Variant Narrowing and Equational Unification

Santiago Escobar[1]

Universidad Politécnica de Valencia, Spain.

José Meseguer[2]

University of Illinois at Urbana-Champaign, USA.

Ralf Sasse[3]

University of Illinois at Urbana-Champaign, USA.

Abstract

Narrowing is a well-known complete procedure for equational E-unification when E can be decomposed as a union $E = \Delta \uplus B$ with B a set of axioms for which a finitary unification algorithm exists, and Δ a set of confluent, terminating, and B-coherent rewrite rules. However, when $B \neq \emptyset$, effective narrowing strategies such as basic narrowing easily fail to be complete and cannot be used. This poses two challenges to narrowing-based equational unification: (i) finding effective narrowing strategies that are complete modulo B under mild assumptions on B, and (ii) finding sufficient conditions under which such narrowing strategies yield *finitary* E-unification algorithms. Inspired by Comon and Delaune's notion of E-variant for a term, we propose a new narrowing strategy called *variant narrowing* that has a search space potentially much smaller than full narrowing, is complete, and yields a finitary E-unification algorithm when E has the finite variant property. We also discuss applications to symbolic reachability analysis of concurrent systems specified as rewrite theories, and in particular to the formal analysis of cryptographic protocols modulo the algebraic properties of the underlying cryptographic functions.

Keywords: Equational unification, narrowing, finite variant property, symbolic reachability analysis, cryptographic protocol analysis.

1 Introduction

Equational unification is the solving of existentially quantified problems $\exists \boldsymbol{x}\ t =_E t'$ modulo an equational theory E. If the equations E are convergent, it is well-known that narrowing provides a complete unification procedure for E-unification [13]. This result extends to narrowing modulo a set B of equational axioms. That is, if $E = \Delta \uplus B$, where Δ is a set of oriented equations that are convergent and coherent modulo B, then narrowing with Δ modulo B is also a complete E-unification

[1] Email: sescobar@dsic.upv.es

[2] Email: meseguer@cs.uiuc.edu

[3] Email: rsasse@cs.uiuc.edu

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

procedure [14]. In practice, however, full narrowing, i.e., considering all narrowing sequences, can be highly inefficient. This has led to the search for complete narrowing strategies that have a much smaller search space; and to conditions under which narrowing terminates, so that a finitary unification algorithm can be obtained. Hullot's basic narrowing [13] is one such strategy, which is complete[4] and terminates under suitable conditions. The problem, however, is that basic narrowing is complete for $B = \emptyset$, but is *incomplete* for a general set B of axioms, and in particular for associativity-commutativity (AC) (see [22,2] and Example 7.3).

This paper addresses the problem of finding complete narrowing procedures modulo B, under minimal assumptions on B, which have a much smaller search space than full narrowing, and for which finitary unification conditions can be given. Specifically, inspired by the notion of E-variant of a term due to Comon and Delaune [2], we propose a new narrowing method called *variant narrowing* with the following properties: (i) it only uses substitutions in normal form modulo B; (ii) it is complete under very general assumptions on B and Δ; (iii) if Δ has the finite variant property modulo B, it can be used to both compute all the finite variants of a term in a very space-effective way, and to obtain a *finitary* E-unification algorithm.

Indeed, when Δ has the finite variant property modulo B, we explain in detail how variant narrowing can be specialized into two terminating algorithms, one for computing the finite set of variants of any term, and another optimized one for providing a finitary E-unification algorithm that computes a complete and minimal set of E-unifiers.

Our own, specific motivation for working on this topic comes from our interest in developing complete methods for *symbolic reachability analysis* of a concurrent system specified as a rewrite theory of the form $\mathcal{R} = (\Sigma, E, R)$, where the states of the system are equivalence classes of Σ-terms modulo E, and the concurrent transitions are specified by rewrite rules R, which are applied modulo E to such states. Symbolic reachability analysis problems for $\mathcal{R}$ are then goals of the form $\exists \boldsymbol{x}\; t \longrightarrow^{*}_{R/E} t'$. That is, we are given a possibly infinite set of initial states denoted by the term t with variables, and we want to know whether there is a substitution instance of t from which we can *reach* a substitution instance of the set of states denoted by the term t'. Under reasonable assumptions on $\mathcal{R}$, such as the topmost character of the rules R (see [18]), *narrowing* with the rules R *modulo* E provides a complete semidecision procedure for solving such reachability goals. But this procedure of course requires performing E-unification at each narrowing step with a rule in R. If $E = \Delta \uplus B$, where Δ is a set of oriented equations that are convergent and coherent modulo B, then E-unification can be performed by narrowing with Δ modulo B. But this can produce an infinite set of unifiers for each single step of narrowing modulo E with a rule in R, making the entire reachability analysis still possible, but very ineffective. A much more attractive case is one in which Δ has the finite variant property modulo B, and we have a finitary unification algorithm for B. In particular, this situation can often occur in rewrite theories $\mathcal{R} = (\Sigma, \Delta \uplus B, R)$, where R describes the transitions of a *cryptographic communication protocol*, and the equational theory $E = \Delta \uplus B$ describes the *algebraic properties of the cryptographic*

[4] Basic narrowing is complete for normalized substitutions, see [13], though it does also produce non-normalized substitutions.

functions.

