Asymmetric Unification and the Combination Problem in Disjoint Theories

Serdar Erbatur, Deepak Kapur, Andrew Marshall, Catherine Meadows, Paliath Narendran, Christophe Ringeissen

Asymmetric Unification and the Combination Problem in Disjoint Theories

Serdar Erbatur, Deepak Kapur, Andrew M. Marshall, Catherine Meadows, Paliath Narendran, Christophe Ringeissen

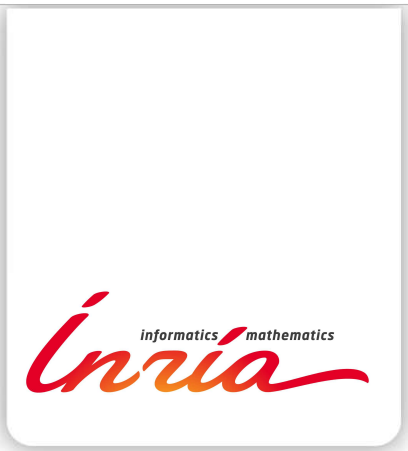
RESEARCH REPORT

N° 8476

February 2014

Project-Team Cassis

ISSN 0249-6399 ISRN INRIA/RR--8476--FR+ENG



Asymmetric Unification and the Combination Problem in Disjoint Theories

Serdar Erbatur*, Deepak Kapur†‡, Andrew M. Marshall§, Catherine Meadows¶, Paliath Narendran‖**, Christophe Ringeissen††

Project-Team Cassis

Research Report n° 8476 — February 2014 — 19 pages

Abstract: Asymmetric unification is a new paradigm for unification modulo theories that introduces irreducibility constraints on one side of a unification problem. It has important applications in symbolic cryptographic protocol analysis, for which it is often necessary to put irreducibility constraints on portions of a state. However many facets of asymmetric unification that are of particular interest, including its behavior under combinations of disjoint theories, remain poorly understood. In this paper we give a new formulation of the method for unification in the combination of disjoint equational theories developed by Baader and Schulz that both gives additional insights into the disjoint combination problem in general, and furthermore allows us to extend the method to asymmetric unification, thus giving the first unification method for asymmetric unification in the combination of disjoint theories.

Key-words: Equational theory, asymmetric unification, combination problem

* Università degli Studi di Verona
† University of New Mexico
‡ Partially supported by the NSF grant CNS-0905222
§ Supported by an ASEE postdoctoral fellowship under contract to the NRL
¶ Naval Research Laboratory
‖ University at Albany—SUNY
** Partially supported by the NSF grant CNS-0905286
†† LORIA – INRIA Nancy-Grand Est

RESEARCH CENTRE
NANCY – GRAND EST

615 rue du Jardin Botanique
CS20101
54603 Villers-lès-Nancy Cedex

Unification asymétrique et problème de combinaison dans des théories disjointes

Résumé : L'unification asymétrique est un nouveau paradigme pour l'unification modulo des théories basé sur l'introduction de contraintes d'irréductibilité sur les membres droits d'un problème d'unification. Cette forme particulière d'unification a d'importantes applications dans l'analyse de protocoles cryptographiques où il est souvent nécessaire de mettre des contraintes d'irréductibilité sur des portions d'un état. Toutefois des facettes particulièrement intéressantes de l'unification asymétrique, comme son comportement dans des mélanges de théories disjointes, demeurent encore mal comprises. Dans ce papier, nous donnons une nouvelle formulation de la méthode de combinaison introduite par Baader et Schulz pour l'unification dans le mélange de théories équationnelles disjointes. Celle permet d'obtenir à la fois un nouvel éclairage du problème de combinaison disjointe et une extension de la méthode à l'unification asymétrique. On obtient ainsi la première méthode de combinaison pour l'unification asymétrique dans le mélange de théories équationnelles disjointes.

Mots-clés : Théorie équationnelle, Unification asymétrique, problème de combinaison

1 Introduction

We examine the disjoint combination problem in the newly developed paradigm of asymmetric unification. This new unification problem was developed based on newly identified requirements arising from symbolic cryptographic protocol analysis [9]. Its application involves unification-based exploration of a space in which the states obey rich equational theories that can be expressed as a decomposition $R \uplus E$, where R is a set of rewrite rules that is confluent, terminating and coherent modulo E. However, in order to apply state space reduction techniques, it is usually necessary for at least part of this state to be in normal form, and to remain in normal form even after unification is performed. This requirement can be expressed as an *asymmetric* unification problem $\{s_1 =^{\downarrow} t_1, \ \ldots, \ s_n =^{\downarrow} t_n\}$ where the $=^{\downarrow}$ denotes a unification problem with the restriction that any unifier leaves the right-hand side of each equation irreducible (see Definition 4).

The concept of asymmetric unification has its genesis in the unification method that is commonly used in symbolic analysis of cryptographic protocols. Here, two different requirements must be satisfied. The first is to have a generic unification algorithm that can be applied to a large class of equational theories that are encountered in cryptographic protocol analysis. The second is to guarantee that certain terms always be in normal form with respect to R (see Section 2), so that it is possible to apply state space reduction techniques. This is done by decomposing the theory into $R \uplus E$ so that R has the *finite variant property* [7] with respect to E, i.e., for any term t there is a finite set of irreducible variants $V(t)$ of pairs (u, σ), where u is a term and σ is a substitution, so that for each $(u, \sigma) \in V(t)$ we have $t\sigma \downarrow\!=_E u$ and for any substitution τ there is a $(u, \sigma) \in V(t)$ and a substitution ρ such that $t\tau \downarrow\!=_E u\rho$. In other words, the set of variants gives a complete representation of the irreducible forms of t under any substitution. A unification problem is then solved by computing the variants of each side and unifying those modulo E. This approach to unification is used in a number of tools, including ProVerif [4], OFMC [16], Maude-NPA [10], and Tamarin [15]. More recently, it has been formalized in a procedure known as *folding variant narrowing* [12], which terminates if and only if the terms being unified have a finite number of variants.

Although variant narrowing is sound and complete for theories with the finite variant property, it is not optimally efficient. In [8] it is pointed out that this issue can often be addressed by computing the set of variants of only one side of a unification problem $s =^{?} t$, replacing it with a new asymmetric problem $s =^{\downarrow} t_1, \ \ldots, s =^{\downarrow} t_n$. One may then apply more efficient special-purpose asymmetric unification algorithms that satisfy the irreducibility constraints. Recent work on asymmetric algorithms for exclusive-or [14], [9] and free Abelian groups [14] indicate that such algorithms can lead to significant enhancement of performance.

Although asymmetric unification has the potential of playing an important role in cryptographic protocol analysis, and possibly other unification-based state exploration as well, it is still not that well understood. Until the development of special-purpose algorithms for exclusive-or and free Abelian group theories mentioned above, the only known asymmetric unification algorithm was variant narrowing. Since then, some better understanding has been developed. For Example, we know that asymmetric unification is strictly harder than "symmetric" unification. In particular, there are theories for which symmetric unification is decidable and asymmetric unification is not. Still, there are many questions that remain to be answered. One of the most important of these unanswered questions is the problem of asymmetric unification in a combination of theories, in particular how to produce an algorithm for the combined theory by combining algorithms for the separate theories. This is particularly significant for cryptographic protocol analysis. Cryptographic protocols generally make use of more than one cryptoalgorithm. Often, these cryptoalgorithms can be described in terms of disjoint equational theories. In the case in

which the algorithm used is variant narrowing, the problem is straightforward. If the combination of two theories with the finite variant property also has the finite variant property, then one applies variant narrowing. However, in attempting to combine theories with special-purpose algorithms, the path is less clear. This is an important point with respect to efficiency since, as pointed out above, special-purpose asymmetric unification algorithms have the promise of being more efficient than variant narrowing.

In this paper we take the first step to solving this problem, by showing that the combination method for the unification problem in disjoint equational theories developed by Baader and Schulz in [2] can be modified and extended to the asymmetric unification paradigm, thus providing the first general combination method for this new paradigm. The only restrictions on this new method are those inherited from the asymmetric unification problem and those inherited from Baader and Schulz. From [2] we require that the algorithms being combined solve *the asymmetric unification with linear constant restriction problem*, although we show this reduces to solving the *general* asymmetric unification problem.

2 Preliminaries

We use the standard notation of equational unification [3] and term rewriting systems [1]. The set of Σ-terms, denoted by $T(\Sigma, \mathcal{X})$, is built over the signature Σ and the (countably infinite) set of variables $\mathcal{X}$. The terms $t|_p$ and $t[u]_p$ denote respectively the subterm of t at the position p, and the term t having u as subterm at position p. The symbol of t occurring at the position p (resp. the top symbol of t) is written $t(p)$ (resp. $t(\epsilon)$). The set of positions of a term t is denoted by $Pos(t)$, the set of non variable positions for a term t over a signature Σ is denoted by $Pos(t)_\Sigma$. A Σ-*rooted* term is a term whose top symbol is in Σ. The set of variables of a term t is denoted by $Var(t)$. A term is *ground* if it contains no variables. A term t is *linear* if each variable of t occurs only once in t.

A Σ-*substitution* σ is an endomorphism of $T(\Sigma, \mathcal{X})$ denoted by $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ if there are only finitely many variables $x_1, \ldots, x_n$ not mapped to themselves. We call the *domain* of σ the set of variables $\{x_1, \ldots, x_n\}$ and the *range* of σ the set of terms $\{t_1, \ldots, t_n\}$. Application of a substitution σ to a term t (resp. a substitution ϕ) may be written $t\sigma$ (resp. $\phi\sigma$).

Given a first-order signature Σ, and 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 will be often called an equational theory. An axiom $l = r$ is *variable-preserving* if $Var(l) = Var(r)$. An axiom $l = r$ is *linear* (resp. *collapse-free*) if l and r are linear (resp. non-variable terms). An equational theory is *variable-preserving* (resp. linear/ collapse-free) if all its axioms are variable-preserving (resp. linear/ collapse-free). An equational theory E is *finite* if for each term t, there are finitely many terms s such that $t =_E s$.

