitive closure $\leftrightarrow_E^*$ of an equational step $\leftrightarrow_E$ defined as follows: $s \leftrightarrow_E t$ if there exist a position p of s, $l = r$ (or $r = l$) in E, and substitution σ such that $s|_p = l\sigma$ and $t = s[r\sigma]_p$. An axiom $l = r$ is *regular* if $Var(l) = Var(r)$. An axiom $l = r$ is *collapse-free* if l and r are non-variable terms. An equational theory is *regular* (resp., collapse-free) if all its axioms are regular (resp., collapse-free). A term t is *subterm collapse-free modulo* E if it is not the case that $t =_E u$ where u is any strict subterm of t. An equational theory E is *subterm collapse-free* if for any term t, t is subterm collapse-free modulo E.

A theory E is *syntactic* if it has a finite *resolvent presentation* S, defined as a finite set of axioms S such that each equality $t =_E u$ has an equational proof $t \leftrightarrow_S^* u$ with at most one equational step $\leftrightarrow_S$ applied at the root position. One can easily check that $C = \{x * y = y * x\}$ (Commutativity) and $AC = \{x*(y*z) = (x*y)*z,\ x*y = y*x\}$ (Associativity-Commutativity) are regular, collapse-free, and linear (variables occur only once). Moreover, C and AC are syntactic [19]. An axiom $l = r$ is *shallow* if variables can only occur at a position at depth at most 1 in both l and r. An equational theory is *shallow* if all its axioms are shallow. For example, C is shallow, but A is not. It has been shown in [8] that shallow theories are syntactic.

Equational Unification. A Σ-equation is a pair of Σ-terms denoted by $s =^? t$ or simply $s = t$ when it is clear from the context that we do not refer to an axiom. A *flat* Σ-equation is either an equation between variables or a *non-variable flat* Σ-equation of the form $x_0 = f(x_1, \ldots, x_n)$ where $x_0, x_1, \ldots, x_n$ are variables and f is a function symbol in Σ. An E-unification problem is a set of Σ-equations,

$G = \{s_1 =^? t_1, \ldots, s_n =^? t_n\}$, or equivalently a conjunction of Σ-equations. The set of variables in G is denoted by $Var(G)$. A solution to G, called an *E-unifier*, is a substitution σ such that $s_i\sigma =_E t_i\sigma$ for all $1 \leq i \leq n$, written $E \models G\sigma$. A substitution σ is *more general modulo* E than θ on a set of variables V, denoted as $\sigma \leq_E^V \theta$, if there is a substitution τ such that $x\sigma\tau =_E x\theta$ for all $x \in V$. $\sigma|_V$ denotes the substitution σ restricted to the set of variables V. A *Complete Set of E-Unifiers* of G, denoted by $CSU_E(G)$, is a set of substitutions such that each $\sigma \in CSU_E(G)$ is an E-unifier of G, and for each E-unifier θ of G, there exists $\sigma \in CSU_E(G)$ such that $\sigma \leq_E^{Var(G)} \theta$. An *E-unification algorithm* is an algorithm that computes a finite $CSU_E(G)$ for all E-unification problems G. An inference rule $G \vdash G'$ for E-unification is *sound* if each E-unifier of G' is an E-unifier of G; and *complete* if for each E-unifier σ of G, there exists an E-unifier σ' of G' such that $\sigma' \leq_E^{Var(G)} \sigma$. An inference system for E-unification is *sound* if all its inference rules are sound; and *complete* if for each E-unification problem G on which an inference applies and each E-unifier σ of G, there exist an E-unification problem G' inferred from G and an E-unifier σ' of G' such that $\sigma' \leq_E^{Var(G)} \sigma$. Thus, the set of E-unifiers is preserved by a sound and complete inference system for E-unification. The definition of complete inference system adopted here allows us to take into account the rules that need to be applied with a don't know nondeterministic choice in order to preserve the set of E-unifiers. When a don't know nondeterminism is necessary to apply some rules, we mention it explicitly. By default, the inference rules are applied using a don't care nondeterminism: when several rules are applicable, it is sufficient to apply one of them.

A set of equations $G = \{x_1 =^? t_1,\ \ldots,\ x_n =^? t_n\}$ is said to be in *tree solved form* if each x_i is a variable occurring once in G. Given an idempotent substitution $\sigma = \{x_1 \mapsto t_1,\ \ldots,\ x_n \mapsto t_n\}$ (such that $\sigma\sigma = \sigma$), $\hat{\sigma}$ denotes the corresponding tree solved form. A set of equations is said to be in *dag solved form* if they can be arranged as a list $x_1 =^? t_1,\ \ldots,\ x_n =^? t_n$ where (a) each left-hand side x_i is a distinct variable, and (b) $\forall\, 1 \leq i \leq j \leq n$: x_i does not occur in t_j. A set of equations $\{x_1 =^? t_1,\ \ldots,\ x_n =^? t_n\}$ is a *cycle* if for any $i \in [1, n-1], x_{i+1} \in Var(t_i)$, $x_1 \in Var(t_n)$, and there exists $j \in [1, n]$ such that t_j is not a variable. Given two disjoint signatures Σ_0 and Σ_1 and any $i = 1, 0$, Σ_i-terms (including the variables) and Σ_i-equations (including the equations between variables) are called *Σ_i-pure*. A term t is called a *Σ_i-rooted* term if its root symbol is in Σ_i. An *alien* subterm of a Σ_i-rooted term t is a Σ_j-rooted subterm s of t ($i \neq j$) such that all superterms of s are Σ_i-rooted. Given a Σ_0-theory E, a theory $F \cup E$ is a *conservative extension* of E if $=_{F\cup E}$ and $=_E$ coincide on Σ_0-terms. When $F \cup E$ is a conservative extension of E, E-unification is said to be *complete for solving the Σ_0-fragment of $F \cup E$-unification* if for any Σ_0-pure $F \cup E$-unification problem G, any $CSU_E(G)$ is a $CSU_{F\cup E}(G)$. If F and E have disjoint signatures, E-unification is known to be complete for solving the Σ_0-fragment of $F \cup E$-unification.

Equational Rewrite Relations. Given a signature Σ, an oriented Σ-axiom is called a rewrite rule of the form $l \to r$ if l is not a variable and $Var(r) \subseteq Var(l)$. Given a set R of rewrite rules and an Σ-equational theory E, A term s R,E-*rewrites* to a term t, denoted by $s \to_{R,E} t$, if there exist a position p of s, $l \to r \in R$, and substitution σ such that $s|_p =_E l\sigma$ and $t = s[r\sigma]_p$. The term s is said to be R,E-*reducible*, and $s|_p$ is called a *redex*. The symmetric relation $\leftarrow_{R,E} \cup \to_{R,E} \cup =_E$ is denoted by $\longleftrightarrow_{R\cup E}$. The rewrite relation $\to_{R,E}$ is Church-Rosser modulo E if $\longleftrightarrow^*_{R\cup E}$ is included in $\to^*_{R,E} \circ =_E \circ \leftarrow^*_{R,E}$. When $=_E \circ \to_{R,E} \circ =_E$ is terminating, the following properties are equivalent [17]: (1) $\to_{R,E}$ is Church-Rosser modulo E; (2) for any terms t, t', $t \longleftrightarrow^*_{R\cup E} t'$ if and only if $t\downarrow =_E t'\downarrow$, where $t\downarrow$ (resp., $t'\downarrow$) denotes any normal form w.r.t $\to_{R,E}$ of t (resp., t'). The rewrite relation $\to_{R,E}$ is E-*convergent* if $=_E \circ \to_{R,E} \circ =_E$ is terminating and $\to_{R,E}$ is Church-Rosser modulo E. A function symbol that does not occur in $\{l(\epsilon) \mid l \to r \in R\}$ is called a *constructor* for R. Let Σ_0 be the subsignature of Σ that consists of all function symbols occurring in the axioms of E. An E-convergent rewrite relation $\to_{R,E}$ is said to be E-*constructed* if all symbols in Σ_0 are constructors for R. When $\to_{R,E}$ is clear from the context, a normal form w.r.t $\to_{R,E}$ is said to be *normalized*. A substitution σ is *normalized* if, for every variable x in the domain of σ, $x\sigma$ is normalized. An instance $l\sigma \to r\sigma$ of a rule $l \to r \in R$ is a *right-reduced* instance if $\sigma_{|Var(r)}$ is normalized. A term t is an *innermost redex* if no subterm of t is a redex. An E-convergent $\to_{R,E}$ is *IR1* if every innermost redex is R,E-reducible to a normal form in one step.