To make explicit the relationship of the present work with these applications, we use one such cryptographic theory $E = \Delta \uplus B$ (including encryption-decryption and exclusive or) as our running example. Also, in Section 6 we discuss yet another cryptographic theory underlying the Diffie-Hellman protocol for which variant narrowing has been used to find an attack in the Maude-NPA tool [6,7,5]. Our own experience (see [7,5]) has taught us an important additional lesson, namely, that a typed setting supporting sorts and subsorts can greatly help in making narrowing-based unification algorithms finitary. For this reason, we develop the entire paper in the setting of order-sorted equational theories.

The paper is organized as follows. In Section 2 we explain basic concepts and rewriting. Then in Section 3 we introduce the necessary narrowing concepts. In Section 4 we recapitulate results about variants and explain our variant narrowing approach. Section 5 describes our variant narrowing procedure for equational unification. Section 6 describes an application of our work to cryptographic protocol analysis. We conclude in Section 7 and discuss related and future work. If you are interested in the proofs you can find them in the technical report [9].

2 Preliminaries

We follow the classical notation and terminology from [21] for term rewriting and from [16,17] for rewriting logic and order-sorted notions. We assume an *order-sorted signature* Σ with a finite poset of sorts $(\mathsf{S}, \leq)$ and a finite number of function symbols. We furthermore assume that: (i) each connected component in the poset ordering has a top sort, and for each $\mathsf{s} \in \mathsf{S}$ we denote by $[\mathsf{s}]$ the top sort in the component of s; and (ii) for each operator declaration $f : \mathsf{s}_1 \times \ldots \times \mathsf{s}_\mathsf{n} \to \mathsf{s}$ in Σ, there is also a declaration $f : [\mathsf{s}_1] \times \ldots \times [\mathsf{s}_\mathsf{n}] \to [\mathsf{s}]$. We assume an S-sorted family $\mathcal{X} = \{\mathcal{X}_\mathsf{s}\}_{\mathsf{s} \in \mathsf{S}}$ of mutually disjoint variable sets with each $\mathcal{X}_\mathsf{s}$ countably infinite. $\mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ is the set of terms of sort s, and $\mathcal{T}_{\Sigma,\mathsf{s}}$ is the set of ground terms of sort s. We write $\mathcal{T}_\Sigma(\mathcal{X})$ and $\mathcal{T}_\Sigma$ for the corresponding term algebras. For a term t we write $\mathit{Var}(t)$ for the set of all variables in t, and write $\mathit{Var}(t_1, \ldots, t_k)$ instead of $\mathit{Var}(t_1) \cup \cdots \cup \mathit{Var}(t_k)$. The set of positions of a term t is written $\mathit{Pos}(t)$, and the set of non-variable positions $\mathit{Pos}_\Sigma(t)$. The root of a term is Λ. The subterm of t at position p is $t|_p$ and $t[u]_p$ is the term t where $t|_p$ is replaced by u. A *substitution* σ is a sorted mapping from a finite subset of $\mathcal{X}$, written $\mathit{Dom}(\sigma)$, to $\mathcal{T}_\Sigma(\mathcal{X})$. The set of variables introduced by σ is $\mathit{Ran}(\sigma)$. The identity substitution is id. Substitutions are homomorphically extended to $\mathcal{T}_\Sigma(\mathcal{X})$. The application of a substitution σ to a term t is denoted by $t\sigma$. The restriction of σ to a set of variables V is $\sigma|_V$. Composition of two substitutions is denoted by $\sigma\sigma'$, meaning $X(\sigma\sigma') = (X\sigma)\sigma'$ for any variable X. We call a substitution σ a *renaming* if there is another substitution σ^{-1} such that $(\sigma\sigma^{-1})|_{\mathit{Dom}(\sigma)} = \mathit{id}$.

A Σ-*equation* is an unoriented pair $t = t'$, where $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ for some sort $\mathsf{s} \in \mathsf{S}$. Given Σ and a set E of Σ-equations such that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s, order-sorted equational logic induces a congruence relation $=_E$ on terms $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ (see [17]). Throughout this paper we assume that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s. An *equational theory* (Σ, E) is a set of Σ-equations.