A Σ-equation is a pair of Σ-terms denoted by $s =^? t$. An E-unification problem is a set of Σ-equations, $\mathcal{S} = \{s_1 =^? t_1, \ldots, s_m =^? t_m\}$. The set of variables of $\mathcal{S}$ is denoted by $Var(\mathcal{S})$.

A solution to $\mathcal{S}$, called an *E-unifier*, is a substitution σ such that $s_i\sigma =_E t_i\sigma$ for all $1 \leq i \leq m$. 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 $x \in V$. Two substitutions θ_1 and θ_2 are *equivalent modulo* E on a set of variables V, denoted as $\theta_1 =_E^V \theta_2$, if and only if $x\theta_1 =_E x\theta_2$ for all $x \in V$. A *complete set of E-unifiers* of $\mathcal{S}$ is a set of substitutions denoted by $CSU_E(\mathcal{S})$ such that each $\sigma \in CSU_E(\mathcal{S})$ is an E-unifier of $\mathcal{S}$, and for each E-unifier θ of $\mathcal{S}$, there exists $\sigma \in CSU_E(\mathcal{S})$ such that $\sigma \leq_E^{Var(\mathcal{S})} \theta$.

Equational unification problems are classified based on the function symbols that appear in them, i.e., their signature (Sig). An E-unification problem S is *elementary* if and only if $Sig(S) =$

$Sig(E)$. S is called an E-unification problem *with constants* if $Sig(S) \setminus Sig(E)$ contains only free constants. Finally, if there are uninterpreted function symbols in $Sig(S) \setminus Sig(E)$, then S is called a general E-unification problem.

Let E_1 and E_2 be two equational theories built over the disjoint signatures Σ_1 and Σ_2. The elements of Σ_i will be called *i-symbols*. A term t is an *i-term* if and only if it is of the form $t = f(t_1, , \ldots, t_n)$ for an i-symbol f or t is a variable. An i-term is *pure (or an i-pure term)* if it only contains i-symbols and variables. An equation $s =^? t$ is i-pure (or just pure) iff there exists an i such that s and t are i-pure terms or variables. A subterm s of an i-term t is called an *alien subterm* (or just *alien*) of t iff it is a non-variable j-term, $j \neq i$, such that every proper superterm of s in t is an i-term. A unification problem S is an *i-pure problem* if all equations in S are i-pure.

Definition 1. *Let Γ be an E-unification problem, let $\mathcal{X}$ denote the set of variables occurring in Γ and $\mathcal{C}$ the set of free constants occurring in Γ. For a given linear ordering $<$ on $\mathcal{X} \cup \mathcal{C}$, and for each $c \in \mathcal{C}$ define the set V_c as $\{x \mid x \text{ is a variable with } x < c\}$. An* E-unification problem with linear constant restriction *(LCR) is an E-unification problem with constants, Γ, where each constant c in Γ is equipped with a set V_c of variables. A solution of the problem is an E-unifier σ of Γ such that for all c, x with $x \in V_c$, the constant c does not occur in $x\sigma$. We call σ an* E-unifier with linear constant restriction.

A *rewrite rule* is an ordered pair $l \to r$ such that $l, r \in T(\Sigma, \mathcal{X})$ and $l \notin \mathcal{X}$. We use R to denote a term rewrite system which is defined as a set of rewrite rules. The rewrite relation on $T(\Sigma, \mathcal{X})$, written $t \to_R s$, hold between t and s iff there exists a non-variable $p \in Pos_\Sigma(t)$, $l \to r \in R$ and a substitution σ, such that $t|_p = l\sigma$ and $s = t[r\sigma]_p$. The relation $\to_{R/E}$ on $T(\Sigma, \mathcal{X})$ is $=_E \circ \to_R \circ =_E$. The relation $\to_{R,E}$ on $T(\Sigma, \mathcal{X})$ is defined as: $t \to_{R,E} t'$ if there exists a position $p \in Pos_\Sigma(t)$, a rule $l \to r \in R$ and a substitution σ such that $t|_p =_E l\sigma$ and $t' = t[r\sigma]_p$. The transitive (resp. transitive and reflexive) closure of $\to_{R,E}$ is denoted by $\to^+_{R,E}$ (resp. $\to^*_{R,E}$). A term t is $\to_{R,E}$ *irreducible* (or in R, E-*normal form*) if there is no term t' such that $t \to_{R,E} t'$. If $\to_{R,E}$ is confluent and terminating we denote the irreducible version of a term, t, by $t \to^!_{R,E}$ or $t \downarrow_{R,E}$.

Definition 2. *A rewrite rule $l \to r$ is* duplicating *if r contains more occurrences of some variable than l; otherwise, $l \to r$ is* non-duplicating. *We say that R is non-duplicating if every $l \to r \in R$ is non-duplicating.*

Definition 3. *We call $(\Sigma,\ E,\ R)$ a* decomposition *of an equational theory Δ over a signature Σ if $\Delta = R \uplus E$ and R and E satisfy the following conditions:*

1. *E is variable preserving, i.e., for each $s = t$ in E we have $Var(s) = Var(t)$.*
2. *E has a finitary and complete unification algorithm. That is, an algorithm that produces a finite complete set of unifiers.*
3. *For each $l \to r \in R$ we have $Var(r) \subseteq Var(l)$.*
4. *R is confluent and terminating modulo E, i.e., the relation $\to_{R/E}$ is confluent and terminating.*
5. *The relation $\to_{R,E}$ is E-coherent, i.e., $\forall t_1, t_2, t_3$ if $t_1 \to_{R,E} t_2$ and $t_1 =_E t_3$ then $\exists\ t_4, t_5$ such that $t_2 \to^*_{R,E} t_4$, $t_3 \to^+_{R,E} t_5$, and $t_4 =_E t_5$.*

This definition is inherited directly from [9] where asymmetric unification and the corresponding theory decomposition are first defined. The last restrictions ensure that $s \to^!_{R/E} t$ iff $s \to^!_{R,E} t$ (see [11], [9]).

Definition 4 (Asymmetric Unification)**.** *Given a decomposition* (Σ, E, R) *of an equational theory, a substitution* σ *is an* asymmetric R, E-unifier *of a set* $\mathcal{S}$ *of asymmetric equations* $\{s_1 =^{\downarrow} t_1, \ \ldots, \ s_n =^{\downarrow} t_n\}$ *iff for each asymmetric equations* $s_i =^{\downarrow} t_i$, σ *is an* $(E \cup R)$*-unifier of the equation* $s_i =^{?} t_i$ *and* $(t_i \downarrow_{R,E})\sigma$ *is in* R, E*-normal form. A set of substitutions* Ω *is a* complete set of asymmetric R, E*-unifiers of* $\mathcal{S}$ *(denoted* $CSAU_{R\cup E}(\mathcal{S})$ *or just* $CSAU(\mathcal{S})$ *if the background theory is clear) iff: (i) every member of* Ω *is an asymmetric* R, E*-unifier of* $\mathcal{S}$*, and (ii) for every asymmetric* R, E*-unifier* θ *of* $\mathcal{S}$ *there exists a* $\sigma \in \Omega$ *such that* $\sigma \leq_E^{Var(\mathcal{S})} \theta$*.*

Example 1. *Let* $R = \{x \oplus 0 \to x, \ x \oplus x \to 0, \ x \oplus x \oplus y \to y\}$ *and* E *be the AC theory for* $\oplus$*. Consider the equation* $y \oplus x =^{\downarrow} x \oplus a$*, the substitution* $\sigma_1 = \{y \mapsto a\}$ *is an asymmetric solution but,* $\sigma_2 = \{x \mapsto 0, \ y \mapsto a\}$ *is not.*

Definition 5 (Asymmetric Unification with Linear Constant Restriction)**.** *Let* $\mathcal{S}$ *be a set of of asymmetric equations with some LCR. A substitution* σ *is an* asymmetric R, E-unifier *of* $\mathcal{S}$ *with LCR iff* σ *is an asymmetric solution to* $\mathcal{S}$ *and* σ *satisfies the LCR.*

3 Combining Asymmetric Unification Algorithms

Here we modify and extend the method for unification in the union of disjoint equational theories, developed by Baader and Schulz [2], to the combination of *asymmetric* unification algorithms in the union of disjoint equational theories.

3.0.1 Problem Description:

Let Δ_1 and Δ_2 denote two equational theories with disjoint signatures Σ_1 and Σ_2. Let Δ be the combination, $\Delta = \Delta_1 \cup \Delta_2$, of the two theories having signature $\Sigma_1 \cup \Sigma_2$. Let A_i, $i \in \{1, 2\}$, be an asymmetric Δ_i-unification with linear constants restriction algorithm. We then give an algorithm which uses A_1 and A_2 to solve the *elementary* asymmetric unification problem over Δ. Recall that elementary implies that terms can only contain symbols in the signature of the theory or variables. But this is not restrictive, if we wish to have additional free functional symbols, these function symbols define a new empty theory and lead to another combination. Therefore, in what follows we will assume that a problem, Γ_0, in the combined theory Δ, is an elementary asymmetric Δ-unification problem. In order to satisfy the requirements for asymmetric unification we make the following assumptions.
Restrictions: for each constituent theory (Σ_i, Δ_i):

1. There is a decomposition $\Delta_i = R_i \uplus E_i$ and $u \to^{!}_{R_i,E_i} v$ iff $u \longrightarrow^{!}_{R_i/E_i} v$ (see note (2) below).
2. E_i is collapse-free and there exists a finitary E_i-unification algorithm.
3. There exists a finitary complete asymmetric Δ_i-unification algorithm with linear constants restriction, A_i (see note (3) below).
4. Variables are $\to_{R_i,E_i}$-normal forms.
5. Each R_i is non-duplicating.