When R is a finite set of rules, the pair (R,E) is called an *equational term rewrite system* (TRS). We say that a property is satisfied by an equational TRS (R,E) if this property is satisfied by $\to_{R,E}$. Given a TRS (R,E), $R^=$ denotes the set of equalities $\{l = r \mid l \to r \in R\}$, and $R^= \cup E$ is the *equational theory of* (R,E). For sake of brevity, we may use $R \cup E$ instead of $R^= \cup E$.

To simplify the notation, we often use tuples of terms, like $\bar{u} = (u_1, \ldots, u_n)$, $\bar{v} = (v_1, \ldots, v_n)$. Applying a substitution σ to $\bar{u}$ is the tuple $\bar{u}\sigma = (u_1\sigma, \ldots, u_n\sigma)$. The tuples $\bar{u}$ and $\bar{v}$ are said to be E-equal, denoted by $\bar{u} =_E \bar{v}$, if $u_1 =_E v_1, \ldots, u_n =_E v_n$. Similarly, $\bar{u} \to^*_R \bar{v}$ if $u_1 \to^*_R v_1, \ldots, u_n \to^*_R v_n$, $\bar{u}$ is normalized if $u_1, \ldots, u_n$ are normalized, and $\bar{u} =^? \bar{v}$ is $\{u_1 =^? v_1, \ldots, u_n =^? v_n\}$.

3 Closure by Equational Paramodulation

From now on, let E be a regular and collapse-free Σ_0-theory, and F a Σ-theory such that $\Sigma_0 \subseteq \Sigma$. We assume a reduction ordering $>$ on terms such that $>$ is E-compatible, meaning that $s' =_E s > t =_E t'$ implies $s' > t'$. It is important to note that a single reduction ordering $>$ is used even in the context of a union of theories. In that case, $>$ is assumed to be defined on terms built over the combined signature. Given a set of equalities F, $Gr(F)$ denotes the set of ground instances of F. A set F of ground equalities is $>$-*orientable* if each equality in F can be oriented into a rule $l \to r$ such that $l > r$ and l is $\Sigma\backslash\Sigma_0$-rooted. A set F of equalities is $>$-*orientable* if $Gr(F)$ is $>$-orientable. A ground equality $s = t$ is *optimally joinable* w.r.t a $>$-orientable set F of ground

equalities if for $F^{>} = \{l \to r \mid l > r, l = r \text{ or } r = l \text{ in } F\}$ there exists a rewrite proof $s \to^*_{F^{>},E} s' =_E t' \leftarrow^*_{F^{>},E} t$ for which each rewrite step $u \to_{F^{>},E} v$ in $s \to^*_{F^{>},E} s'$ and in $t \to^*_{F^{>},E} t'$ is applied at a position p such that $u|_p$ is an innermost redex and $v|_p$ is in normal form w.r.t $\to_{F^{>},E}$. An equality $s = t$ is *optimally joinable* w.r.t a $>$-orientable set F of equalities if each ground instance of $s = t$ is optimally joinable w.r.t $Gr(F)$. Given a finite set of equalities F, the *E-paramodulation closure* of F is inductively defined as follows as a partial function:

— If F is $>$-orientable, then $PC^0(F) = F$; otherwise $PC^0(F)$ is undefined.

— For any $k \geq 0$, assume $PC^k(F)$ is defined. Let PE be the set of all equalities e obtained by:

> E-**Paramodulation** $g = d[l'],\ l = r \ \vdash\ (g = d[r])\sigma$
> where l' is not a variable, $\sigma \in CSU_E(l' =^? l)$, and $l\sigma \not< r\sigma$

using premises in $PC^k(F)$ and such that e is not optimally joinable w.r.t $PC^k(F)$. If PE is $>$-orientable, then $PC^{k+1}(F) = PC^k(F) \cup PE$; otherwise $PC^{k+1}(F)$ is undefined. If $PC^k(F)$ is defined for any $k \geq 0$, then $PC(F) = \bigcup_{k\geq 0} PC^k(F)$; otherwise $PC(F)$ is undefined.

Example 1. Consider the equational theory $E_2 = \{rm(x, x \cup m) = m\}$ where $\cup$ is an AC-symbol. Notice that the left-to-right orientation of E_2 provides an AC-compatible reduction ordering for which we have $PC(E_2) = E_2$ because there is no non-variable overlap between a left-hand side of a rule and a right-hand side.

Definition 1 (E-constructed theory). *Let E be a regular and collapse-free theory. A finite set of equalities F is said to be an E-*constructed theory *if there exists an E-compatible reduction ordering $>$ such that $PC(F)$ is defined; F is* closed by E-paramodulation *if $PC(F) = F$.*

Given an E-constructed theory F and $Gr = Gr(PC(F))$, we define the following sets of ground rules for any $s = t$ or $t = s$ in Gr such that $s > t$:

- $I^{s=t} = \begin{cases} \emptyset, & \text{if } s \text{ or } t \text{ is } R^{<s=t}, E\text{-reducible} \\ \{s \to t\}, & \text{otherwise} \end{cases}$
- $R^{<s=t} = \bigcup_{(u=v)<(s=t)} I^{u=v}$, *where the equalities are ordered by treating them as multisets of terms: $(u = v) < (s = t)$ iff $\{s, t\}$ is strictly greater than $\{u, v\}$ w.r.t the multiset extension of $>$,*
- $R_F = \bigcup_{s=t\in Gr} I^{s=t}$.

Theorem 1. *Let R_F be the set of ground rules introduced in Definition 1 for an E-constructed theory F. Then, all the symbols of E are constructors for R_F, the rewrite relation $\to_{R_F,E}$ is E-convergent on ground terms and for any ground terms s, t, $s =_{F\cup E} t$ iff $s \downarrow_{R_F,E} =_E t \downarrow_{R_F,E}$.*

Proof. (Sketch) Assume $\to_{R_F,E}$ is not Church-Rosser modulo E on ground terms. In that case, there exists a non-joinable critical pair possibly generated by E-**Paramodulation**, provided that it is not optimally joinable. This critical pair cannot be optimally joinable, otherwise it would be joinable. Thus E-**Paramodulation** applies, and this contradicts the definition of R_F. □

Note that we overlap with non-maximal sides in E-**Paramodulation**. This allows us to build a rewrite relation $\rightarrow_{R_F,E}$ which is both E-convergent and *IR1*. The next lemma is a direct consequence of Definition 1.

Lemma 1. *Let (R, E) be any E-constructed TRS and $>$ the reduction ordering defined by $s > t$ if $s \rightarrow^+_{R,E} t$. Then, $R^=$ is an E-constructed theory. If $\rightarrow_{R,E}$ is IR1, then $R^=$ is an E-constructed theory closed by E-paramodulation.*

Lemma 1 provides us a way to get an E-constructed theory closed by E-paramodulation starting from any forward-closed E-constructed TRS since any E-constructed TRS is forward-closed iff it is *IR1* [18,15].

Lemma 2. *If F is an E-constructed theory, then E-unification is complete for solving the Σ_0-fragment of $F \cup E$-unification.*

A proof of Lemma 2 is developed in Appendix A.

Example 2. Consider the Group Keys example from Section 1. Since E_1 is closed by AC-paramodulation $E_1 = PC(E_1)$. In addition, since $\Sigma_0 = \{\cup\}$, the conditions of Definition 1 are satisfied. Orienting the rule of E_1 from left to right we obtain a ground AC-convergent system $\rightarrow_{E_1,AC}$. Finally, from Lemma 1 we have an AC-constructed theory.

4 Equational Syntacticness

In this section, we introduce an equational extension of the classical notion of syntactic theory.

Definition 2 (E-syntactic theory). *Consider a Σ_0-theory E and a Σ-theory $F \cup E$. Let S be a finite set of $F \cup E$-equalities $l = r$ such that l or r is $\Sigma \backslash \Sigma_0$-rooted. The set S is said to be an* E-resolvent presentation *of $F \cup E$ if for any $F \cup E$-equality $t =_{F \cup E} t'$ there exists an equational proof $t \leftrightarrow^*_{S \cup E} t'$ with the following property: if there is an S-equational step applied at the root position, then it is the only $S \cup E$-equational step applied at the root position. The equational theory $F \cup E$ is said to be* E-syntactic *if there exists an E-resolvent presentation of $F \cup E$.*

When E is the empty theory over an empty signature Σ_0, an E-syntactic theory (resp., an E-resolvent presentation) corresponds to the classical definition of a syntactic theory (resp., a resolvent presentation) [19,24].