The *E-subsumption* preorder $\leq_E$ (or $\leq$ if E is understood) holds between $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$, denoted $t \leq_E t'$ (meaning that t is more general than t'), if there is a substitution σ such that $t\sigma =_E t'$; such a substitution σ is said to be an *E-match* from t to t'. For substitutions σ, ρ and a set of variables V we define $\sigma|_V =_E \rho|_V$ if $x\sigma =_E x\rho$ for all $x \in V$; $\sigma|_V \leq_E \rho|_V$ if there is a substitution η such that $(\sigma\eta)|_V =_E \rho|_V$; $\sigma|_V \simeq_E \rho|_V$ if there is a renaming η such that $(\sigma\eta)|_V =_E \rho|_V$; and $\sigma|_V <_E \rho|_V$ if $\sigma|_V \leq_E \rho|_V$ and $\sigma|_V \not\simeq_E \rho|_V$.

An *E-unifier* for a Σ-equation $t = t'$ is a substitution σ such that $t\sigma =_E t'\sigma$. For $\mathit{Var}(t) \cup \mathit{Var}(t') \subseteq W$, a set of substitutions $\mathcal{U}$ is said to be a *complete* set of E-unifiers of the equation $t = t'$ away from W if: (i) each $\sigma \in \mathcal{U}$ is an E-unifier of $t = t'$; (ii) for any E-unifier ρ of $t = t'$ there is a $\sigma \in \mathcal{U}$ such that $\sigma|_W \leq_E \rho|_W$; (iii) for all $\sigma \in \mathcal{U}$, $\mathit{Dom}(\sigma) \subseteq (\mathit{Var}(t) \cup \mathit{Var}(t'))$ and $\mathit{Ran}(\sigma) \cap W = \emptyset$. We write $\mathit{CSU}_E(t = t')$ to denote a complete set of E-unifiers of $t = t'$. A complete set of E-unifiers $\mathit{CSU}_E(t = t')$ is called *minimal* if any proper subset of $\mathit{CSU}_E(t = t')$ fails to be complete.

We say that an equational theory (Σ, E) has a *unification algorithm* if there is an algorithm generating a complete set of E-unifiers $\mathit{CSU}_E(t = t')$ for any E-unification problem $t = t'$ in (Σ, E); we say that the algorithm is *finitary* if the generated set $\mathit{CSU}_E(t = t')$ is always finite for any $t = t'$; and we say that the algorithm is *minimal* if the generated set $\mathit{CSU}_E(t = t')$ is always minimal for any $t = t'$.

A *rewrite rule* is an oriented pair $l \to r$, where $l \notin \mathcal{X}$, and $l, r \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$ for some sort $\mathsf{s} \in \mathsf{S}$. An *(unconditional) order-sorted rewrite theory* is a triple $\mathcal{R} = (\Sigma, E, R)$ with Σ an order-sorted signature, E a set of Σ-equations, and R a set of rewrite rules. The rewriting relation on $\mathcal{T}_\Sigma(\mathcal{X})$, written $t \to_R t'$ or $t \xrightarrow{p}_R t'$ holds between t and t' iff there exist $p \in \mathit{Pos}_\Sigma(t)$, $l \to r \in R$ and a substitution σ, such that $t|_p = l\sigma$, and $t' = t[r\sigma]_p$. The relation $\to_{R/E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ is $=_E; \to_R; =_E$. Note that $\to_{R/E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ induces a relation $\to_{R/E}$ on $\mathcal{T}_{\Sigma/E}(\mathcal{X})$ by $[t]_E \to_{R/E} [t']_E$ iff $t \to_{R/E} t'$. The transitive closure of $\to_{R/E}$ is denoted by $\to^+_{R/E}$ and the transitive and reflexive closure of $\to_{R/E}$ is denoted by $\to^*_{R/E}$. We say that a term t is $\to_{R/E}$-irreducible (or just R/E-irreducible) if there is no term t' such that $t \to_{R/E} t'$.

We say that the relation $\to_{R/E}$ is *terminating* if there is no infinite sequence $t_1 \to_{R/E} t_2 \to_{R/E} \cdots \to_{R/E} \cdots$. We say that the relation $\to_{R/E}$ is *confluent* if whenever $t \to^*_{R/E} t'$ and $t \to^*_{R/E} t''$, there exists a term t''' such that $t' \to^*_{R/E} t'''$ and $t'' \to^*_{R/E} t'''$. We say that $\to_{R/E}$ is *convergent* if it is confluent and terminating. An order-sorted rewrite theory $\mathcal{R} = (\Sigma, E, R)$ is convergent (resp. terminating, confluent) if the relation $\to_{R/E}$ is convergent (resp. terminating, confluent). In a convergent order-sorted rewrite theory, for each term $t \in \mathcal{T}_\Sigma(\mathcal{X})$, there is a unique (up to E-equivalence) R/E-irreducible term t' obtained from t by rewriting to canonical form, which is denoted by $t \to^!_{R/E} t'$ or $t{\downarrow}_{R/E}$ (when t' is not relevant).