Notes on the Restrictions:

1. All Restrictions, except (3), are due to the asymmetric unification definition.

2. The definition of decomposition requires that $\longrightarrow_{R_i/E_i}$ be confluent and terminating. Thus, if $u \to^!_{R_i,E_i} v$ iff $u \longrightarrow^!_{R_i/E_i} v$, we have that $\to_{R_i,E_i}$ is also confluent and terminating.
3. We show in Section 3.5 that there exists an asymmetric Δ_i-unification algorithm with linear constants restriction if there exists a *general* asymmetric Δ_i-unification algorithm.

According to our Restrictions, E_1 and E_2 are both variable preserving and collapse-free. Consequently, we have the following property:

Lemma 1. *$t \neq_{E_1 \cup E_2} s$, if t is a non-variable i-term and s is a non-variable j-term, $j \neq i$.*

3.1 Rewriting in the Combined Theory

The definition of asymmetric unification in the combined theory Δ, where $\Delta = \Delta_1 \cup \Delta_2$, requires us to not only find Δ-unifiers but also decide if a term is in $\to_{(R_1 \cup R_2),(E_1 \cup E_2)}$ normal form. Therefore, we need to first ensure the modularity of rewriting, i.e., ensure that we can compute $\longrightarrow_{(R_1 \cup R_2),(E_1 \cup E_2)}$-normal forms.

Consider now the combined theory (Σ, Δ), where $\Sigma = \Sigma_1 \cup \Sigma_2$ and $\Delta = \Delta_1 \cup \Delta_2$. Let $\mathcal{R} = R_1 \cup R_2$ and $\mathcal{E} = E_1 \cup E_2$. *Therefore, $\to_{\mathcal{R},\mathcal{E}}$ denotes $\to_{R_1 \cup R_2, E_1 \cup E_2}$.*

Theorem 1. $\to_{\mathcal{R},\mathcal{E}} = \longrightarrow_{R_1,E_1} \cup \longrightarrow_{R_2,E_2}$

Proof. Follows from the the fact that $\Sigma_1 \cap \Sigma_2 = \emptyset$ and $\mathcal{E} = E_1 \cup E_2$ is variable preserving and collapse-free. □

The relation $\longrightarrow_{R_i,E_i}$ is decidable for each sub-theory due to the assumption that $\longrightarrow_{R_i,E_i}$ is convergent. Therefore we obtain the following corollary to Theorem 1.

Corollary 1. *The relation $\longrightarrow_{\mathcal{R},\mathcal{E}}$ is decidable.*

Note, with respect to termination, $R_1 \cup R_2$ is non-duplicating, this is due to the disjoint theories and the fact that each R_i is non-duplicating by assumption. Since $R_1 \cup R_2$ is non-duplicating termination is obtained due to the results of [17], where it is shown that non-duplicating implies termination in the combination of terminating rewrite systems. Next we would like to know that $\longrightarrow_{\mathcal{R},\mathcal{E}}$ is complete with respect to $\longrightarrow_{\mathcal{R}/\mathcal{E}}$, i.e., $u \to^!_{R_i,E_i} v$ iff $u \longrightarrow^!_{R_i/E_i} v$, which is not true in general. For this to be true we need to know that $\longrightarrow_{\mathcal{R},\mathcal{E}}$ is $\mathcal{E}$-coherent, which implies the result (see [11]).

Lemma 2. *If there exist terms t_0, t_1 and t_2 such that $t_0 \leftrightarrow^*_{\mathcal{E}} t_2$ and $t_0 \to_{\mathcal{R},\mathcal{E}} t_1$ then there exists a term t_3 such that $t_2 \to_{\mathcal{R},\mathcal{E}} t_3$.*

Proof. If $t_0 = t_2$ then the result follows. Therefore, let $t_0 \leftrightarrow^+_{\mathcal{E}} t_2$, which implies that

$$t_0 = k_1 \leftrightarrow_{d_1=g_1} k_2 \leftrightarrow_{d_2=g_2} k_2 \ldots \leftrightarrow_{d_n=g_n} k_m = t_2$$

where each $d_l = g_l \in E_1 \cup E_2$.

We can now proceed by induction on m, demonstrating at each step there exists a $\to_{\mathcal{R},\mathcal{E}}$ reduction. Consider a step $k_l \leftrightarrow_{d_l=g_l} k_{l+1}$ and assume that $k_l \to_{\mathcal{R},\mathcal{E}} u$ for some term u. By the assumptions, there exist p, q, σ, δ and $l \to r \in R_1 \cup R_2$ such that $k_l|_p = d_l\sigma$, $k_{l+1} = k_l[g_l\sigma]_p$, $k_l|_q =_{E_1 \cup E_2} l\delta$ and $u = k_l[r\delta]_q$. If $p||q$ (not comparable with respect to the prefix ordering) then the result follows, so we assume that p and q are comparable with respect to the prefix ordering. Without loss of generality assume that k_l is an i-term, for $i \in \{1, 2\}$. We can also assume that one (or both) p or q occur in $(k_l)^{\pi_i}$. Otherwise, we could just consider the alien subterm which contains both reductions.

Now assume that $p \leq q$ which implies that $q = pq'$, i.e., p is a prefix of q. Since one or both p and q occur in $(k_l)^{\pi_i}$ and $p \leq q$, we have that p is a non-variable position in $(k_l)^{\pi_i}$, which implies $d_l = g_l \in E_i$ since the signatures of E_1 and E_2 are disjoint.

We then have two cases: first, the term rooted at q is not an alien subterm and second, the term rooted at q is an alien subterm.

1. If $k_l|_q$ is not an alien then its is also an i-term, which implies that $l \to r \in R_i$ and $k_l|_q =_{E_i} l\delta$. In this case the result follows due to the coherence property of $\to_{R_i,E_i}$. That is, since $k_l =_{E_i} k_{l+1}$, $k_l \to_{R_i,E_i} u$, there exists some u' such that $k_{l+1} \to_{R_i,E_i} u'$, which is a reduction in k_{l+1}.

2. Otherwise, the term rooted at q is an alien and thus a j-term ($j \neq i$). If we consider $(k_l)^{\pi_i}$, then $k_l|_q$ under the projection π_i is a variable y. Since E_1 and E_2 are variable-preserving, the variable y is maintained in the following sequence:

$$k_l =_{\mathcal{E}} (k_l[d_l\sigma]_p)^{\pi_i}\pi^{-1} =_{\mathcal{E}} (k_l[g_l\sigma]_p)^{\pi_i}\pi^{-1} =_{\mathcal{E}} k_{l+1}$$

Therefore, y occurs in $(k_l[g_l\sigma]_p)^{\pi_i}$ at some position q' and since $y\pi^{-1} =_{\mathcal{E}} l\delta$, we have that $k_{l+1}|_{q'} =_{\mathcal{E}} l\delta$, i.e., there is a reduction in k_{l+1}.

Now assume that $q \leq p$ which implies that $p = qp'$. We again have two cases.

1. If both p and q occur in $(k_l)^{\pi_i}$ we can again use the coherence property to show the result.

2. Now assume that the term rooted at p is an alien subterm. In this case the result follows since changing an alien subterm via $E_1 \cup E_2$ will not effect a reduction in the superterm via $\to_{\mathcal{R},\mathcal{E}}$. Since $(k_l|_q)^{\pi_i} =_{E_i} (k_{l+1}|_q)^{\pi_i}$, we have

$$l\delta =_{\mathcal{E}} k_l|_q =_{\mathcal{E}} (k_l|_q)^{\pi_i}\pi^{-1} =_{\mathcal{E}} (k_{l+1}|_q)^{\pi_i}\pi^{-1} =_{\mathcal{E}} k_{l+1}|_q$$

which implies a reduction in k_{l+1}.

□

Theorem 2. *$\to_{\mathcal{R},\mathcal{E}}$ is $\mathcal{E}$-coherent.*

Proof. If $t_0 \to_{\mathcal{R},\mathcal{E}} t_1$ and $t_0 =_{\mathcal{E}} t_2$, then by Lemma 2, there exists a term, t_3, such that $t_2 \to_{\mathcal{R},\mathcal{E}} t_3$. Thus, $t_1 \longleftrightarrow_{R_1\cup R_2\cup E_1\cup E_2} t_3$. Now the combined system has the properties (normal form variables, E_i collapse-free, and disjoint signatures) such that the Church-Rosser result in [13] applies. This implies the existence of terms t_4 and t_5 such that $t_1 \to^*_{\mathcal{R},\mathcal{E}} t_4$, $t_3 \to^*_{\mathcal{R},\mathcal{E}} t_5$ and $t_4 =_{\mathcal{E}} t_5$. □

Therefore, based on Corollary 1 and Theorem 2, $u \to^*_{\mathcal{R},\mathcal{E}} v$ iff $u \to^*_{\mathcal{R}/\mathcal{E}} v$ which implies the following:

Theorem 3. *$t =_{\mathcal{R}\cup\mathcal{E}} s$ iff $t\downarrow_{\mathcal{R},\mathcal{E}} =_{\mathcal{E}} s\downarrow_{\mathcal{R},\mathcal{E}}$*

3.2 Asymmetry in the Projection of Terms

Now that we have established the modular results for rewriting we can use the well defined normal forms to define projections onto pure terms. Later we will use the bijection defined below to prove that if the original problem has a solution then there exists solutions to the pure sub-problems. This is accomplished by mapping the combined solution into two pure solutions. In order for this to work we also need to ensure that equality modulo E and asymmetric restrictions

are maintained after the mapping is applied. Let $\mathcal{X}$ and $\mathcal{Y}$ be disjoint sets of variables that are countably infinite. Let $T(\Sigma, \mathcal{X})$ be the set of $\Sigma_1 \cup \Sigma_2$-terms over $\mathcal{X}$. We define a bijection

$$\pi : (T(\Sigma, \mathcal{X}) \downarrow_{\mathcal{R},\mathcal{E}})_{/=_\mathcal{E}} \to \mathcal{Y} \tag{1}$$

The bijection π induces two mappings π_1 and π_2 of terms in $T(\Sigma, \mathcal{X})$ to terms in $T(\Sigma, \mathcal{Y})$ as follows. For each $x \in \mathcal{X}$, $x^{\pi_1} := \pi(x)$. If $t = f(t_1, \ldots, t_n)$ for a 1-symbol f, then $t^{\pi_1} := f(t_1^{\pi_1}, \ldots, t_n^{\pi_1})$. If t is a 2-term then $t^{\pi_1} := y$ where $y = \pi([s]_\mathcal{E})$ for the unique $\to_{\mathcal{R},\mathcal{E}}$-irreducible term s of t, where $[s]_\mathcal{E}$ denotes the equivalence class of s modulo $\mathcal{E}$. The mapping π_2 is defined analogously.