Lemma 3. *Assume $F \cup E$ is E-syntactic. Consider any terms $\bar{s}, \bar{t}$ and any function symbols f, g such that $f(\bar{s})$ or $g(\bar{t})$ is $\Sigma \backslash \Sigma_0$-rooted. Then, $f(\bar{s}) =_{F \cup E} g(\bar{t})$ iff either $f, g \in \Sigma \backslash \Sigma_0$, $f = g$ and $\bar{s} =_{F \cup E} \bar{t}$, or there exist $f(\bar{l}) = g(\bar{r}) \in S$ and a substitution σ such that $\bar{s} =_{F \cup E} \bar{l}\sigma$ and $\bar{t} =_{F \cup E} \bar{r}\sigma$.*

Proof. This follows from Definition 2. Consider the proof of $f(\bar{s}) =_{S\cup E} g(\bar{t})$ where S is the E-resolvent presentation of $F \cup E$. Since S is an E-resolvent presentation and $f(\bar{s})$ or $g(\bar{t})$ is $\Sigma\backslash\Sigma_0$-rooted, there can only be one or no S-equational steps at the root position and no E-equational steps. If there is no S-equational step at the root position, then $f = g$ and $\bar{s} =_{S\cup E} \bar{t}$ which implies $\bar{s} =_{F\cup E} \bar{t}$. If there is an S-equational step at the root position, then it is the only step applied at the root position. Thus, there exist $f(\bar{l}) = g(\bar{r}) \in S$ and a substitution σ such that $\bar{s} =_{S\cup E} \bar{l}\sigma$ and $\bar{t} =_{S\cup E} \bar{r}\sigma$, which implies the result. □

The following lemma states the connection between syntacticness and the partial form of syntacticness represented by E-syntacticness.

Lemma 4. *Let F be any E-constructed theory. Then, $F \cup E$ is syntactic iff $F \cup E$ is E-syntactic and E is syntactic.*

Proof. For both directions, we proceed by induction on the size of $F \cup E$-equalities, where the size of an equality is defined as the number of function symbols occurring in the equality.

For the only-if direction, consider $S_{F\cup E}$ is a resolvent presentation of a theory $F \cup E$ such that F is E-constructed. Let $S_E = \{l = r \mid l = r \in S_{F\cup E}, \text{ and } l, r \text{ are } \Sigma_0\text{-terms}\}$. By induction on the size of $F \cup E$-equalities between Σ_0-terms, we can prove that, for any $t =_{F\cup E} t'$ where t and t' are Σ_0-terms, there exists an equational proof $t \longleftrightarrow^*_{S_E} t'$ with at most one step applied at the root position. Since $=_E$ and $=_{F\cup E}$ coincide on Σ_0-terms, S_E is resolvent presentation of E. Let $S = \{l = r \mid l = r \in S_{F\cup E}, \{l(\epsilon), r(\epsilon)\} \cap (\Sigma\backslash\Sigma_0) \neq \emptyset\}$. Since F is E-constructed, there exist some particular $F \cup E$-equational proofs (cf. Appendix C) which permit us to prove the following statement by induction on the size of $F\cup E$-equalities: for any $t =_{F\cup E} t'$ there exists an equational proof $t \longleftrightarrow^*_{S\cup E} t'$ such that any S-equational step applied at the root position is necessarily the unique $S\cup E$-equational step applied at the root position. Therefore, S is an E-resolvent presentation of $F \cup E$.

For the if-direction, consider S_E is a resolvent presentation of E and S is an E-resolvent presentation of a theory $F \cup E$ such that F is E-constructed. Let $S_{F\cup E} = S \cup S_E$. Thanks to the same particular $F \cup E$-equational proofs as the ones used above (cf. Appendix C), we can prove the following statement by induction on the size of $F \cup E$-equalities: for any $t =_{F\cup E} t'$ there exists an equational proof $t \longleftrightarrow^*_{S_{F\cup E}} t'$ with at most one step applied at the root position. Therefore, $S_{F\cup E}$ is a resolvent presentation of $F \cup E$. □

5 Hierarchical Unification

We present a general result to build a hierarchical unification procedure for E-syntactic theories. The rules in Fig. 1 provide the skeleton of the type of hierarchical procedure we are looking for. The procedure is parameterized by an E-unification algorithm and an inference system U like the one given in Fig. 2. The rules, **Coalesce**, **Split**, **Flatten**, and **VA** are used to separate the

equations, U is used to simplify the $\Sigma\backslash\Sigma_0$-equations, and finally, **Solve**, is used to apply the E-unification algorithm on Σ_0-equations.

Coalesce $\{x = y\} \cup G \vdash \{x = y\} \cup (G\{x \mapsto y\})$
where x and y are distinct variables occurring both in G.

Split $\{f(\bar{v}) = t\} \cup G \vdash \{x = f(\bar{v}), x = t\} \cup G$
where $f \in \Sigma\backslash\Sigma_0$, t is a non-variable term and x is a fresh variable.

Flatten $\{v = f(\dots, u, \dots)\} \cup G \vdash \{v = f(\dots, x, \dots), x = u\} \cup G$
where $f \in \Sigma\backslash\Sigma_0$, v is a variable, u is a non-variable term, and x is a fresh variable.

VA $\{s = t[u]\} \cup G \vdash \{s = t[x], x = u\} \cup G$
where t is Σ_0-rooted, u is an alien subterm of t, and x is a fresh variable.

Solve $G \cup G_0 \vdash G \cup \hat{\sigma}_0$
where G is a set of $\Sigma\backslash\Sigma_0$-equations, G_0 is a set of Σ_0-equations, G_0 is E-unifiable and not in tree solved form, $\hat{\sigma}_0$ is the tree solved form associated to $\sigma_0 \in CSU_E(G_0)$, and w.l.o.g for any $x \in Dom(\sigma_0)$, $x\sigma_0 \in Var(G_0)$ if $x\sigma_0$ is a variable.

Fig. 1. H_E rules

Dec $\{x = f(\bar{v}), x = f(\bar{w})\} \cup G \vdash \{x = f(\bar{v}), \bar{v} = \bar{w}\} \cup G$
where $f \in \Sigma\backslash\Sigma_0$.

Mut$_S$ $\{x = f(\bar{v}), x = g(\bar{w})\} \cup G \vdash \{x = f(\bar{v}), \bar{v} = \bar{l}, \bar{w} = \bar{r}\} \cup G$
where $f(\bar{l}) = g(\bar{r}) \in S$.

Fig. 2. DM_S rules

Definition 3 (Hierarchical unification procedure). *Assume a Σ_0-theory E, an E-unification algorithm computing a finite $CSU_E(G_0)$ for all E-unification problems G_0, a Σ-theory $F \cup E$ for which E-unification is complete for solving the Σ_0-fragment of $F \cup E$-unification, and an inference system U satisfying the following assumptions: U transforms only non-variable flat $\Sigma\backslash\Sigma_0$-equations; U is sound and complete for $F \cup E$-unification; U is parameterized by some finite set S of $F \cup E$-equalities such that the soundness of each inference $\vdash_U$ follows from at most one equality in S. Under these assumptions, $H_E(U)$ is the inference system defined as the repeated application of some inference from H_E (cf. Fig. 1) or U, using the following order of priority: **Coalesce**, **Split**, **Flatten**, **VA**, U, **Solve**. An $F \cup E$-unification problem is* separate*, also called in* separate form*, if it is a normal form w.r.t $H_E\backslash\{$**Solve**$\}$. $H_E(U)$ is a* hierarchical unification procedure *for $F \cup E$ if the $F \cup E$-unifiable normal forms w.r.t $H_E(U)$ are the separate dag solved forms.*

Note that when we speak of an inference system, U, this is not just a set of rules but also a strategy for apply those rules, for instance to avoid non-termination [13]. The theory-specific rules in $\{\mathbf{Solve}\} \cup U$ are applied using a don't know nondeterminism. From now on, an inference system $H_E(U)$ always denotes a hierarchical unification procedure.