For substitutions σ, ρ and a set of variables V we define $\sigma|_V \to_{R/E} \rho|_V$ if there is $X \in V$ such that $X\sigma \to_{R/E} X\rho$ and for all other $Y \in V$ we have $Y\sigma =_E Y\rho$. We write $\sigma{\downarrow}_{R/E}$ for the normalized version of σ. A substitution σ is called *R/E-normalized* if $X\sigma$ is R/E-irreducible for all $X \in \mathit{Dom}(\sigma)$.

2.1 R, E-rewriting

Since E-congruence classes can be infinite, $\rightarrow_{R/E}$-reducibility is undecidable in general. Therefore, R/E-rewriting is usually implemented [14] by R, E-rewriting. We assume the following properties on R and E:

(i) E is *regular*, i.e., for each $t = t'$ in E, we have $Var(t) = Var(t')$, and *sort-preserving*, i.e., for each substitution σ, we have $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$ if and only if $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$, and all variables in $Var(t)$ have a top sort.

(ii) E has a finitary and complete unification algorithm, which implies that E-matching is finitary and complete.

(iii) For each $t \to t'$ in R we have $Var(t') \subseteq Var(t)$.

(iv) R is *sort-decreasing*, i.e., for each $t \to t'$ in R, each $\mathsf{s} \in \mathsf{S}$, and each substitution σ, $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$ implies $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$.

(v) The rewrite rules R are *confluent and terminating modulo* E, i.e., the relation $\rightarrow_{R/E}$ is confluent and terminating.

Definition 2.1 [3,23,20] Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties (i)–(v) above. We define the relation $\rightarrow_{R,E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ by $t \rightarrow_{R,E} t'$ iff there is a $p \in Pos_\Sigma(t)$, $l \to r$ in R and substitution σ such that $t|_p =_E l\sigma$ and $t' = t[r\sigma]_p$.

Note that, since E-matching is decidable, $\rightarrow_{R,E}$ is decidable. Notions such as confluence, termination, irreducible terms or normalized substitution are defined in a straightforward manner for $\rightarrow_{R,E}$. Note that since R is convergent (modulo E), the relation $\rightarrow^!_{R,E}$ is decidable, i.e., it terminates and produces a unique term (up to E-equivalence) for each initial term t, denoted by $t{\downarrow}_{R,E}$. Of course $t \rightarrow_{R,E} t'$ implies $t \rightarrow_{R/E} t'$, but the converse need not hold. To prove completeness of $\rightarrow_{R,E}$ w.r.t. $\rightarrow_{R/E}$ we need the following additional assumption.

(vi) $\rightarrow_{R,E}$ is E*-coherent* [20,14], i.e., $\forall t_1, t_2, t_3$ we have $t_1 \rightarrow_{R,E} t_2$ and $t_1 =_E t_3$ implies $\exists t_4, t_5$ such that $t_2 \rightarrow^*_{R,E} t_4$, $t_3 \rightarrow^+_{R,E} t_5$, and $t_4 =_E t_5$.

The following theorem in [14, Proposition 1] that generalizes ideas in [20] and has an easy extension to order-sorted theories, links $\rightarrow_{R/E}$ with $\rightarrow_{R,E}$.

Theorem 2.2 (Correspondence) [20,14] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (i)–(vi) *above. Then $t_1 \rightarrow^!_{R/E} t_2$ if and only if $t_1 \rightarrow^!_{R,E} t_3$ where $t_2 =_E t_3$.*

3 R, E-Narrowing

Narrowing generalizes rewriting by performing unification at non-variable positions instead of the usual matching. The essential idea behind narrowing is to *symbolically* represent the rewriting relation between terms as a narrowing relation between more general terms.

Definition 3.1 (see, e.g., [14,18]) Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties (i)–(vi) above. Let E has a minimal, finitary and complete unification algorithm. The R, E*-narrowing* relation on $\mathcal{T}_\Sigma(\mathcal{X})$ is defined as

$t \overset{\sigma}{\rightsquigarrow}_{R,E} t'$ (or $\overset{\sigma}{\rightsquigarrow}$ if R, E is understood) if there is $p \in Pos_{\Sigma}(t)$, a rule $l \to r$ in R, and $\sigma \in CSU_E(t|_p = l)$ such that $t' = (t[r]_p)\sigma$.