Given a substitution σ, σ^{π_i} denotes the abstraction defined by $\sigma^{\pi_i}(x) = (\sigma(x))^{\pi_i}$, for all x is the domain of σ. These two mapping can be seen as projections from mixed terms into pure terms. More informally, we can view an i-abstraction as method for converting a mixed term into a pure term by replacing the alien subterms with variables. Recall that we assume that variables are $\longrightarrow_{R_i,E_i}$-irreducible and thus by modularity $\to_{\mathcal{R},\mathcal{E}}$-irreducible. As in [2] we can also define the inverse, π^{-1} of π as a substitution that maps the variables $y \in \mathcal{Y}$ back to terms $\pi^{-1}(y)$ and is the identity on all other variables. Note that, $\pi^{-1}(t^{\pi_i}) =_\mathcal{E} t$, if t is in $\mathcal{R},\mathcal{E}$-normal form or an i-term with normal form aliens.

Theorem 4. *Let s and t be i-pure terms. Let t and σ be in $\mathcal{R},\mathcal{E}$-normal form, such that $s\sigma =_\Delta t\sigma$. Then $s\sigma^{\pi_i} =_{\Delta_i} t\sigma^{\pi_i}$ and $t\sigma$ is in $\mathcal{R},\mathcal{E}$-normal form iff $t\sigma^{\pi_i}$ is in R_i, E_i-normal form.*

Proof. We can without loss of generality assume that t is in $\to_{\mathcal{R},\mathcal{E}}$-normal form. If $(s\sigma) =_{\Delta_i} (t\sigma)$ then

$$(s\sigma) \xrightarrow[\mathcal{R},\mathcal{E}]{*} r \longleftrightarrow_\mathcal{E} u \xleftarrow[\mathcal{R},\mathcal{E}]{*} (t\sigma)$$

We first show that $(s\sigma)^{\pi_i} \xrightarrow[R_i,E_i]{} r^{\pi_i}$. Then by symmetry we get that $(s\sigma)^{\pi_i} =_{\Delta_i} (t\sigma)^{\pi_i}$. It will then remain to show the asymmetric property.

Consider $(s\sigma) = s_0 \to_{\mathcal{R},\mathcal{E}} s_1 \to_{\mathcal{R},\mathcal{E}} \ldots \to_{\mathcal{R},\mathcal{E}} r$. We need to show that this implies that $s_0^{\pi_i} \longrightarrow_{R_i,E_i} s_1^{\pi_i} \longrightarrow_{R_i,E_i} \ldots \longrightarrow_{R_i,E_i} r^{\pi_i}$. Since we assume that variables are irreducible the case where s is a variable is trivial. Thus lets assume that s is an i-pure term and consider $s\sigma$. Notice since σ is $\to_{\mathcal{R},\mathcal{E}}$-reduced the position, p, of the redex in $s\sigma$ must be a non-variable position in s and thus an i-term. This implies that $s_0 \to_{R_i,E_i} s_1$ or that there exists a $\to_{\mathcal{R},\mathcal{E}}$*-reduced* substitution δ, a position p (corresponding to a position, and thus an i-pure subterm, in s) and rule $l \to r \in R_i$ such that $s_0|_p =_{E_i} l\delta$ and $s_1 = s_0[r\delta]_p$.

Let u be the redex in s_0, then $s_0^{\pi_i} = s_0^{\pi_i}[u^{\pi_i}]_p$ and $s_1^{\pi_i} = s_0^{\pi_i}[(r\delta)^{\pi_i}]_p$. Since the reduction must occur at a position corresponding to an i-pure term we have that

$$(s_0)^{\pi_i}|_p = u^{\pi_i} =_{E_i} (l\delta)^{\pi_i} = l\delta^{\pi_i} \to_{R_i} r\delta^{\pi_i} = (r\delta)^{\pi_i}$$

which implies that $s_0^{\pi_i} \longrightarrow_{R_i,E_i} s_1^{\pi_i}$. Now since E_i is variable-preserving and $Var(r) \subseteq Var(l)$, the reduction does not introduce new variables such that under the image of δ new reducible alien subterms are produced. Therefore, we can proceed by induction to show that $s_0^{\pi_i} \longrightarrow_{R_i,E_i} s_1^{\pi_i} \longrightarrow_{R_i,E_i} \ldots \longrightarrow_{R_i,E_i} r^{\pi_i}$.

Now, we need only show that $(t\sigma)^{\pi_i}$ is in $\to_{R_i,E_i}$-normal form. Assume that this is not the case, that there exists a position, p in $((t\sigma)^{\pi_i})$, a rule, $l \to r$, in R_i and a E_i-matching substitution, θ, such that $(t\sigma)^{\pi_i}|_p =_{E_i} l\theta$. Then, by the definition of π^{-1} we have

$$(t\sigma)|_q =_{E_1 \cup E_2} (t\sigma)^{\pi_i}|_p\pi^{-1} =_{E_i} l\theta\pi^{-1} = l\theta'$$

$$(t\sigma)|_q =_\mathcal{E} l\theta'$$

For some position q in $t\sigma$, which exists due to $\mathcal{E}$ being collapse-free and variable preserving. However, this contradicts the assumption that $t\sigma$ was in $\to_{\mathcal{R},\mathcal{E}}$-normal form. □

3.3 Asymmetric Unification with Linear Constant Restriction

We present the combination Algorithm, *AsymComb*, in Figure 1. Let us first give a rough, intuitive overview of the steps. First, equations are purified using variable abstraction and splitting (steps 1 and 2). This ensures that the original problem is separated into pure problems which can be solved by the algorithms for the pure theories. Next, a variable identification is non-deterministically chosen, allowing for the testing all the ways the variables may be equated to other variables. Then, a linear ordering and theory indices are non-deterministically chosen. Note that a shared variable can only "belong" exclusively to one theory. Since we don't know beforehand what variable belongs to which theory the non-deterministic selections allow us to check all the possibilities. In addition, each solution to the original problem will correspond to one or more linear ordering among the variables. Next, the problem is split into two pure problems where the linear ordering defines a linear constant restriction. The pure problems are solved by asymmetric unification algorithms with linear constant restriction. The solutions returned by the sub-algorithms are combined into solutions for the original problem. The Algorithm *AsymComb* (cf. Figure 1) must also ensure that we only combine a specific type of unifier, which ensures asymmetry.

The notions of identification, theory indexes and linear constant restrictions, have all been used in [2] (see Section 2 for definitions). In order to handle the asymmetry restriction we introduce two additional notions, which ensure pure problem solutions having these properties will result in asymmetric combined solutions.

Definition 6. *(Injective)*
A substitution, σ_i, is said to be injective *modulo Δ_i if for any two variables x, y in the domain of σ_i, we have that $x\sigma_i =_{\Delta_i} y\sigma_i$ if and only if $x = y$.*

Definition 7. *(Theory Preserving)*
A substitution σ_i, solving an i-pure problem Γ_i, is said to be theory preserving *if for any variable x of index i in the domain of σ_i, $x\sigma_i$ is not a variable of index $j \neq i$.*

With respect to the combination algorithm this definition basically states that a substitution σ_i, which solves an i-pure problem, Γ_i, produced by Algorithm *AsymComb* (cf. Figure 1), is theory-preserving if for all $x \in Dom(\sigma_i)$, $x\sigma_i \neq c$ where c is a free constant. This is due to the fact that for the pure sub-problems produced by the combination algorithm the only free constants will be those corresponding to shared variables of a different index. *Note, the definition of theory-preserving does not restrict σ_i from sending an i-variable x to a non-variable i-term whose leafs are j-variables.* Thus, if $x\sigma_i = t$ and t is an i-term, then t may contain j-variables. In addition, since the Algorithm *AsymComb* assigns the variable indexes, it can always check the substitutions returned by the algorithms for the pure theories to ensure that they are injective and theory-preserving.

Definition 8. *Let σ_1 and σ_2 be unifiers with linear constant restriction for $\Gamma_{5,1}$ and $\Gamma_{5,2}$ such that $\Gamma_{5,i}$ is the set of i-pure equations from Γ_4 and $<$ is the corresponding linear ordering. The* combined solution *$\sigma_1 \odot \sigma_2$ is defined by induction on $<$:*

Let x be the least variable with respect to the ordering $<$ from step 4 and let i be its index. Since the solution σ_i of $\Gamma_{5,i}$ satisfies the constant restriction induced by $<$, $x\sigma_i$ does not contain any variables of index $j \neq i$. We define $x(\sigma_1 \odot \sigma_2)$ to be $x\sigma_i$.

Let x be an arbitrary variable of index i and let $y_1, \ldots, y_m$ be the variables of index $j \neq i$ occurring in $x\sigma_i$. Again, due to the constant restriction, the variables $y_1, \ldots, y_m$ have to be smaller than x. This implies that $y_1(\sigma_1 \odot \sigma_2), \ldots, y_m(\sigma_1 \odot \sigma_2)$ are already defined. The term $x(\sigma_1 \odot \sigma_2)$ is obtained from $x\sigma_i$ by replacing y_k by $y_k(\sigma_1 \odot \sigma_2)$, and we define $x(\sigma_1 \odot \sigma_2)$ to be $x\sigma_i(\sigma_1 \odot \sigma_2)$.