Lemma 5. *Any hierarchical unification procedure for $F \cup E$ is a sound and complete $F \cup E$-unification procedure.*

Proof. Let $H_E(U)$ be a hierarchical unification procedure as given in Definition 3. All the rules in $H_E \backslash \{\mathbf{Solve}\}$ are always sound and complete, independently from the underlying equational theory. By assumption on $F \cup E$ and U, $H_E(U)$ is sound and complete. Since the $F \cup E$-unifiable normal forms w.r.t $H_E(U)$ are assumed to be the separate dag solved forms, collecting all the separate dag solved forms reached by $H_E(U)$ provides a complete set of $F \cup E$-unifiers. □

It will now be useful to consider an E-syntactic theory $F \cup E$ for which all the $\Sigma \backslash \Sigma_0$-rooted terms are subterm collapse-free modulo $F \cup E$. This allows us to get a possible instantiation of the hierarchical unification procedure.

Lemma 6. *Assume a Σ_0-theory E, an E-unification algorithm, a Σ-theory $F \cup E$ such that F is E-constructed, $F \cup E$ is E-syntactic with an E-resolvent presentation S, and all the $\Sigma \backslash \Sigma_0$-rooted terms are subterm collapse-free modulo $F \cup E$. Given E, $F \cup E$ and DM_S the inference system from Fig. 2, all the assumptions of Definition 3 are satisfied to get a hierarchical unification procedure $H_E(DM_S)$, and $H_E(DM_S)$ is a sound and complete $F \cup E$-unification procedure.*

Proof. By Lemma 2, **Solve** is sound and complete. By Lemma 3, DM_S is sound and complete. Moreover, the soundness of each inference rule in DM_S follows from at most one equality in S.

Consider any separate form $G_1 \wedge G_0$ containing a cycle with at least one equation in G_1. By assumption, this cycles has no solution in $F \cup E$. Consequently, the separate dag solved forms are the $F \cup E$-unifiable normal forms w.r.t $H_E(DM_S)$. Hence, all the assumptions of Definition 3 are satisfied and Lemma 5 applies. □

In Lemma 6, one can notice that E is necessarily collapse-free and E-unification is finitary. So, E is syntactic according to [19]. By Lemma 4, $F \cup E$ is not only E-syntactic but syntactic when Lemma 6 applies.

In the following, we focus on combinations of E-constructed theories admitting terminating hierarchical unification procedures. The case of regular and collapse-free E-constructed theories is studied in Section 6. The class of E-constructed theories closed by E-paramodulation is considered in Section 7.

6 Combination of Regular Collapse-Free Theories

In this section we extend the approach initiated in [15] moving from the restricted case of subterm collapse-free theories to the less restrictive regular and collapse-free theories. Let us consider a union $F_1 \cup F_2 \cup E$ of regular collapse-free theories

such that F_1 and F_2 are E-constructed theories. The signatures of E, F_1 and F_2 are respectively denoted by Σ_0, Σ_1 and Σ_2. The theories F_1 and F_2 are assumed to share only the symbols of E, meaning that $\Sigma_0 = \Sigma_1 \cap \Sigma_2$. We can show that, for any $i = 1, 2$, $F_i \cup E$-unification is complete for solving the Σ_i-fragment of $F_1 \cup F_2 \cup E$-unification (cf. Appendix B). This paves the way of building a combined procedure for $F_1 \cup F_2 \cup E$, but some additional restrictions on $F_1 \cup F_2 \cup E$ are needed. The theory $F_1 \cup F_2 \cup E$ is said to be a *simple combination* if the following two conditions hold: First, for any $\Sigma_1 \backslash \Sigma_0$-rooted term t_1 and any $\Sigma_2 \backslash \Sigma_0$-rooted term t_2, t_1 cannot be equal to t_2 modulo $F_1 \cup F_2 \cup E$. Second, for any term t and any position p in t such that $\bigcup_{q \leq p} \{t(q)\}$ contains at least both a symbol in $\Sigma_1 \backslash \Sigma_0$ and a symbol in $\Sigma_2 \backslash \Sigma_0$, t cannot be equal to $t|_p$ modulo $F_1 \cup F_2 \cup E$. These two conditions mean that there are no solutions to conflicts of theories and no solutions to compound cycles. Let us now introduce a technical lemma which is useful to get a hierarchical unification procedure for $F_1 \cup F_2 \cup E$.

Lemma 7. *Let Σ_1 and Σ_2 be two signatures such that $\Sigma_0 = \Sigma_1 \cap \Sigma_2$. Consider E is a Σ_0-theory and for $i = 1, 2$, F_i is an E-constructed Σ_i-theory such that $F_i \cup E$ admits a sound and complete unification procedure of the form $H_E(U_i)$. If $F_1 \cup F_2 \cup E$ is a simple combination, then we have that*

- *$H_E(U_1 \cup U_2)$ is a sound and complete $F_1 \cup F_2 \cup E$-unification procedure,*
- *if for $i = 1, 2$, S_i is an E-resolvent presentation of $F_i \cup E$, then $S_1 \cup S_2$ is an E-resolvent presentation of $(F_1 \cup F_2) \cup E$.*

Proof. According to the assumptions, any normal form w.r.t $H_E(U_1 \cup U_2)$ is $F_1 \cup F_2 \cup E$-unifiable iff it is in dag solved form. Then, Lemma 5 applies.

Assume now S_i is an E-resolvent presentation of $F_i \cup E$ for $i = 1, 2$. In that case, $S_1 \cup S_2$ is an E-resolvent presentation of $(F_1 \cup F_2) \cup E$ since by assumption it is not possible to have $t_1 =_{F_1 \cup F_2 \cup E} t_2$ for some $\Sigma_1 \backslash \Sigma_0$-rooted term t_1 and some $\Sigma_2 \backslash \Sigma_0$-rooted term t_2. □

We study below a possible way to satisfy the assumptions of Lemma 7, thanks to a property on the shape of normal forms.

Definition 4 (E-capped theory). *Let F be an E-constructed theory over the signature Σ. A Σ-term t is said to be* E-capped *if there exist a constant-free Σ_0-term u and a substitution σ such that $t = u\sigma$, $Dom(\sigma) = Var(u)$ and $Ran(\sigma)$ is a set of $\Sigma \backslash \Sigma_0$-rooted terms. The E-constructed theory F is said to be* E-capped *if any normal form w.r.t $\rightarrow_{R_F, E}$ of any $\Sigma \backslash \Sigma_0$-rooted ground term is E-capped.*

In Definition 4, the term u can be a variable, to take into account the case where the normal form of a $\Sigma \backslash \Sigma_0$-rooted ground term remains $\Sigma \backslash \Sigma_0$-rooted.

Example 3. Consider $\Sigma_0 = \{*\}$ and the Σ_0-theory E defined by an emptyset of Σ_0-axioms.

First, let $(R_{\mathcal{D}}, E)$ be the E-constructed TRS where $R_{\mathcal{D}} = \{h(x * y) \rightarrow h(x) * h(y)\}$. The term $h(x) * h(y)$ is E-capped because $h(x) * h(y) = u\sigma$ for the Σ_0-term with no constants $u = v * w$ and the substitution $\sigma = \{v \mapsto h(x), w \mapsto h(y)\}$.

Notice that $h(x)$ is also E-capped since $h(x) = u\sigma$ for $u = v$ and $\sigma = \{v \mapsto h(x)\}$. By induction on the length of outermost derivations, we can show that any normal form w.r.t $(R_{\mathcal{D}}, E)$ of any term rooted by h is E-capped. Thus, $R^{=}_{\mathcal{D}}$ is E-capped.

Second, let $(R_{\mathcal{D}1}, E)$ be the E-constructed TRS where $R_{\mathcal{D}1} = \{f(x * y, z) \to f(x, z) * f(y, z)\}$. In a way similar to $R^{=}_{\mathcal{D}}$, we can show that $R^{=}_{\mathcal{D}1}$ is E-capped.

Lemma 8. *Assume E is a Σ_0-theory. If for $i = 1, 2$, F_i is a regular collapse-free E-capped Σ_i-theory, and $\Sigma_1 \cap \Sigma_2 = \Sigma_0$, then $F_1 \cup F_2$ is a regular collapse-free E-capped $\Sigma_1 \cup \Sigma_2$-theory such that $F_1 \cup F_2 \cup E$ is a simple combination.*

Proof. (Sketch) Let us consider the *height of layers* of a term t, inductively defined as follows: $ht(t) = 0$ if t is a variable; $ht(t) = 1$ if t is a non-variable pure term; $ht(t) = 1 + \max\{ht(u) \mid u \text{ is an alien subterm of } t\}$ if t is not pure.