In the following, we write $t \overset{id}{\rightsquigarrow}_{R,E} t'$ instead of $t \overset{\theta}{\rightsquigarrow}_{R,E} t'$ when $\theta|_{Var(t)}$ is a renaming, to indicate that θ does not really introduce new terms in t. The following results originally established in [14, Propositions 2 and 3] and extended to order-sorted theories link $\to_{R,E}$ with $\rightsquigarrow_{R,E}$.

Theorem 3.2 (Correctness) [14] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties (i)–(vi) above. If $t_1 \overset{\theta}{\rightsquigarrow}{}^{*}_{R,E} t_2$, then for any substitution ρ, $t_1\theta\rho \to^{*}_{R,E} t_2\rho$. Furthermore, the number of narrowing steps in $t_1 \overset{\theta}{\rightsquigarrow}{}^{*}_{R,E} t_2$ coincides with the number of rewrite steps in $t_1\theta\rho \to^{*}_{R,E} t_2\rho$.*

Theorem 3.3 (Completeness w.r.t. Normalized Substitutions) [14] *Let $\mathcal{R} =(\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties (i)–(vi) above. Let t_1 be a term and θ be a R, E-normalized substitution. If $t_1\theta \to^{!}_{R,E} t_2$, then there exists a term t'_2 and two R, E-normalized substitutions θ' and ρ s.t. $t_1 \overset{\theta'}{\rightsquigarrow}{}^{*}_{R,E} t'_2$, $\theta|_{Var(t_1)} =_E (\theta'\rho)|_{Var(t_1)}$, and $t_2 =_E t'_2\rho$. Furthermore, the number of rewriting and narrowing steps coincide.*

We can easily extend the previous result to allow non-normalized substitutions.

Lemma 3.4 (Completeness) *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties (i)–(vi) above. Let t_1 be a term and θ be any substitution. If $t_1\theta \to^{!}_{R,E} t_2$, then there exists a term t'_2 and two R, E-normalized substitutions θ' and ρ s.t. $t_1 \overset{\theta'}{\rightsquigarrow}{}^{*}_{R,E} t'_2$, $(\theta{\downarrow}_{R,E})|_{Var(t_1)} =_E (\theta'\rho)|_{Var(t_1)}$, and $t_2 =_E t'_2\rho$.*

The narrowing relation $\rightsquigarrow_{R,E}$ is known to give a sound and complete $R \uplus E$-unification procedure [14, Theorem 5] that under assumptions (i)–(vi) can be extended to order-sorted theories in a straightforward way. By abuse of notation, we view $R \uplus E$ as an equational theory even though R is defined as a set of rules instead of a set of equations.

Theorem 3.5 (Complete $R \uplus E$-unification Procedure) [14] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties (i)–(vi) above. Let t, t' be two terms. Then, the set of substitutions $\sigma|_{Var(t,t')}$ such that $(t \approx t') \overset{\sigma}{\rightsquigarrow}{}^{*}_{\widehat{R},E} \mathtt{tt}$ is a complete set of $R \uplus E$-unifiers for $t = t'$, where $\approx$ and $\mathtt{tt}$ are new symbols*[5] *and $\widehat{R} = R \cup \{x \approx x \to \mathtt{tt}\}$.*

When we restrict ourselves to order-sorted rewrite theories satisfying properties (i)–(vi) above, the complete set of unifiers of two terms can be restricted to normalized substitutions without loss of generality, as shown in the following Proposition. Moreover, we can obtain a minimal complete set of unifiers by considering only the most general normalized substitutions.

Proposition 3.6 (Minimal and Complete $R \uplus E$-unification Procedure) *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties (i)–(vi)*

[5] That is, we extend Σ to $\widehat{\Sigma}$ by adding a new sort Truth, not related to any sort in Σ, with constant $\mathtt{tt}$, and for each top sort of a connected component [s], an operator $\approx$: [s] × [s] → Truth.

above. Let t, t' be two terms. Then, the set of substitutions $\sigma|_{Var(t,t')}$ such that $(t \approx t') \overset{\sigma}{\rightsquigarrow}{}^{*}_{\widehat{R},E}$ $\texttt{tt}$ and there is no narrowing sequence $(t \approx t') \overset{\sigma'}{\rightsquigarrow}{}^{*}_{\widehat{R},E}$ $\texttt{tt}$ such that $\sigma'|_{Var(t,t')} <_E \sigma|_{Var(t,t')}$, is a minimal and complete set of $R \uplus E$-unifiers for $t = t'$.