Input: Γ_0, the initial unification problem over the signature $\Sigma_1 \cup \Sigma_2$, where we assume the right hand sides of the equations are normalized.

1. **Variable Abstraction**: Let $s =^{\downarrow} t \in \Gamma_0$.
   (a) Right Abstraction: For each alien subterm t_1 of t, let x be a variable not occurring in the current system and let t' be the term obtained from replacing t_1 by x in t. Then the original equation is replaced by two equations $s =^{\downarrow} t'$ and $x =^{\downarrow} t_1$.
   (b) Left Abstraction: For each alien subterm s_1 of s let x be a variable not occurring in the current system and let s' be the term obtained from replacing s_1 by x in s. Then the original equation is replaced by two equations $s' =^{\downarrow} t$ and $s_1 =^{\downarrow} x$.

   The output is a system Γ_1 such that all terms are pure.
2. **Split non-pure equations**: Each non-pure equation of the form $s =^{\downarrow} t$ is replaced by two equations $s =^{\downarrow} x$, $x =^{\downarrow} t$ where x is always a new variable. The results is a system Γ_2 of pure equations.
3. **Variable Identification**: Consider all the possible partitions of the set of variables. Each partition produces a new system Γ_3 as follows. The variables in each class of the partition are "identified" with each other by choosing an element of the class as a representative and replacing in the system all occurrences of variables in each class by their representative.
4. **Choose an ordering and Theory index**: For each Γ_3 we consider all the possible strict orderings $<$ on the variables of the system and all mappings *ind* from the set of variables into the set of indices $\{1, 2\}$. Each pair $(<, ind)$ yields a new system Γ_4.
5. **Split the system**: Each Γ_4 is split into two systems $\Gamma_{5,1}$ and $\Gamma_{5,2}$, the first containing only 1-equations and the second only 2-equations. In the system $\Gamma_{5,i}$ the variables of index $j \neq i$ are treated as constants. Each $\Gamma_{5,i}$ is now a unification problems with linear constant restriction, where the linear ordering $<$ defines the set V_c for each constant c corresponding to an index $j \neq i$ variable.
6. **Compute** $M_{i,j}$: For the initial system Γ_0 let $\{(\Gamma^1_{5,1}, \Gamma^1_{5,2}), \ldots, (\Gamma^n_{5,1}, \Gamma^n_{5,2})\}$ be the output of the decomposition. For $i = 1, \ldots, n$ and $j = 1, 2$, let $M_{i,j} = CSAU_{\Delta_j}(\Gamma^i_{5,j})$ produced by Algorithm A_j, where substitutions that are non-injective and not theory-preserving are discarded.
7. **Output**: For $i = 1, \ldots, n$ the set of substitutions $\sigma_1 \odot \sigma_2$ such that $\sigma_1 \in M_{i,1}$ and $\sigma_2 \in M_{i,2}$.

Figure 1: Algorithm *AsymComb*

Lemma 3. *(Baader-Schulz [2])*
The combined unifier $\sigma_1 \odot \sigma_2$ from Definition 8 is a unifier of Γ_4.

Example 2. *Let $\Delta_1 = R_1 \cup E_1$, where $R_1 = \{e(x, d(x, y)) \to y,\ d(x, e(x, y)) \to y\}$ and $E_1 = \emptyset$. Let $\Delta_2 = R_2 \cup E_2$, where $R_2 = \{x \oplus 0 \to x,\ x \oplus x \to 0,\ x \oplus x \oplus y \to y\}$ and $E_2 = \{x \oplus y = y \oplus x,\ (x \oplus y) \oplus z = x \oplus (y \oplus z)\}\}$. Let $\Delta = \Delta_1 \cup \Delta_2$.*

Consider the initial problem Γ_0 consisting of the following:
$\{x_0 \oplus x_1 \oplus x_2 =^{\downarrow} x_3 \oplus x_4,\ e(x_1, d(0, x_5)) =^{\downarrow} x_2 \oplus x_0,\ e(x_1, d(x_0, e(x_2, x_6))) =^{\downarrow} e(x_7, x_5)\}$

Let us now examine the action of Algorithm AsymComb *(cf. Figure 1) on Γ_0 and how it would find a particular asymmetric solution. The first 2 steps produce the set of pure equations Γ_2:*
$\{x_0 \oplus x_1 \oplus x_2 =^{\downarrow} x_3 \oplus x_4,\ e(x_1, d(z_0, x_5)) =^{\downarrow} z_1,\ 0 =^{\downarrow} z_0,\ z_1 =^{\downarrow} x_2 \oplus x_0,\ e(x_1, d(x_0, e(x_2, x_6))) =^{\downarrow} e(x_7, x_5)\}$.

The next step considers the set of variable partitions, one of which is the following partition

$\{\{x_0, x_3\}, \{x_2, x_4\}, \{x_5, z_1\}, \{x_1, z_0, x_7\}, \{x_6\}\}$ *Choosing a representative for each set and doing the replacement the Algorithm would produce the following* Γ_3 *from that partition:* $\{x_0 \oplus x_1 \oplus x_2 =^{\downarrow} x_0 \oplus x_2,\ e(x_1, d(x_1, x_5)) =^{\downarrow} x_5,\ 0 =^{\downarrow} x_1,\ x_5 =^{\downarrow} x_2 \oplus x_0,\ e(x_1, d(x_0, e(x_2, x_6))) =^{\downarrow} e(x_1, x_5)\}$.

The next step considers the possible pairs of variable orderings and theory indexes. One pair that would be produced is the following: $x_6 > x_5 > x_2 > x_1 > x_0$, *index*-1 $= \{x_0, x_1, x_2, x_5\}$ *and index*-2 $= \{x_6\}$.

Next Γ_4 *is produced from that pair and split into pure sets to produce* $\Gamma_{5,1}$ *and* $\Gamma_{5,2}$. *Let us denote a variable,* y, *being treated as a constant as* $\mathbf{y}$. *Then,* $\Gamma_{5,1}$ *is the following set of equations:* $\{x_0 \oplus x_1 \oplus x_2 =^{\downarrow} x_0 \oplus x_2,\ 0 =^{\downarrow} x_1,\ x_5 =^{\downarrow} x_2 \oplus x_0\}$ *and* $\Gamma_{5,2}$ *is the following set of equations:* $\{e(\boldsymbol{x}_1, d(\boldsymbol{x}_1, \boldsymbol{x}_5)) =^{\downarrow} \boldsymbol{x}_5,\ e(\boldsymbol{x}_1, d(\boldsymbol{x}_0, e(\boldsymbol{x}_2, x_6))) =^{\downarrow} e(\boldsymbol{x}_1, \boldsymbol{x}_5)\}$

Next $\Gamma_{5,1}$ *is solved with* A_1 *and* $\Gamma_{5,2}$ *with* A_2, *where the linear constant restriction is obtained via the linear ordering and theory index. The last step is to combine each pair of substitutions* (σ_1, σ_2) *into a substitution* σ, *where* σ_i *is an injective and theory-preserving asymmetric with LCR solution to* $\Gamma_{5,i}$ *returned by* A_i. *One such pair is* $\sigma_1 = \{x_1 \mapsto 0,\ x_5 \mapsto x_2 \oplus x_0\}$ *and* $\sigma_2 = \{x_6 \mapsto d(\boldsymbol{x}_2, e(\boldsymbol{x}_0, \boldsymbol{x}_5))\}$. *Applying Definition 8 we get the following solution,* $\{x_1 \mapsto 0,\ x_3 \mapsto x_0,\ x_4 \mapsto x_2,\ x_5 \mapsto x_2 \oplus x_0,\ x_6 \mapsto d(x_2, e(x_0, x_2 \oplus x_0)),\ x_7 \mapsto 0\}$, *which is an asymmetric solution to* Γ_0 *(existential variables* z_0, z_1 *are removed).*

Before presenting the proof details lets us briefly point out the main differences between Algorithm *AsymComb* (cf. Figure 1) and the algorithm of [2]. While the general framework of the two algorithms is similar there are several key differences. First, we do not consider general theories. Due to the restrictions inherited from the definition of asymmetric unification we must consider theories with specific structure, namely the decomposition. This requires new results for showing the correctness of the algorithm and new results for showing that the required properties for asymmetric unification are maintained. Second, we must identify the specific unifiers which satisfy the asymmetry. We accomplish this by identifying two key properties, theory preservation (Definition. 7) and injectivity (Definition. 6).

3.4 Correctness

We show in this section that the Algorithm *AsymComb* (cf. Figure 1) is both sound and complete for the decision problem. In addition, we show that the algorithm produces a complete set of asymmetric unifiers.

Lemma 4. *Assume that* σ_1 *and* σ_2 *are pure, injective, theory-preserving and* R_i, E_i*-normalized unifiers modulo respectively* $\Delta_1 = R_1 \uplus E_1$ *and* $\Delta_2 = R_2 \uplus E_2$ *and they satisfy the same linear constant restriction. Then, the substitution* $\sigma = \sigma_1 \odot \sigma_2$ *satisfies the following properties: (1)* σ *is an injective substitution modulo* $\Delta_1 \cup \Delta_2$. *(2)* σ *is* $\mathcal{R}, \mathcal{E}$*-normalized.*

Proof. We proceed by induction on the linear ordering.
Base case: Let v be the smallest variable, say of index i. Then, σ is clearly injective and $\mathcal{R}, \mathcal{E}$-normalized for variables smaller or equal to v, since $v\sigma = v\sigma_i$ is R_i, E_i-normalized, and so also $\mathcal{R}, \mathcal{E}$-normalized.