By contradiction, assume there exist a term t and a position p such that $t =_{F_1 \cup F_2 \cup E} t|_p$ and the path from ϵ to p contains both a symbol in $\Sigma_1 \backslash \Sigma_0$ and a symbol in $\Sigma_2 \backslash \Sigma_0$. Let $u = t|_p$ and let t' and u' be the respective normal forms w.r.t $\to_{R_{F_1} \cup R_{F_2}, E}$ of t and u (viewed as ground terms). Since $t' =_E u'$ and E is regular collapse-free, t' and u' have the same height of layers. By the E-capped assumption, t and t' have the same height of layers, as well as u and u'. Thus t and u have the same height of layers, which leads to a contradiction since the path from ϵ to p includes both a symbol in $\Sigma_1 \backslash \Sigma_0$ and a symbol in $\Sigma_2 \backslash \Sigma_0$.

Assume there exist some $\Sigma_1 \backslash \Sigma_0$-rooted term t_1 and some $\Sigma_2 \backslash \Sigma_0$-rooted term t_2 such that $t_1 =_{F_1 \cup F_2 \cup E} t_2$. Then, $t'_1 =_E t'_2$ where t'_1 and t'_2 are the respective normal forms w.r.t $\to_{R_{F_1} \cup R_{F_2}, E}$ of t_1 and t_2 (viewed as ground terms). The E-capped assumption implies that t'_i must still contain a symbol in $\Sigma_i \backslash \Sigma_0$ for $i = 1, 2$. Since E is regular collapse-free, it is impossible to have $t'_1 =_E t'_2$. □

By Lemma 8, the two assumptions of Lemma 7 can be satisfied, and this leads to the following hierarchical unification procedure.

Corollary 1. *Assume E is a Σ_0-theory; for $i = 1, 2$, F_i is a regular collapse-free E-capped Σ_i-theory, all the $\Sigma_i \backslash \Sigma_0$-rooted terms are subterm collapse-free modulo $F_i \cup E$, S_i is an E-resolvent presentation of $F_i \cup E$; and $\Sigma_1 \cap \Sigma_2 = \Sigma_0$. Then $F_1 \cup F_2$ is a regular collapse-free E-capped theory, $S_1 \cup S_2$ is an E-resolvent presentation of $F_1 \cup F_2 \cup E$, and $H_E(DM_{S_1} \cup DM_{S_2})$ is a sound and complete $F_1 \cup F_2 \cup E$-unification procedure.*

Proof. By Lemmas 8, 7, 6 and the fact that $H_E(DM_{S_1 \cup S_2})$ coincides with $H_E(DM_{S_1} \cup DM_{S_2})$. □

Example 4. (Example 3 continued) There exists an E-resolvent presentation $S_{\mathcal{D}}$ (resp., $S_{\mathcal{D}1}$) of $R_{\mathcal{D}} \cup E$ (resp., $R_{\mathcal{D}1} \cup E$). By Corollary 1, $H_E(DM_{S_{\mathcal{D}}} \cup DM_{S_{\mathcal{D}1}})$ is a sound and complete $R_{\mathcal{D}} \cup R_{\mathcal{D}1} \cup E$-unification procedure.

To study the termination of the combined hierarchical unification procedure given in Lemma 7, we reuse the notion of decreasingness initiated in [15].

Definition 5 (Decreasingness). *Consider a complexity measure defined as a mapping C from separate forms to natural numbers. A $H_E(U)$ inference system is said to be* C-decreasing *if for any separate form $G \cup G_0$ we have that*

- *for any G' such that $G \cup G_0 \vdash_U G' \cup G_0$, the separate form of $G' \cup G_0$ does not increase C;*
- *for any G'_0 such that $G \cup G_0 \vdash_{\textbf{\textit{Solve}}} G \cup G'_0$, then either the separate form of $G \cup G'_0$ is in normal form w.r.t $H_E(U)$, or it decreases C.*

$H_E(U)$ is terminating if there exists some C such that $H_E(U)$ is C-decreasing.

Theorem 2. *Assume a theory E, an E-unification algorithm, and a complexity measure C defined on separate forms. Let F_1 and F_2 be two regular collapse-free E-capped theories sharing only symbols in E such that, for $i = 1, 2$, $F_i \cup E$ admits a C-decreasing unification algorithm of the form $H_E(U_i)$. Then $F_1 \cup F_2$ is a regular collapse-free E-capped theory such that $F_1 \cup F_2 \cup E$ admits a C-decreasing unification algorithm of the form $H_E(U_1 \cup U_2)$.*

Proof. $F_1 \cup F_2$ is a regular collapse-free E-capped theory by Lemma 8. In addition, Lemma 7 and Lemma 5 can be applied. Hence, $H_E(U_1 \cup U_2)$ provides a sound and complete $F_1 \cup F_2 \cup E$-unification procedure. Moreover, $H_E(U_1 \cup U_2)$ is C-decreasing and so it is terminating. □

This theorem subsumes a similar result from [15]. The advantage now is that we don't need to check the subterm-collapse freeness property, which can be a difficult task. Rather, we need only to check regularity and collapse-freeness, and this can be trivially achieved by examining the axioms. For example, Theorem 2 allows us to obtain a combined hierarchical unification algorithm for the exponentiation theories from Section 1.

7 Combination of Theories Closed by *E*-Paramodulation

In this section, we focus on E-constructed theories F such that $PC(F) = F$. The next lemma follows from a very similar argument to Lemma 3.

Lemma 9. *Let F be an E-constructed theory closed by E-paramodulation. For each ground equality $u =_{F \cup E} v$ such that u is $\Sigma \backslash \Sigma_0$-rooted and v is normalized w.r.t $\rightarrow_{R_F,E}$, one of the following is true: (1) $u = f(\bar{u})$, $v = f(\bar{v})$ and $\bar{u} =_{F \cup E} \bar{v}$; (2) $u = f(\bar{u})$, there exist $f(\bar{s}) = t \in F$ and a substitution σ normalized w.r.t $\rightarrow_{R_F,E}$ such that $\bar{u} =_{F \cup E} \bar{s}\sigma$, $v =_E t\sigma$ and $\bar{s}\sigma, t\sigma$ are normalized w.r.t $\rightarrow_{R_F,E}$.*

The inference system BSM_F given in Fig. 3 can be used to show the existence of a hierarchical unification algorithm for the class of E-constructed theories closed by E-paramodulation. One can notice that each inference rule in BSM_F generates some boxed terms. This particular annotation of terms, detailed in [20,11], allows us to control the rule applications, disregarding needless inferences on boxed terms in such a way that the termination is guaranteed.

Imit $\bigcup_i\{x = f(\bar{v}_i)\} \cup G \vdash \{x = \boxed{f(\bar{y})}\} \cup \bigcup_i\{\bar{y} = \bar{v}_i\} \cup G$
where $f \in \Sigma\backslash\Sigma_0$, $i > 1$, $\bar{y}$ are fresh variables and there are no more equations $x = f(\dots)$ in G.

MutConflict$_F$ $\{x = f(\bar{v})\} \cup G \vdash \{x = \boxed{t}, \boxed{\bar{s}} = \bar{v}\} \cup G$
where $f \in \Sigma\backslash\Sigma_0$, $f(\bar{s}) = t$ is a fresh instance of an equality in F, $f(\bar{v})$ is unboxed, and (there is another equation $x = u$ in G with a non-variable term u or $x = f(\bar{v})$ occurs in a cycle).

ImitCycle $\{x = f(\bar{v})\} \cup G \vdash \{x = \boxed{f(\bar{y})}, \bar{y} = \bar{v}\} \cup G$
where $f \in \Sigma\backslash\Sigma_0$, $f(\bar{v})$ is unboxed, $\bar{y}$ are fresh variables and $x = f(\bar{v})$ occurs in a cycle.

