On Asymmetric Unification and the Combination Problem in Disjoint Theories

(Extended Abstract)

Serdar Erbatur[1], Deepak Kapur[2] [*], Andrew M. Marshall[3][†], Catherine Meadows[3],
Paliath Narendran[4] [‡]and Christophe Ringeissen[5]

[1] Università degli Studi di Verona, Italy
[2] University of New Mexico, Albuquerque, NM, USA
[3] Naval Research Laboratory, Washington, DC, USA
[4] University at Albany–SUNY, Albany, NY, USA
[5] LORIA – INRIA Nancy-Grand Est, Nancy, France

A full version of this work [5] appeared in the proceedings of the 17th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2014). In the following, we provide a summary of this work.

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 [4]. 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 are 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.

Although asymmetric unification has the potential of playing an important role in cryptographic protocol analysis, and possibly other unification-based state explorations as well, it is still not that well understood. Until the development of special-purpose algorithms for exclusive-or and free Abelian group theories, the only known asymmetric unification algorithm was variant narrowing. One important question 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

[*] Partially supported by the NSF grant CNS-0905222
[†] ASEE postdoctoral fellowship under contract to the NRL.
[‡] Partially supported by the NSF grant CNS-0905286

efficiency since special-purpose asymmetric algorithms have the promise of being more efficient than variant narrowing.

In this work 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. The only restrictions on this new method are those inherited from the asymmetric unification problem and those inherited from Baader and Schulz.

2 Asymmetric Unification

We use the standard notation of equational unification [3] and term rewriting systems [1].

Definition 2.1. 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.*

Definition 2.2. 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 $l \rightarrow r \in R$ we have $Var(r) \subseteq Var(l)$. (4) R is confluent and terminating modulo E, i.e., the relation $\rightarrow_{R/E}$ is confluent and terminating. (5) $\rightarrow_{R,E}$ is E-coherent, i.e., $\forall t_1, t_2, t_3$ if $t_1 \rightarrow_{R,E} t_2$ and $t_1 =_E t_3$ then $\exists\ t_4, t_5$ such that $t_2 \rightarrow^*_{R,E} t_4$, $t_3 \rightarrow^+_{R,E} t_5$, and $t_4 =_E t_5$.

This definition is inherited directly from [4]. The last restrictions ensure that $s \rightarrow^!_{R/E} t$ iff $s \rightarrow^!_{R,E} t$, therefore it is sufficient to consider R, E rather then R/E (see [4]).

Definition 2.3 (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 2.4. Let $R = \{x \oplus 0 \rightarrow x,\ x \oplus x \rightarrow 0,\ x \oplus x \oplus y \rightarrow y\}$ 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 2.5 (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

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 $\Sigma_1 \cup \Sigma_2$. We assume Δ_i

admits a a decomposition (Σ_i, E_i, R_i), and an asymmetric Δ_i-unification with linear constant restriction algorithm is known for $i = 1, 2$. In [5], we show that the Baader-Schulz combination method [2] designed for unification can be reused for asymmetric unification. A slight adaptation is required to construct combined unifiers that are necessarily asymmetric.

Theorem 3.1. *([5]) Asymmetric $\Delta_1 \cup \Delta_2$-unification is decidable (resp. finitary) if asymmetric Δ_i-unification with LCR is decidable (resp. finitary), for $i = 1, 2$.*

As in [2], it can be shown that there exists an asymmetric Δ_i-unification algorithm with LCR if and only if there exists an asymmetric Δ_i-unification algorithm with free symbols. Therefore, the above theorem can be rephrased in terms of asymmetric unification with free symbols.

Example 3.2. Let $\Delta_1 = R_1 \cup E_1$, where $R_1 = \{e(x, d(x, y)) \rightarrow y,\ d(x, e(x, y)) \rightarrow y\}$ and $E_1 = \emptyset$. Let $\Delta_2 = R_2 \cup E_2$, where $R_2 = \{x \oplus 0 \rightarrow x,\ x \oplus x \rightarrow 0,\ x \oplus x \oplus y \rightarrow y\}$ and $E_2 = \{x \oplus y = y \oplus x,\ (x \oplus y) \oplus z = x \oplus (y \oplus z)\}\}$. Consider the set of equations $\{x_0 \oplus x_1 \oplus x_2 =^{\downarrow} x_3 \oplus x_4,\ e(x_1, d(0, x_5)) =^{\downarrow} x_2 \oplus x_0,\ e(x_1, d(x_0, e(x_2, x_6))) =^{\downarrow} e(x_7, x_5)\}$. After purification, we get 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, we would produce the following Γ_3: $\{x_0 \oplus x_1 \oplus x_2 =^{\downarrow} x_0 \oplus x_2,\ e(x_1, d(x_1, x_5)) =^{\downarrow} x_5,\ 0 =^{\downarrow} x_1,\ x_5 =^{\downarrow} x_2 \oplus x_0,\ e(x_1, d(x_0, e(x_2, x_6))) =^{\downarrow} e(x_1, x_5)\}$. 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: $\{e(\mathbf{x}_1, d(\mathbf{x}_1, \mathbf{x}_5)) =^{\downarrow} \mathbf{x}_5,\ e(\mathbf{x}_1, d(\mathbf{x}_0, e(\mathbf{x}_2, x_6))) =^{\downarrow} e(\mathbf{x}_1, \mathbf{x}_5)\}$. Next $\Gamma_{5,i}$ is solved with LCR. The last step is to combine each pair of substitutions (σ_1, σ_2) into a substitution σ. One such pair is $\sigma_1 = \{x_1 \mapsto 0,\ x_5 \mapsto x_2 \oplus x_0\}$ and $\sigma_2 = \{x_6 \mapsto d(\mathbf{x}_2, e(\mathbf{x}_0, \mathbf{x}_5))\}$. Thus, we get the following asymmetric solution, $\{x_1 \mapsto 0,\ x_3 \mapsto x_0,\ x_4 \mapsto x_2,\ x_5 \mapsto x_2 \oplus x_0,\ x_6 \mapsto d(x_2, e(x_0, x_2 \oplus x_0)),\ x_7 \mapsto 0\}$, (existential variables z_0, z_1 are removed).

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] 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.

[5] Serdar Erbatur, Deepak Kapur, Andrew M. Marshall, Catherine Meadows, Paliath Narendran, and Christophe Ringeissen. On asymmetric unification and the combination problem in disjoint theories. In Anca Muscholl, editor, *Foundations of Software Science and Computation Structures*, volume 8412 of *Lecture Notes in Computer Science*, pages 274–288. Springer Berlin Heidelberg, 2014.