Inductive case: Assume the the properties holds for variables smaller than a variable y of index i. To show that (1) holds, assume by contradiction that there exists a variable x strictly smaller than y such that $x\sigma =_{\Delta_1 \cup \Delta_2} y\sigma$. Since σ is $\mathcal{R}$, $\mathcal{E}$-normalized for variables smaller than y, we have that $x\sigma =_{\Delta_1 \cup \Delta_2} y\sigma$ implies $x\sigma^{\pi_i} =_{\Delta_i} y\sigma^{\pi_i}$. Since σ is injective for variables smaller than y, there exists a renaming ρ such that $x\sigma^{\pi_i}\rho = x\sigma_i$ and $y\sigma^{\pi_i}\rho = y\sigma_i$. Therefore $x\sigma_i =_{\Delta_i} y\sigma_i$, which is a contradiction.

Consider now the property (2): if $y\sigma$ is $\mathcal{R},\mathcal{E}$-reducible, then $(y\sigma)^{\pi_i}$ is R_i, E_i-reducible, which means that $y\sigma_i\rho$ and $y\sigma_i$ are R_i, E_i-reducible too, which contradicts the assumption that σ_i is an R_i, E_i-normalized substitution. □

Lemma 5. *Let Γ_0 be a solvable asymmetric Δ-unification problem, where $\Delta = \Delta_1 \cup \Delta_2$. Assume there exists a pair $(\Gamma_{5,1}, \Gamma_{5,2})$ produced by the Algorithm* AsymComb *(cf. Figure 1) on Γ_0 and a pair (σ_1, σ_2) such that $\sigma_i \in CSAU_{\Delta_i}(\Gamma_{5,i})$ for $i = 1, 2$.*
Then, there exists pairs $(\Gamma'_{5,1}, \Gamma'_{5,2})$ produced by the Algorithm AsymComb on Γ_0 and a pair (ϕ_1, ϕ_2) such that ϕ_i is injective *and* theory-preserving*, $\phi_i \in CSAU_{\Delta_i}(\Gamma'_{5,i})$ for $i = 1, 2$, and $\phi_1 \odot \phi_2 \leq^{Var(\Gamma_0)}_{\Delta} \sigma_1 \odot \sigma_2$.*

Proof. Construct $(\Gamma'_{5,1}, \Gamma'_{5,2})$ and (σ'_1, σ'_2): Let Γ_4 be the conjunction of $\Gamma_{5,1}$ and $\Gamma_{5,2}$. Then there exists a linear ordering, $<$, and a theory index, *ind*. From Γ_4 we can construct a new Γ'_4 as follows: If there exists x, y in the domain of σ_i such that $x\sigma_i =_{\Delta_i} y\sigma_i$ we add $x = y$ to the variable identification. If there exists variables x, y such that x is an index i variable, y is an index j variable and $x\sigma_i = y$, we replace all x with y in the variable identification. *ind* and $<$ remain the same. The result of these steps is a new Γ'_4, which also gives us a new pair $(\Gamma'_{5,1}, \Gamma'_{5,2})$. We can now define the new pair of substitutions (σ'_1, σ'_2) as follows: Let $Dom(\sigma'_i) = Var(\Gamma'_{5,i})$. $\forall x \in Dom(\sigma'_i)$, $x\sigma'_i = x\sigma_i$ and is the identity on all other variables.

Show that σ'_1 and σ'_2 are theory-preserving and injective unifiers of $\Gamma'_{5,1}$ and $\Gamma'_{5,2}$: This follows from the construction of Γ'_4, where variables violating the definitions have been removed.

Show that $\forall x \in Var(\Gamma_0)$ $x\sigma =_{\Delta} x\sigma'$: First, by the definition of σ' for all $x \in Dom(\sigma')$, $x\sigma' = x\sigma$. Therefore, we need only consider the variables removed by the variable identification step. From Definition 8, for any variable x in the initial system replaced by a variable y during the identification step, $x\sigma := y\sigma$. Since any identifications occuring in the definition of Γ_4 must also occur in Γ'_4, $x\sigma' := y\sigma' = y\sigma = x\sigma$. Now consider the variable identifications added to construct Γ'_4 but not existing in Γ_4. If $x = y$ is added because $x\sigma_i = y\sigma_i$, without loss of generality assume x is replaced by y, then $x\sigma' := y\sigma' = y\sigma =_{\Delta} x\sigma$. Lastly if x is replaced by y because $x\sigma_i = y$, then $x\sigma' := y\sigma = x\sigma$.

To complete the proof, there exists $\phi_i \in CSAU_{\Delta}(\Gamma'_{5,i})$ such that $\phi_i \leq^{Var(\Gamma_0)}_{\Delta} \sigma'_i$ for $i = 1, 2$. By the definition of $\odot$, we have that $\phi_1 \odot \phi_2 \leq^{Var(\Gamma_0)}_{\Delta} \sigma'_1 \odot \sigma'_2 = \sigma'$, and $\sigma' =^{Var(\Gamma_0)}_{\Delta} \sigma$. Therefore, $\phi_1 \odot \phi_2 \leq^{Var(\Gamma_0)}_{\Delta} \sigma_1 \odot \sigma_2 = \sigma$. □

Lemma 6. *For each asymmetric unifier of a problem Γ_0, there exists a pair $(\Gamma_{5,1}, \Gamma_{5,2})$ computed by the Algorithm* AsymComb *(cf. Figure 1), where for each $\Gamma_{5,i}$ there exist a substitution τ_i which asymmetrically solves $\Gamma_{5,i}$.*

Proof. We present a very similar proof to the one presented in [2], containing the necessary updates to account for the asymmetry. Let τ be an $\Delta_1 \cup \Delta_2$-asymmetric solution to Γ_0. Without loss of generality we can assume that τ is a solution to Γ_2 and that τ is normalized on $Var(\Gamma_2)$.

- *Identify $\Gamma_{5,1}$ and $\Gamma_{5,2}$*
  - We obtain the system Γ_3 by defining a partition of the variables as follows: two variables x and y are in the same class of the partition if $x\tau = y\tau$. This also implies that τ is an asymmetric solution to Γ_3.
  - We obtain the system Γ_4 by defining a theory index and linear ordering as follows:

* The variable y gets index i if $y\tau$ is an i-term. If $y\tau$ is a variable then we can arbitrarily define its index as 1.
* In order to define the linear ordering we start with the strict partial ordering, $y < x$ iff $y\tau$ is a strict subterm of $x\tau$. The partial ordering can then be arbitrarily extended to a linear ordering.

This also implies that τ is an asymmetric solution to Γ_4, since this step does not modify any equation.

- *Define τ_i*
  Recall the bijection $\pi : (T(\Sigma, \mathcal{X}) \downarrow_{\mathcal{R},\mathcal{E}})_{/=_E} \longrightarrow \mathcal{Y}$. We add two additional restrictions. First, $Var(\Gamma_4) \subseteq \mathcal{Y}$. Since τ is assumed to be normalized on $Var(\Gamma_2)$ we have that for all $y \in Var(\Gamma_4)$, $y\tau$ is $\longrightarrow_{\mathcal{R},\mathcal{E}}$-irreducible. Second, we need $\pi(y\tau) = y$, which is obtained due to the variable identification step. This bijection then induces 2 mappings, π_1 and π_2, which are defined as described above. These mappings are used to define τ_i as follows:

$$\forall y \in Var(\Gamma_4),\ y\tau_i = (y\tau)^{\pi_i} \tag{2}$$

- *Show τ_i is an asymmetric solution to $\Gamma_{5,i}$*
  Assume $s =^{\downarrow} t$ is an equation in $\Gamma^1_{5,i}$. First, this equation must exist in Γ_4 and therefore asymmetrically solvable by τ. That is, $s\tau =^{\downarrow}_{\Delta_1 \cup \Delta_2} t\tau$. Since $s =^{\downarrow} t \in \Gamma^1_{5,i}$, it must be an i-equation. These facts combined allow us to apply Theorem 4 to get $(s\tau)^{\pi_i} =^{\downarrow}_{\Delta_i} (t\tau)^{\pi_i}$. Since $s =^{\downarrow} t$ is an i-equation we get that $(s\tau)^{\pi_i} = s\tau_i$ and $(t\tau)^{\pi_i} = t\tau_i$, which implies that τ_i is an asymmetric solution to $s =^{\downarrow} t$.

□

Lemma 7. *Let Γ_0 be an asymmetric Δ-unification problem. For each asymmetric unifier τ of Γ_0 there exists a pair $(\Gamma_{5,1}, \Gamma_{5,2})$ in the output set of the Algorithm* AsymComb *(cf. Figure 1), and a pair of substitutions (σ_1, σ_2) with each $\sigma_i \in CSAU_{\Delta_i}(\Gamma_{5,i})$, such that $\sigma = \sigma_1 \odot \sigma_2$ is an injective asymmetric solution to Γ_0 with $\sigma \leq^{Var(\Gamma_0)}_{\Delta} \tau$.*

Proof. From Lemma 6 we have that given τ there exists a pair $(\Gamma^1_{5,1}, \Gamma^1_{5,2})$ and substitutions (τ^1_1, τ^1_2) such that τ^1_i asymmetrically solves $\Gamma^1_{5,i}$. Now, if τ^1_i is an asymmetric solution to $\Gamma^1_{5,i}$, there exists a substitution τ^2_i produced by the algorithm A_i such that $\tau^2_i \in CSAU_{\Delta_i}(\Gamma^1_{5,i})$ and $\tau^2_i \leq^{Var(\Gamma_{5,i})}_{\Delta_i} \tau^1_i$. Furthermore, as in Lemma 5, by the definition of $\odot$, we have that $\tau^2 = \tau^2_1 \odot \tau^2_2 \leq^{Var(\Gamma_0)}_{\Delta} \tau^1_1 \odot \tau^1_2 = \tau$ (see Lemma 9 in the Appendix for an alternate proof of this fact).