Fig. 3. BSM_F rules

Theorem 3. *Consider any E-constructed theory F closed by E-paramodulation and the inference system BSM_F given in Fig. 3. Then, $F \cup E$ is an E-syntactic theory admitting a unification algorithm of the form $H_E(BSM_F)$.*

Proof. $F \cup E$ is E-syntactic since an E-resolvent presentation of $F \cup E$ is $F \cup \{l\sigma = g\sigma \mid l = r, g = d \in F, l\sigma \not< r\sigma, g\sigma \not< d\sigma, \sigma \in CSU_E(r =^? d), l\sigma \neq g\sigma\}$. By Lemma 9, BSM_F satisfies the assumption of Definition 3. Since the separate dag solved forms are the $F \cup E$-unifiable normal forms w.r.t $H_E(BSM_F)$, Lemma 5 applies and so $H_E(BSM_F)$ is a sound and complete $F \cup E$-unification procedure. Moreover $H_E(BSM_F)$ can be proved terminating using the same proof as the one developed in [11,15] for forward-closed E-constructed TRSs. Thus, $H_E(BSM_F)$ is a sound and complete terminating $F \cup E$-unification procedure. □

Theorem 4. *If F_1 and F_2 are two E-constructed theories closed by E-paramodulation and sharing only symbols in E, then $F_1 \cup F_2$ is an E-constructed theory closed by E-paramodulation.*

Proof. (Sketch) The maximal sides of equalities in F_i are necessarily $\Sigma_i\backslash\Sigma_0$-rooted for $i = 1, 2$. Therefore, it is impossible to apply E-**Paramodulation** with one premise in F_1 and the other one in F_2. □

Corollary 2. *If for $i = 1, 2$, F_i is an E-constructed Σ_i-theory closed by E-paramodulation, and $\Sigma_1 \cap \Sigma_2 = \Sigma_0$, then $F_1 \cup F_2 \cup E$ is an E-syntactic theory admitting a unification algorithm of the form $H_E(BSM_{F_1} \cup BSM_{F_2})$.*

Proof. By Theorems 4, 3, and the fact that $H_E(BSM_{F_1 \cup F_2})$ coincides with $H_E(BSM_{F_1} \cup BSM_{F_2})$. □

Example 5. Continuing Example 2 and Example 1, we can notice that E_1 and E_2 are both AC-constructed and closed by AC-paramodulation. By Theorem 4, $E_1 \cup E_2$ is closed by AC-paramodulation. Furthermore, $E_1 \cup E_2$ is an AC-syntactic theory admitting a unification algorithm of the form $H_{AC}(BSM_{E_1} \cup BSM_{E_2})$.

Theorem 4 can be applied to *IR1* E-constructed TRSs combined with some particular shallow theories.

Definition 6 (Shallow extension). *Let (R, E) be an E-constructed TRS over the signature Σ, and Σ' a signature extension of Σ. A* shallow extension of (R, E) *is an equational Σ'-theory $F \cup R^{=}$ where F is a finite set of shallow Σ'-equalities $l = r$ such that $l(\epsilon), r(\epsilon) \in (\Sigma' \backslash \Sigma) \cup X$ and all the ground terms occurring in F are Σ-terms in normal form w.r.t (R, E).*

A shallow extension $F \cup R^{=}$ of (R, E) can be viewed as a union of two E-constructed theories sharing only symbols in E (plus, some additional constants). The first theory, say F', is obtained from F by performing a constant abstraction of maximal ground terms rooted by symbols defined by R. The second theory is given by a set of rules, say R', defined as R plus all the rules $t \to c$ for each abstracted ground term t, c being the constant that abstracts t. We can show that F' admits a finite closure by E-paramodulation. If (R, E) is an *IR1* E-constructed TRS, then so is (R', E), and $R'^{=}$ is closed by E-paramodulation according to Lemma 1. Then, Theorem 4 can be applied to get:

Theorem 5. *Assume (R, E) is any E-constructed TRS such that $\to_{R,E}$ is IR1, $F \cup R^{=}$ is any shallow extension of (R, E), and $>$ is a reduction ordering including $\to_{R,E}$ such that $PC(F)$ is defined. Then, $PC(F \cup R^{=})$ is finite.*

8 Conclusion

Assuming a regular collapse-free theory E and an E-unification algorithm, we have studied the (combined) unification problem in (unions of) E-constructed theories. Our notion of constructor seems to be closely related to the one used in [5] but this remains to be formally shown.

As future work, it would be interesting to apply our hierarchical approach to unification in order-sorted equational theories, to handle for instance order-sorted AC-convergent rewrite systems with the Finite Variant Property that can be used for homomorphic encryption [27]. In the near future, we plan to reuse the notion of E-constructed theory in order to investigate the possible extension of the combination methods developed in [14] for two knowledge problems of particular interest in the analysis of protocols. These combination methods have been initially developed for the case of theories sharing only absolutely free constructors and we believe that the framework above will be useful to lift these methods to the case of theories sharing only constructors modulo E.

In a longer term, we envision to study the possible development of a hierarchical approach to solve the disunification problem modulo theories closed by E-paramodulation. The disunification problem has been already successfully considered for forward-closed rewrite systems [22]. Since paramodulation-closed theories bear similarities with forward-closed rewrite systems, investigating a hierarchical approach to solve the disunification problem [2,22] appears to be a promising research direction.

References

1. Baader, F., Nipkow, T.: Term rewriting and all that. Cambridge University Press (1998)
2. Baader, F., Schulz, K.U.: Combination techniques and decision problems for disunification. Theor. Comput. Sci. **142**(2), 229–255 (1995)
3. Baader, F., Schulz, K.U.: Unification in the union of disjoint equational theories: Combining decision procedures. J. Symb. Comput. **21**(2), 211–243 (1996)
4. Baader, F., Snyder, W.: Unification theory. In: Robinson, J.A., Voronkov, A. (eds.) Handbook of Automated Reasoning (in 2 volumes), pp. 445–532. Elsevier and MIT Press (2001)
5. Baader, F., Tinelli, C.: Combining decision procedures for positive theories sharing constructors. In: Tison, S. (ed.) Rewriting Techniques and Applications, 13th International Conference, RTA 2002, Copenhagen, Denmark, July 22-24, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2378, pp. 352–366. Springer (2002)
6. Bouchard, C., Gero, K.A., Lynch, C., Narendran, P.: On forward closure and the finite variant property. In: Fontaine, P., Ringeissen, C., Schmidt, R.A. (eds.) Frontiers of Combining Systems - 9th International Symposium, FroCoS 2013, Nancy, France, September 18-20, 2013. Proceedings. Lecture Notes in Computer Science, vol. 8152, pp. 327–342. Springer (2013)
7. Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J., Milner, K.: On ends-to-ends encryption: Asynchronous group messaging with strong security guarantees. In: Lie, D., Mannan, M., Backes, M., Wang, X. (eds.) Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018. pp. 1802–1819. ACM (2018)
8. Comon, H., Haberstrau, M., Jouannaud, J.P.: Syntacticness, cycle-syntacticness, and shallow theories. Inf. Comput. **111**(1), 154–191 (1994)
9. Comon-Lundh, H., Delaune, S.: The finite variant property: How to get rid of some algebraic properties. In: Giesl, J. (ed.) Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3467, pp. 294–307. Springer (2005)
10. Domenjoud, E., Klay, F., Ringeissen, C.: Combination techniques for non-disjoint equational theories. In: Bundy, A. (ed.) Automated Deduction - CADE-12, 12th International Conference on Automated Deduction, Nancy, France, June 26 - July 1, 1994, Proceedings. Lecture Notes in Computer Science, vol. 814, pp. 267–281. Springer (1994)
11. Eeralla, A.K., Erbatur, S., Marshall, A.M., Ringeissen, C.: Rule-based unification in combined theories and the finite variant property. In: Martín-Vide, C., Okhotin, A., Shapira, D. (eds.) Language and Automata Theory and Applications - 13th International Conference, LATA 2019, St. Petersburg, Russia, March 26-29, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11417, pp. 356–367. Springer (2019)
12. Erbatur, S., Kapur, D., Marshall, A.M., Narendran, P., Ringeissen, C.: Hierarchical combination. In: Bonacina, M.P. (ed.) Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings. Lecture Notes in Computer Science, vol. 7898, pp. 249–266. Springer (2013)
13. Erbatur, S., Marshall, A.M., Kapur, D., Narendran, P.: Unification over distributive exponentiation (sub)theories. J. Autom. Lang. Comb. **16**(2-4), 109–140 (2011)