4 Variants and Variant Narrowing

Although the narrowing relation $\rightsquigarrow_{R,E}$ gives a sound and complete $R \uplus E$-unification procedure, narrowing can be infinite in general, that is, this $R \uplus E$-unification procedure may not terminate even if a finite number of unifiers exist. A natural approach would be to study classes of rewrite theories where $R \uplus E$-unification is finitary and the narrowing relation $\rightsquigarrow_{R,E}$ is terminating, as studied for the case when $E = \emptyset$ in [13,15,4,19]. However, narrowing modulo E can generate many infinite sequences, specially when we consider associativity and commutativity axioms, as shown in [2,22], making it impossible to extend the good termination properties of previously studied classes of rewrite theories. In this paper, we propose a new notion of narrowing with rules Δ modulo axioms B, called *variant narrowing*, that: (i) is complete for any (Σ, B, Δ) satisfying the properties (i)–(vi) and avoids many wasteful narrowing sequences that would be created by full narrowing; and (ii) if the rules Δ satisfy the finite variant property modulo B as defined by Comon and Delaune in [2], then it can be specialized into a *terminating* and complete narrowing algorithm. We first need the notion of decomposition of an equational theory into rules and axioms.

Definition 4.1 Let (Σ, E) be an order-sorted equational theory. We call (Δ, B) a *decomposition* of E if $E = \Delta \uplus B$ and (Σ, B, Δ) is an order-sorted rewrite theory satisfying properties (i)–(vi).

Example 4.2 Let us consider the following equational theory for the exclusive or operator and the cancellation equations for public encryption/decryption. The exclusive or symbol $\oplus$ has associative and commutative (AC) properties with 0 as its unit. The symbol pk is used for public key encryption and the symbol sk for private key encryption. The equations E are as follows.

$$
\begin{array}{rlrlrl}
X \oplus 0 = X & (1) & pk(K, sk(K, M)) = M & (4) & X \oplus (Y \oplus Z) = (X \oplus Y) \oplus Z & (6)\\
X \oplus X = 0 & (2) & sk(K, pk(K, M)) = M & (5) & X \oplus Y = Y \oplus X & (7)\\
X \oplus X \oplus Y = Y & (3) & & & &
\end{array}
$$

This equational theory (Σ, E) has a decomposition into Δ containing the oriented version of equations (1)–(5) and B containing the last two associativity and commutativity equations (6)–(7) for $\oplus$. Note that equations (1)–(2) are not AC-coherent, but adding equation (3) is sufficient to recover that property.

Since narrowing can be infinite in general (specially when we consider associativity and commutativity axioms) we use the notion of *variant*, and of *finite variants* and the *finite variant property* proposed by Comon and Delaune in [2] as a technical concept that will provide a suitable characterization of unification w.r.t. an equational theory E in terms of narrowing.

Definition 4.3 [2] Given a term t and an equational theory E, we say that (t', θ) is an *E-variant* of t if $t\theta =_E t'$, where $Dom(\theta) \subseteq Var(t)$ and $Ran(\theta) \cap Var(t) = \emptyset$.

Definition 4.4 [2] Let (Δ, B) be a decomposition of an equational theory (Σ, E). A *minimal and complete set of E-variants* of a term t, denoted $V_{\Delta,B}(t)$, is a set S of E-variants of t such that, for each substitution σ, there is a variant $(t', \rho) \in S$ and a substitution θ such that: (i) t' is Δ, B-irreducible, (ii) $(t\sigma){\downarrow_{\Delta,B}} =_B t'\theta$, (iii) $(\sigma{\downarrow_{\Delta,B}})|_{Var(t)} =_B (\rho\theta)|_{Var(t)}$, and (iv) (t', ρ) is minimal, i.e., there is no $(t'', \rho') \in S$ and τ such that $\rho|_{Var(t)} =_B (\rho'\tau)|_{Var(t)}$ and $t' =_B t''\tau$.

Note that, due to the use of minimality in the previous definition, membership in $V_{\Delta,B}(t)$ is checked modulo renaming, i.e., $(t', \rho) \in V_{\Delta,B}(t)$ if there is (t'', ρ') in the set $V_{\Delta,B}(t)$ and a renaming τ such that $\rho =_B \rho'\tau$ and $t' =_B t''\tau$.

Definition 4.5 [2] Let (Δ, B) be a decomposition of an order-sorted equational theory (Σ, E). Then E, and thus (Δ, B), has the *finite variant property* if for each term t, we can compute a finite, minimal, and complete set of E-variants, denoted $FV_{\Delta,B}(t)$. We will call (Δ, B) a *finite variant decomposition* of E if (Δ, B) has the finite variant property.