From Lemma 5, there exists a pair $(\Gamma^2_{5,1}, \Gamma^2_{5,2})$ produced by AsymComb and a pair (σ_1, σ_2) such that σ_i is *injective* and *theory-preserving*, $\sigma_i \in CSAU_{\Delta_i}(\Gamma^2_{5,i})$ and $\sigma = \sigma_1 \odot \sigma_2 \leq^{Var(\Gamma_0)}_{\Delta} \tau^2$. By Lemma 4, σ is an injective asymmetric solution to Γ_4. Finally, $\sigma \leq^{Var(\Gamma_0)}_{\Delta} \tau^2$ and $\tau^2 \leq^{Var(\Gamma_0)}_{\Delta} \tau$, and so $\sigma \leq^{Var(\Gamma_0)}_{\Delta} \tau$. □

We can now show the the Algorithm *AsymComb* (cf. Figure 1) is correct, i.e., both sound and complete.

Theorem 5. *Let Γ_0 be a combined asymmetric unification problem. Γ_0 is asymmetrically unifiable if and only if the Algorithm* AsymComb *(cf. Figure 1) returns a combined substitution.*

Proof. From Lemma 3, the substitutions returned are unifiers. From Lemma 4 the substitutions are asymmetric. Completeness follows from Lemma 7. □

Now we can consider the complete set of unifiers.

Theorem 6. *Let Γ_0 be an asymmetric Δ-unification problem. Then, for every $\tau \in CSAU(\Gamma_0)$, Algorithm* AsymComb *(cf. Figure 1) produces an injective substitution σ such that $\sigma \leq_{\Delta}^{Var(\Gamma_0)} \tau$.*

Proof. For any problem, Γ_0, the Algorithm AsymComb will try every combination of variable identification, theory index and linear ordering, i.e. every possible pair of sub-problems $(\Gamma_{5,1}, \Gamma_{5,2})$. Furthermore, the Algorithm AsymComb will combine every pair, (σ_1, σ_2), of injective and theory preserving solutions such that $\sigma_i \in CSAU_{\Delta_i}(\Gamma_{5,i})$, $i \in \{1, 2\}$. Thus, the result follows from Lemma 7. □

3.5 Obtaining Linear Constant Restriction Algorithms

If one has a *general* asymmetric unification algorithm an algorithm that respects an LCR can be obtained. The construction is based on the construction given in [2] with modifications for asymmetry. Given Γ, an asymmetric unification problem with a linear constant restriction, we construct a general unification problem Γ' such that Γ is solvable iff Γ' is solvable. Let $<$ denote the linear ordering. Let $\mathcal{X}$ denote the variables of Γ and let C denote the set of all free constants in Γ. Now, we construct Γ' as follows: The free constants in Γ are treated as variables in Γ'. For each free constant c of Γ we add a new free function symbol f_c which has arity $|V_c|$. Recall that $V_c = \{x \in \mathcal{X} | x < c\}$. $\Gamma' = \Gamma \cup \{c =^{\downarrow} f_c(x_1, \ldots, x_n) \mid c \in C \text{ and } V_c = \{x_1, \ldots, x_n\}\}$

Theorem 7. *The Asymmetric E-unification problem with linear constant restriction, Γ, is solvable iff the general Asymmetric E-unification problem Γ' is solvable.*

Proof. Let σ be an $\rightarrow_{\mathcal{R},\mathcal{E}}$ normalized, asymmetric solution to Γ. σ' is defined on $\mathcal{X} \cup C$ by induction on $<$ as follows:

1. Least element of $\mathcal{X} \cup C$.
   (a) If the least element is a variable $x \in \mathcal{X}$ then $x\sigma' := x\sigma$.
   (b) If the least element is a constant $c \in C$ then $c\sigma' := f_c$, i.e., f_c is a constant.
2. Arbitrary element
   - For and arbitrary $x \in \mathcal{X}$, let $c_1, \ldots, c_m \in C$ be the free constants occurring in $x\sigma$. Then $x\sigma'$ is obtained from $x\sigma$ by replacing c_k by $c_k\sigma'$ $(k = 1, \ldots, m)$.
   - For an arbitrary $c \in C$, where by definition Γ' contains the equation $c =^{\downarrow} f_c(x_1, \ldots, x_n)$. Then $c\sigma' := f_c(x_1\sigma', \ldots, x_n\sigma')$.

It remains to be shown that σ' is an asymmetric solution to Γ'. First, consider the equations of the form $c =^{\downarrow} f_c(x_1, \ldots, x_n)$, by definition σ' solves this equation. In addition, since f_c is a new free function symbol it will not match any rule. Thus if there exists a reduction it exists in a variable position. We can then show by induction and the asymmetry of σ that there cannot be a reduction in any of the variable positions. Next consider an equation, $s =^{\downarrow} t$, from Γ. Here the fact that σ' solves these equations is shown in [2]. In addition since a reduction in $t\sigma'$ would imply a reduction in $t\sigma$, σ' is also an asymmetric unifier.

Assume that σ' is an asymmetric solution to Γ'. It is shown in [2] that if for all $x \in \Gamma$ we define σ as $x\sigma := (x\sigma)^{\pi_1}$, where the symbols f_c are treated as 2-symbols and the remaining as 1-symbols, then σ is a solution to Γ. Since the projection onto 1-pure terms will not introduce new reductions, σ is also an asymmetric solution. □

We can also obtain a complete set of unifiers for the LCR version of the problem if we have a complete set of unifiers for the general asymmetric unification problem. Like the result for the decision problem this result is mostly proven in [2] and we need only make some modification for asymmetry and the type of rewriting. We include the construction here for completeness.

Let Γ again denote an asymmetric problem with linear constant restriction and let Γ' denote the constructed general problem (see the construction at the beginning of this section). Now we give a slightly modified version of a construction from [2], showing how a substituation σ' from the complete set of unifiers of Γ' can be used to define a solution σ to Γ. Without loss of generality, we will assume that all substitutions are $\rightarrow_{\mathcal{R},\mathcal{E}}$-normalized. We can use a similar bijection method to help define the solutions. Let Σ' be the signature of Γ', i.e., it includes the new f_c symbols. Let π be a bijection from the set $(T(\Sigma', \mathcal{X}) \downarrow_{\mathcal{R},\mathcal{E}})/_{=_\mathcal{E}}$ onto a set of variables $\mathcal{Y}$. In addition, we require that $\pi(c\sigma') = c$ for the free constants c in Σ, which means that $\mathcal{Y}$ must contains these free constants which are variables in Γ'. This condition is true if $c\sigma' \neq_{\mathcal{R}\cup\mathcal{E}} c'\sigma'$ when $c \neq c'$. Which is satisfied since σ' solves Γ' which implies that $c\sigma' =^{\downarrow}_{\mathcal{R}\cup\mathcal{E}} f_c(x_1\sigma', \ldots, x_n\sigma')$ and $c'\sigma' =^{\downarrow}_{\mathcal{R}\cup\mathcal{E}} f_{c'}(x_1\sigma', \ldots, x_m\sigma')$. This implies the root symbol of the two terms is different. Now that we have a bijection we can again define the mappings π_1 and π_2 as we have done in Section 3.2. However, for the new mappings we let Σ be the signature of the 1-symbols and let the f_c symbols be the 2-symbols. We can now see that the mapping π_1 can be used to define the solution σ to Γ. That is, for all variables, x, in Γ let $x\sigma = (x\sigma')^{\pi_1}$.

Lemma 8. *The set $C(\Gamma) = \{\sigma \mid \sigma' \in CSAU(\Gamma')\}$, where σ is constructed from σ' as described above, is a complete set of asymmetric unifiers with linear constant restriction of Γ.*

Proof. From Proposition 5.3 of [2] we can conclude that $C(\Gamma)$ is a *complete set of unifiers with linear constant restriction* of Γ. However, we need to show that they satisfy the asymmetric restriction. First, recall that $\Gamma \subset \Gamma'$ and let $s =^{\downarrow} t \in \Gamma$. We know that $s\sigma' =^{\downarrow}_{\mathcal{R}\cup\mathcal{E}} t\sigma'$, where the constants of Γ are treated as variables and $t\sigma'$ is in $\rightarrow_{\mathcal{R},\mathcal{E}}$-normal form. Now, assume there is a reduction in $(t\sigma')^{\pi_1}$. Theorem 4 shows that a reduction in $(t\gamma)^{\pi_i}$ implies a reduction in $t\gamma$. A simplified version of that proof can be used here. Simplified since the f_c functions form a free theory having no corresponding rewrite rules, thus all reductions occur in 1-terms. This implies that if there is a reduction in $(t\sigma')^{\pi_1}$ there is a reduction in $t\sigma'$ which contradicts our assumption that $t\sigma'$ is in $\rightarrow_{\mathcal{R},\mathcal{E}}$-normal form. □

4 Conclusions

We give the first general method for the asymmetric unification problem in the combination of disjoint equational theories. It remains to be seen if non-disjoint methods can also be extended to the asymmetric unification paradigm.

With respect to efficiency, the combination algorithm provides a significant first step to more efficient methods since, unlike a narrowing approach, we can now combine efficient special purpose asymmetric unification algorithms. In addition, it should be possible to improve the efficiency of the current algorithm. First, efficiency may be improved by adopting some of the methods introduced by Boudet [6]. Second, It may be possible to identify specific ways of enumerating the variable identifications which do not include redundant/useless partitions. We are currently studying the question of improving the efficiency.