14. Erbatur, S., Marshall, A.M., Ringeissen, C.: Notions of knowledge in combinations of theories sharing constructors. In: de Moura, L. (ed.) Automated Deduction - CADE 26 - 26th International Conference on Automated Deduction, Gothenburg, Sweden, August 6-11, 2017, Proceedings. Lecture Notes in Computer Science, vol. 10395, pp. 60–76. Springer (2017)
15. Erbatur, S., Marshall, A.M., Ringeissen, C.: Terminating non-disjoint combined unification. In: Fernández, M. (ed.) Logic-Based Program Synthesis and Transformation - 30th International Symposium, LOPSTR 2020, Bologna, Italy, September 7-9, 2020, Proceedings. Lecture Notes in Computer Science, vol. 12561, pp. 113–130. Springer (2020)
16. Escobar, S., Sasse, R., Meseguer, J.: Folding variant narrowing and optimal variant termination. J. Log. Algebr. Program. **81**(7-8), 898–928 (2012)
17. Jouannaud, J.P., Kirchner, H.: Completion of a set of rules modulo a set of equations. SIAM J. Comput. **15**(4), 1155–1194 (1986)
18. Kim, D., Lynch, C., Narendran, P.: Reviving basic narrowing modulo. In: Herzig, A., Popescu, A. (eds.) Frontiers of Combining Systems - 12th International Symposium, FroCoS 2019, London, UK, September 4-6, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11715, pp. 313–329. Springer (2019)
19. Kirchner, C., Klay, F.: Syntactic theories and unification. In: Proceedings of the Fifth Annual Symposium on Logic in Computer Science (LICS '90), Philadelphia, Pennsylvania, USA, June 4-7, 1990. pp. 270–277. IEEE Computer Society (1990)
20. Lynch, C., Morawska, B.: Basic syntactic mutation. In: Voronkov, A. (ed.) Automated Deduction - CADE-18, 18th International Conference on Automated Deduction, Copenhagen, Denmark, July 27-30, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2392, pp. 471–485. Springer (2002)
21. Lynch, C., Morawska, B.: Faster *Basic Syntactic Mutation* with sorts for some separable equational theories. In: Giesl, J. (ed.) Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3467, pp. 90–104. Springer (2005)
22. Meseguer, J.: Variant-based satisfiability in initial algebras. Sci. Comput. Program. **154**, 3–41 (2018)
23. Nguyen, K.: Formal verification of a messaging protocol. Internship report (2019), work done under the supervision of Vincent Cheval and Véronique Cortier
24. Nipkow, T.: Proof transformations for equational theories. In: Proceedings of the Fifth Annual Symposium on Logic in Computer Science (LICS '90), Philadelphia, Pennsylvania, USA, June 4-7, 1990. pp. 278–288. IEEE Computer Society (1990)
25. Ringeissen, C.: Unification in a combination of equational theories with shared constants and its application to primal algebras. In: Voronkov, A. (ed.) Logic Programming and Automated Reasoning,International Conference LPAR'92, St. Petersburg, Russia, July 15-20, 1992, Proceedings. Lecture Notes in Computer Science, vol. 624, pp. 261–272. Springer (1992)
26. Schmidt-Schauß, M.: Unification in a combination of arbitrary disjoint equational theories. J. Symb. Comput. **8**(1/2), 51–99 (1989)
27. Yang, F., Escobar, S., Meadows, C.A., Meseguer, J., Narendran, P.: Theories of homomorphic encryption, unification, and the finite variant property. In: Chitil, O., King, A., Danvy, O. (eds.) Proceedings of the 16th International Symposium on Principles and Practice of Declarative Programming, Kent, Canterbury, United Kingdom, September 8-10, 2014. pp. 123–133. ACM (2014)

A Solving the E-Pure Fragment of an E-Constructed Theory

Given a regular and collapse-free Σ_0-theory E, assuming an E-constructed theory F is sufficient to get that E-unification is complete for solving the Σ_0-fragment of $F \cup E$-unification. To prove this fact, let us introduce some technicalities. In this section, we consider the rewrite relation $\rightarrow_{R_F,E}$, which is E-convergent on ground terms according to Theorem 1. A normal form w.r.t $\rightarrow_{R_F,E}$ is simply called a normal form, and a normal form w.r.t $\rightarrow_{R_F,E}$ of a term t is simply denoted by $t{\downarrow}$. When we refer to the normal form of a term (resp., a substitution), this term (resp., this substitution) is supposed to be ground thanks to additional skolemized variables.

Let π be a mapping from $\Sigma\backslash\Sigma_0$-rooted normalized terms to fresh variables such that for any $\Sigma\backslash\Sigma_0$-rooted normalized terms u and u', $\pi(u) = \pi(u')$ iff $u =_E u'$. Given a normalized term t, t^{π_0} is defined inductively as follows:

- $f(t_1, \ldots, t_m)^{\pi_0} = f(t_1^{\pi_0}, \ldots, t_m^{\pi_0})$ if $f \in \Sigma_0$,
- $f(t_1, \ldots, t_m)^{\pi_0} = \pi(f(t_1, \ldots, t_m))$ if $f \in \Sigma\backslash\Sigma_0$,
- $x^{\pi_0} = x$ if x is a (skolemized) variable.

Given a normalized substitution σ, $\sigma^{\pi_0} = \{x \mapsto (x\sigma)^{\pi_0} \mid x \in Dom(\sigma)\}$.

Lemma 10. *Let F be an E-constructed theory. For any Σ_0-terms t and u, and any normalized substitution σ, $t\sigma =_{F\cup E} u\sigma$ implies $t\sigma^{\pi_0} =_E u\sigma^{\pi_0}$.*

Proof. Since $\rightarrow_{R_F,E}$ is E-convergent on ground terms, $t\sigma =_{R\cup E} u\sigma$ if and only if $(t\sigma){\downarrow} =_E (u\sigma){\downarrow}$. Since t and u are Σ_0-terms, all the symbols of E are constructors for R_F, and σ is normalized, we have that $t\sigma = (t\sigma){\downarrow}$ and $u\sigma = (u\sigma){\downarrow}$. Hence, $t\sigma =_E u\sigma$. Then, the $\Sigma\backslash\Sigma_0$-symbols are free with respect to the Σ_0-theory E, and we can use the following well-known equivalence: for any Σ-terms t', u', $t' =_E u'$ if and only if $(t')^{\pi_0} =_E (u')^{\pi_0}$. In particular, we have $t\sigma =_E u\sigma$ if and only if $(t\sigma)^{\pi_0} =_E (u\sigma)^{\pi_0}$. □

Lemma 2 is a direct consequence of Lemma 10.

B Solving the Pure Fragments of a Union of E-Constructed Theories

Given a regular and collapse-free Σ_0-theory E, assume F_i is an E-constructed theory built over the signature Σ_i for $i = 1, 2$, and $\Sigma_0 = \Sigma_1 \cap \Sigma_2$. Then, we can show that $F_i \cup E$-unification is complete for solving the Σ_i-fragment of $F_1 \cup F_2 \cup E$-unification. To prove this fact, we rely on the classical notion of i-abstraction. In this section, we consider the rewrite relation $\rightarrow_{R_{F_1}\cup R_{F_2},E}$ where R_{F_1} and R_{F_2} are given by Definition 1. The rewrite relation $\rightarrow_{R_{F_1}\cup R_{F_2},E}$ is Church-Rosser modulo E on grounds terms since all the symbols in E are constructors for both R_{F_1} and R_{F_2}. Moreover, $\rightarrow_{R_{F_1}\cup R_{F_2},E}$ is terminating since $>$ is supposed to be a

reduction ordering on terms built over $\Sigma_1 \cup \Sigma_2$. A normal form w.r.t $\rightarrow_{R_{F_1} \cup R_{F_2}, E}$ is simply called a normal form, and a normal form w.r.t $\rightarrow_{R_{F_1} \cup R_{F_2}, E}$ of a term t is simply denoted by $t{\downarrow}$. When we refer to the normal form of a term (resp., a substitution), this term (resp., this substitution) is supposed to be ground thanks to additional skolemized variables.