Example 4.6 For (Σ, E) the theory in Example 4.2, $(0, id)$ is an E-variant of the term $t = M \oplus sk(K, pk(K, M))$. In fact, $\{(0, id)\}$ is a minimal and *complete* set of E-variants, because for any substitution σ we have $t\sigma{\downarrow_{\Delta,B}} = 0 =_B 0\ id$. Thus this one variant fulfills the requirements of being a minimal and complete set of E-variants of t.

For the term $s = X \oplus sk(K, pk(K, Y))$ we get seven variants that make up the minimal and complete set of E-variants. Specifically, $(X \oplus Y, id)$, $(Z, \{X \mapsto 0, Y \mapsto Z\})$, $(Z, \{X \mapsto Z, Y \mapsto 0\})$, $(Z, \{X \mapsto Z \oplus U, Y \mapsto U\})$, $(Z, \{X \mapsto U, Y \mapsto Z \oplus U\})$, $(0, \{X \mapsto U, Y \mapsto U\})$, and $(Z_1 \oplus Z_2, \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\})$ are the E-variants; indeed they are a minimal set. The minimality is easily checked as none of the seven given variants subsumes another one, and completeness is left for Example 4.11.

The following result from Comon and Delaune provides the necessary connection between a decomposition and the finite variant property.

Lemma 4.7 [2] *Let (Δ, B) be a decomposition of an equational theory (Σ, E). (Δ, B) satisfies the finite variant property if and only if for every term t, there is a finite set $\Theta(t)$ of substitutions such that*

$$\forall \sigma, \exists \theta \in \Theta(t), \exists \tau\ s.t.\ (\sigma{\downarrow_{\Delta,B}})|_{Var(t)} =_B (\theta\tau)|_{Var(t)} \wedge (t\sigma){\downarrow_{\Delta,B}} =_B ((t\theta){\downarrow_{\Delta,B}})\tau$$

Informally, if there is a finite number of substitutions, satisfying the properties of Lemma 4.7, then narrowing should be able to find those substitutions after a finite number of steps. This idea is characterized by the following definition.

Definition 4.8 [2] Let (Δ, B) be a decomposition of an equational theory (Σ, E). (Δ, B) satisfies the *boundedness property* if for every term t there exists an integer n, denoted $\#_{\Delta,B}(t)$, such that for every Δ, B-normalized substitution σ the normal form of $t\sigma$ is reachable by a Δ, B-rewriting derivation whose length can be bounded by n (thus independently of σ):

$$\forall t, \exists n, \forall \sigma,\ t(\sigma{\downarrow_{\Delta,B}}) \xrightarrow{\leq n}_{\Delta,B} (t\sigma){\downarrow_{\Delta,B}}$$

Finally, the following result provides the necessary connection between the boundedness property and the finite variant property.

Theorem 4.9 [2] *Let (Δ, B) be a decomposition of an equational theory (Σ, E). Then, (Δ, B) satisfies the boundedness property if and only if (Δ, B) is a finite variant decomposition of (Σ, E).*

Therefore, we can effectively compute a complete and minimal set of variants in the following form.

Proposition 4.10 (Computing the Finite Variants I) *Let (Δ, B) be a finite variant decomposition of an order-sorted equational theory (Σ, E). Let $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and $\#_{\Delta,B}(t) = n$. Then, $(s, \sigma) \in FV_{\Delta,B}(t)$ if and only if there is a narrowing derivation $t \overset{\sigma'}{\leadsto}{}^{\leq n}_{\Delta,B} s$ such that s is $\to_{\Delta,B}$-irreducible, $\sigma'|_{Var(t)}$ is $\to_{\Delta,B}$-normalized, $\sigma'|_{Var(t)} \simeq_E \sigma$, and there are no term s' and $\to_{\Delta,B}$-normalized substitutions σ'', τ such that τ is not a renaming, $t \overset{\sigma''}{\leadsto}{}^{\leq n}_{\Delta,B} s'$, $(\sigma''\tau)|_{Var(t)} =_B \sigma'|_{Var(t)}$, and $s'\tau =_B s$.*