Briefly, the only theories that are currently known to have asymmetric unification algorithms are those with the *finite variant property* [7], in which case a general algorithm known as *folding variant narrowing* [12] applies. This is a sizable class, including many, but not all, theories of interest to cryptographic protocol analysis, including cancellation of encryption and decryption,

Diffie-Hellman exponentiation, exclusive-or, and free Abelian groups. It does not include homomorphic encryption from an Abelian group to itself (see [7] for a discussion). In many cases known characterizations of theories with the finite variant property [12, 5] depend on conditions on E and R that can be checked without further reference to Σ, and so for these cases the finite variant property still holds after the addition of uninterpreted function symbols. Thus general asymmetric unification algorithms exist. Moreover, the earlier mentioned special-purpose unification algorithms for exclusive-or and free Abelian groups [14, 9] are also general. In [14] and [9] a general strategy is presented for converting symmetric unification algorithms to asymmetric ones. This opens up an avenue for the development of special-purpose general unification algorithms for theories with and without the finite variant property as well, to which our results would also apply.

There exists an interesting connection between Asymmetric unification and Disunification. Consider a disunification problem $s \neq t$ in the theory $\Delta = E \cup R$ over signature Σ. We can simulate this problem using asymmetric unification. First, let f and g be new function symbols added to Σ. Let $f(x, x) \longrightarrow g(x)$ be a new rule added to R. Now $s \neq t$ can be simulated by $\{s =^{\downarrow} u,\ t =^{\downarrow} v,\ w =^{\downarrow} f(u, v)\}$. Although there is some connection between the two problems they may still be independent and resolving this is an interesting open problem.

References

[1] Franz Baader and Tobias Nipkow. *Term rewriting and all that*. Cambridge University Press, New York, NY, USA, 1998.

[2] Franz Baader and Klaus U. Schulz. Unification in the Union of Disjoint Equational Theories: Combining Decision Procedures. *Journal of Symbolic Computation*, 21(2):211 – 243, 1996.

[3] Franz Baader and Wayne Snyder. Unification Theory. In John Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, pages 445–532. Elsevier and MIT Press, 2001.

[4] Bruno Blanchet. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In *Proceedings of the 14th IEEE Workshop on Computer Security Foundations*, CSFW '01, pages 82–. IEEE Computer Society, 2001.

[5] Christopher Bouchard, Kimberly A. Gero, Christopher Lynch, and Paliath Narendran. On Forward Closure and the Finite Variant Property. In Pascal Fontaine, Christophe Ringeissen, and Renate A. Schmidt, editors, *Frontiers of Combining Systems*, volume 8152 of *Lecture Notes in Computer Science*, pages 327–342. Springer Berlin Heidelberg, 2013.

[6] Alexandre Boudet. Combining Unification Algorithms. *Journal of Symbolic Computation*, 16(6):597 – 626, 1993.

[7] Hubert Comon-Lundh and Stéphanie Delaune. The Finite Variant Property: How to Get Rid of Some Algebraic Properties. In Jürgen Giesl, editor, *Rewriting Techniques and Applications*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2005.

[8] Serdar Erbatur, Santiago Escobar, Deepak Kapur, Zhiqiang Liu, Christopher Lynch, Catherine Meadows, José Meseguer, Paliath Narendran, Sonia Santiago, and Ralf Sasse. Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *Computer Security, ESORICS 2012*, volume 7459 of *Lecture Notes in Computer Science*, pages 73–90. Springer Berlin Heidelberg, 2012.

[9] Serdar Erbatur, Santiago Escobar, Deepak Kapur, Zhiqiang Liu, Christopher A. Lynch, Catherine Meadows, José Meseguer, Paliath Narendran, Sonia Santiago, and Ralf Sasse. Asymmetric Unification: A New Unification Paradigm for Cryptographic Protocol Analysis. In Maria Paola Bonacina, editor, *Automated Deduction, CADE-24*, volume 7898 of *Lecture Notes in Computer Science*, pages 231–248. Springer Berlin Heidelberg, 2013.

[10] Santiago Escobar, Catherine Meadows, and José Meseguer. Maude-NPA: Cryptographic Protocol Analysis Modulo Equational Properties. In *Foundations of Security Analysis and Design V, FOSAD 2007/2008/2009 Tutorial Lectures*, volume 5705 of *Lecture Notes in Computer Science*, pages 1–50. Springer, 2009.

[11] Santiago Escobar, José Meseguer, and Ralf Sasse. Variant Narrowing and Equational Unification. *Electronic Notes Theor. Comput. Science*, 238(3):103–119, 2009.

[12] Santiago Escobar, Ralf Sasse, and José Meseguer. Folding Variant Narrowing and Optimal Variant Termination. *J. Log. Algebr. Program.*, 81(7-8):898–928, 2012.

[13] Jean-Pierre Jouannaud and Yoshihito Toyama. Modular Church-Rosser Modulo: The Complete Picture. *Int. J. Software and Informatics*, 2(1):61–75, 2008.

[14] Zhiqiang Liu. *Dealing Efficiently with Exclusive OR, Abelian Groups and Homomorphism in Cryptographic Protocol Analysis*. PhD thesis, Clarkson University, 2012.

[15] Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In Natasha Sharygina and Helmut Veith, editors, *Computer Aided Verification*, volume 8044 of *Lecture Notes in Computer Science*, pages 696–701. Springer Berlin Heidelberg, 2013.

[16] Sebastian Mödersheim. *Models and Methods for the Automated Analysis of Security Protocols*. PhD thesis, ETH Zurich, 2007.

[17] Michael Rusinowitch. On Termination of the Direct sum of Term-Rewriting Systems. *Information Processing Letters*, 26:65–70, 1987.

A Additional Proof Details

In this section we fill in some additional details from Lemma 7. This results is proven in [2], but for completeness we present the proof here with a few modifications to account for notation.

Lemma 9. *Let τ be a solution to a original problem Γ_0 and let $\tau = (\tau_1 \odot \tau_2)$. Assume there exists a pair (σ_1, σ_2) such that $\tau_i =_{\Delta_i} \sigma_i\lambda_i$. Then, $\tau =_{\Delta}^{Var(\Gamma_0)} \sigma\lambda$ where $\sigma = (\sigma_1 \odot \sigma_2)$ and $\lambda := (\lambda_1 \cup \lambda_2)\pi^{-1}$ such that $(\lambda_1 \cup \lambda_2)$ is the substitution equal to λ_i on Z_i and the identity on all other variables.*

Proof. To make things simpler we can, without loss of generality, assume that σ_i maps the variables in Γ_i to terms containing only variables of index j (which are treated as constants by λ_i) or variables from a fresh set Z_i. This can be done as follows, for all $x \in Dom(\sigma_i)$ rename all the variables of index i in $x\sigma_i$ with variables from Z_i. We may also assume that the domain of λ_i is Z_i and $Var(\Gamma_2)$, Z_1 and Z_2 are pairwise disjoint. We prove $\tau =_{\Delta}^{Var(\Gamma_{5,1}) \cup Var(\Gamma_{5,2})} \sigma\lambda$. It then can be extended, as shown in [2], to $Var(\Gamma_0)$. We prove for any variable z occurring in $y\sigma_i$ that $\sigma\lambda$ and $\lambda_i\pi^{-1}$ coincide modulo Δ.

We proceed by induction on $<$. Recall that $\sigma = \sigma_i\sigma$ for variables of index i. Now without loss of generality lets consider a variables of index 1. Thus on y, $\sigma = \sigma_1\sigma$ and $y\sigma\lambda = y\sigma_1\sigma\lambda$. If y has index 1 then the variables in $y\sigma_1$ are of index 2 or from Z_1.

- First consider the variables of Z_1 and let $z \in Z_1$. Since these are fresh variables, they are not in the domain of σ, thus $z\sigma\lambda = z\lambda$. By the definition of λ, $z\lambda = z\lambda_1\pi^{-1}$.

Let y be the least variable with respect to $<$. By the definition $y\sigma_1$ does not contain any variables of index 2. Thus, $y\sigma_1$ contains variables from Z_1 and for all variables z in $y\sigma_1$, $z\sigma\lambda = z\lambda\pi^{-1}$. This implies that

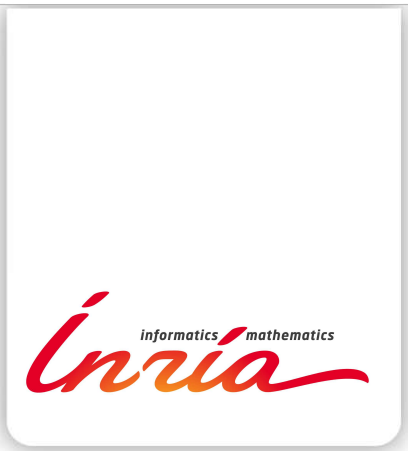
$$y\sigma\lambda = (y\sigma_1)\sigma\lambda = (y\sigma_1)\lambda_1\pi^{-1} =_{\Delta} y\tau_1\pi^{-1} = (y\tau)^{\pi_1}\pi^{-1} =_{\Delta} y\tau.$$

Now let y be an arbitrary variable in $Var(\Gamma_{5,1})$. Let y_2 be an element of $Var(\Gamma_{5,2})$ in $y\sigma_1$. This implies that $y_2 < y$ and thus by induction $y_2\sigma\lambda =_{\Delta} y_2\tau$ and $y_2\tau =_{\Delta} (y_2\tau)^{\pi_1}\pi^{-1} = y_2\tau_1\pi^{-1}$. Since y_2 has index 2 we have that $y_2\tau_1\pi^{-1} = y_2\pi^{-1} = y_2\lambda_1\pi^{-1}$ and thus $y_2\sigma\lambda =_{\Delta} y_2\lambda_1\pi^{-1}$.

Therefore, for any z occurring in $y\sigma_1$, $z\sigma\lambda =_{\Delta} z\lambda_1\pi^{-1}$ and thus

$$y\sigma\lambda = (y\sigma_1)\sigma\lambda =_{\Delta} (y\sigma_1)\lambda_1\pi^{-1} =_{\Delta} y\tau_1\pi^{-1} = (y\tau)^{\pi_1}\pi^{-1} =_{\Delta} y\tau.$$

□



RESEARCH CENTRE
NANCY – GRAND EST

615 rue du Jardin Botanique
CS20101
54603 Villers-lès-Nancy Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399