Let π be a mapping from $(\Sigma_1 \cup \Sigma_2)\backslash\Sigma_0$-rooted normalized terms to fresh variables such that for any $(\Sigma_1 \cup \Sigma_2)\backslash\Sigma_0$-rooted normalized terms u and u', $\pi(u) = \pi(u')$ iff $u =_E u'$. For any $i = 1, 2$ and any normalized term t, the i-abstraction of t is denoted by t^{π_i} and is inductively defined as follows:

- $f(t_1, \ldots, t_m)^{\pi_i} = f(t_1^{\pi_i}, \ldots, t_m^{\pi_i})$ if $f \in \Sigma_i$,
- $f(t_1, \ldots, t_m)^{\pi_i} = \pi(f(t_1, \ldots, t_m))$ if $f \in (\Sigma_1 \cup \Sigma_2)\backslash\Sigma_i$,
- $x^{\pi_i} = x$ if x is a (skolemized) variable.

Given a normalized substitution σ, $\sigma^{\pi_i} = \{x \mapsto (x\sigma)^{\pi_i} \mid x \in Dom(\sigma)\}$.

Lemma 11. *Let $i = 1, 2$. For any Σ_i-rooted term t whose alien subterms are normalized, $t^{\pi_i} =_{F_i \cup E} (t{\downarrow})^{\pi_i}$.*

Proof. Consider a rewrite step $t \rightarrow_{R_{F_1} \cup R_{F_2}, E} t'$ such that $t|_p =_E l$ and $t' = t[r]_p$ for a ground rewrite rule $l \rightarrow r \in R_{F_1} \cup R_{F_2}$. Since all the alien subterms of t are normalized, p occurs necessarily above them. Thus, $l \rightarrow r \in R_{F_i}$. Since E is regular and collapse-free, the alien subterms of $t|_p$ are the same as the alien subterms of l. In addition, we can assume without loss of generality that all the alien subterms of r are normalized. Thus, t' is a Σ_i-rooted term whose alien subterms are normalized. Moreover, we have $t'^{\pi_i} = (t[r]_p)^{\pi_i} = t^{\pi_i}[r^{\pi_i}]_p$. Since the $(\Sigma_1 \cup \Sigma_2)\backslash\Sigma_0$-symbols are free with respect to the Σ_0-theory E and by definition of i-abstraction, we have that $t|_p =_E l$ implies $(t|_p)^{\pi_i} =_E l^{\pi_i}$ and so $(t^{\pi_i})|_p = (t|_p)^{\pi_i} =_E l^{\pi_i}$. Since $l^{\pi_i} =_{F_i} r^{\pi_i}$, we obtain $t^{\pi_i} =_{F_i \cup E} t'^{\pi_i}$. Then, by induction on the length of the rewrite derivation w.r.t $\rightarrow_{R_{F_1} \cup R_{F_2}, E}$, we get $t^{\pi_i} =_{F_i \cup E} (t{\downarrow})^{\pi_i}$. □

Lemma 12. *Let $i = 1, 2$. For any Σ_i-terms t, u and any normalized substitution σ, $t\sigma =_{F_1 \cup F_2 \cup E} u\sigma$ implies $t\sigma^{\pi_i} =_{F_i \cup E} u\sigma^{\pi_i}$.*

Proof. If $t\sigma =_{F_1 \cup F_2 \cup E} u\sigma$ then $(t\sigma){\downarrow} =_E (u\sigma){\downarrow}$. By Lemma 11, $(t\sigma)^{\pi_i} =_{F_i \cup E} ((t\sigma){\downarrow})^{\pi_i}$ and $(u\sigma)^{\pi_i} =_{F_i \cup E} ((u\sigma){\downarrow})^{\pi_i}$. Since the $(\Sigma_1 \cup \Sigma_2)\backslash\Sigma_0$-symbols are free with respect to the Σ_0-theory E and by definition of i-abstraction, we have that $(t\sigma){\downarrow} =_E (u\sigma){\downarrow}$ implies $((t\sigma){\downarrow})^{\pi_i} =_E ((u\sigma){\downarrow})^{\pi_i}$. Hence,

$$t\sigma^{\pi_i} = (t\sigma)^{\pi_i} =_{F_i \cup E} ((t\sigma){\downarrow})^{\pi_i} =_E ((u\sigma){\downarrow})^{\pi_i} =_{F_i \cup E} (u\sigma)^{\pi_i} = u\sigma^{\pi_i}$$

and so $t\sigma^{\pi_i} =_{F_i \cup E} u\sigma^{\pi_i}$. □

As a direct corollary of Lemma 12, we get that for $i = 1, 2$, $F_i \cup E$-unification is complete for solving the Σ_i-fragment of $F_1 \cup F_2 \cup E$-unification. Therefore, an $F_i \cup E$-unification procedure of the form $H_E(U_i)$ for $i = 1, 2$ can be applied without loss of completeness in the combined hierarchical unification procedure for $F_1 \cup F_2 \cup E$ provided by Lemma 7.

C Equational Syntacticness versus Syntacticness

The following lemmas detail the particular $F \cup E$-equational proofs that are useful to prove Lemma 4.

Given an E-constructed theory F, an equality $s =_{F\cup E} t$ is said to be *decomposable* if there exists some $f \in \Sigma\backslash\Sigma_0$ such that $s = f(\bar{s})$, $t = f(\bar{t})$ and $\bar{s} =_{F\cup E} \bar{t}$.

Lemma 13. *Let F be an E-constructed theory. For any equality $t =_{F\cup E} t'$ there exists an $F \cup E$-equational proof of the form:*

$$t \longleftrightarrow^*_{F\cup E} u =_{F\cup E} u' \longleftrightarrow^*_{F\cup E} t'$$

such that

- *there is no equational step applied at the root position in $t \longleftrightarrow^*_{F\cup E} u$ and in $u' \longleftrightarrow^*_{F\cup E} t'$;*
- *$\{u(\epsilon), u'(\epsilon)\} \cap (\Sigma\backslash\Sigma_0) \neq \emptyset$ and $u =_{F\cup E} u'$ is not decomposable, or $u =_E u'$.*

Proof. The equational proof is obtained by analyzing the innermost rewrite derivations $t \to^*_{R_F,E} t\downarrow_{R_F,E}$ and $t' \to^*_{R_F,E} t'\downarrow_{R_F,E}$ that hold when t and t' are viewed as ground terms including some free constants. When t and t' are ground terms, $t =_{F\cup E} t'$ iff

$$t \xrightarrow{\neq\epsilon}{}^*_{R_F,E} u \xrightarrow{\epsilon}{}^{(0|1)}_{R_F,E} u\downarrow_{R_F,E} =_E u'\downarrow_{R_F,E} \xleftarrow{\epsilon}{}^{(0|1)}_{R_F,E} u' \xleftarrow{\neq\epsilon}{}^*_{R_F,E} t'$$

where

- $\xrightarrow{\neq\epsilon}{}^*_{R_F,E}$ and $\xleftarrow{\neq\epsilon}{}^*_{R_F,E}$ denote rewrite derivations where each rewrite step is applied strictly below the root position;
- $\xrightarrow{\epsilon}{}^{(0|1)}_{R_F,E}$ and $\xleftarrow{\epsilon}{}^{(0|1)}_{R_F,E}$ denote rewrite derivations including at most one rewrite step and such that any rewrite step is applied at the root position;
- the strict subterms of u and u' are in normal form w.r.t $\to_{R_F,E}$.

If u and u' are in normal form w.r.t $\to_{R_F,E}$, then $u =_E u'$. Otherwise, $\{u(\epsilon), u'(\epsilon)\} \cap (\Sigma\backslash\Sigma_0) \neq \emptyset$ and $u =_{F\cup E} u'$ is not decomposable. □

Lemma 14. *Let F be an E-constructed theory and S a resolvent presentation of $F\cup E$ (resp., an E-resolvent presentation of $F\cup E$). Given any equality $u =_{F\cup E} u'$ such that $\{u(\epsilon), u'(\epsilon)\} \cap (\Sigma\backslash\Sigma_0) \neq \emptyset$ and $u =_{F\cup E} u'$ is not decomposable, there exists an equational proof $u \leftrightarrow^*_S u'$ (resp., $u \leftrightarrow^*_{S\cup E} u'$) including some S-equational step applied at the root position of the form $\longleftrightarrow^{\epsilon, l=r}_S$ with $\{l(\epsilon), r(\epsilon)\}\cap (\Sigma\backslash\Sigma_0) \neq \emptyset$.*

Proof. If no S-equational step of the indicated form occurs in the equational proof $u \leftrightarrow^*_S u'$, then the equality $u =_{F\cup E} u'$ is decomposable. □