Example 4.11 The equational theory from our running example, i.e., Example 4.2, has the boundedness property, which is shown in [9]. Thus, we can use Proposition 4.10 to get E-variants of $t = M \oplus sk(K, pk(K, M))$. As $t \to^!_{\Delta,B} 0$ we have $t \overset{id}{\leadsto}{}^!_{\Delta,B} 0$. Therefore, $(0, id) \in FV_{\Delta,B}(t)$ and it is the only element of the minimal and complete set of E-variants as no more general narrowing sequences are possible. For $s = X \oplus sk(K, pk(K, Y))$ we get (i) $s \overset{id}{\leadsto}{}^*_{\Delta,B} X \oplus Y$, (ii) $s \leadsto^*_{\{X \mapsto 0, Y \mapsto Z\},\Delta,B} Z$, (iii) $s \leadsto^*_{\{X \mapsto Z, Y \mapsto 0\},\Delta,B} Z$, (iv) $s \leadsto^*_{\{X \mapsto Z \oplus U, Y \mapsto U\},\Delta,B} Z$, (v) $s \leadsto^*_{\{X \mapsto U, Y \mapsto Z \oplus U\},\Delta,B} Z$, (vi) $s \leadsto^*_{\{X \mapsto U, Y \mapsto U\},\Delta,B} 0$, and (vii) $s \leadsto^*_{\{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\},\Delta,B} Z_1 \oplus Z_2$. No more general narrowing sequences are possible so the set of E-variants is minimal and complete.

4.1 Variant Narrowing

Let us first motivate why an alternative narrowing strategy is necessary for confluent and terminating rewrite theories with rules Δ modulo axioms B. Applying narrowing $\leadsto_{\Delta,B}$ to perform $(\Delta \uplus B)$-unification without any restriction is very wasteful, because as soon as a rewrite step $\to_{\Delta,B}$ is enabled in a term that has also narrowing steps $\leadsto_{\Delta,B}$, that rewrite step should be taken before any further narrowing steps are applied, thanks to confluence modulo B. This idea is consistent with the implementation of rewriting logic [23] and, therefore, the relation $\to^!_{\Delta,B}; \leadsto_{\Delta,B}$ makes sense as an optimization of $\leadsto_{\Delta,B}$ (see [12] for discussion about this idea). However, this is still a naive approach, since a rewrite step and a narrowing step satisfy a more general property which is the reason for being able to take the rewrite step and avoiding the narrowing step. Namely, if two narrowing steps $t \overset{\sigma_1}{\leadsto}_{\Delta,B} t_1$ and $t \overset{\sigma_2}{\leadsto}_{\Delta,B} t_2$ are possible and we have that $\sigma_1 \leq_B \sigma_2$ (i.e., σ_1 is more general than σ_2), then it is enough to take only the narrowing step using σ_1. These improvements are formalized as follows.

Definition 4.12 Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties (i)–(vi). Let us consider two narrowing steps $\alpha_1 : t \overset{\sigma_1}{\rightsquigarrow}_{\Delta,B} s_1$ and $\alpha_2 : t \overset{\sigma_2}{\rightsquigarrow}_{\Delta,B} s_2$. We write $\alpha_1 \preceq_B \alpha_2$ if[6] $\sigma_1|_{Var(t)} \leq_B \sigma_2|_{Var(t)}$ and $\alpha_1 \prec_B \alpha_2$ if $\sigma_1|_{Var(t)} <_B \sigma_2|_{Var(t)}$ (i.e., σ_1 is strictly more general than σ_2). We write $\alpha_1 \simeq_B \alpha_2$ if $\sigma_1|_{Var(t)} \simeq_B \sigma_2|_{Var(t)}$. The relation $\alpha_1 \simeq_B \alpha_2$ between two narrowing steps from t defines a set of equivalence classes between such narrowing steps. In what follows we will be interested in choosing a unique representation $\underline{\alpha} \in [\alpha]_{\simeq_B}$ in each equivalence class of narrowing steps from t. Therefore, $\underline{\alpha}$ will always denote a chosen unique representative $\underline{\alpha} \in [\alpha]_{\simeq_B}$.

Definition 4.13 Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties (i)–(vi). We define $t \overset{p,\sigma}{\rightsquigarrow}_{\underline{\Delta},B} s$ as $\underline{\alpha} : t \overset{p,\sigma}{\rightsquigarrow}_{\Delta,B} s$ such that σ is Δ,B-normalized if $\sigma|_{Var(t)}$ is not a renaming, $\underline{\alpha}$ is minimal w.r.t. the order $\preceq_B$, and $\underline{\alpha}$ is a chosen unique representative of its $\simeq_B$-equivalence class.

Note that the relation $\rightarrow^!_{\Delta,B}; \rightsquigarrow_{\Delta,B}$ is (appropriately) simulated by $\rightsquigarrow_{\underline{\Delta},B}$, since in the relation $\rightsquigarrow_{\underline{\Delta},B}$, rewriting steps are always given priority over narrowing steps.

Lemma 4.14 (Normalization of Variant Narrowing) *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties (i)–(vi). Let $t \in \mathcal{T}_\Sigma(\mathcal{X})$. If t is not Δ, B-irreducible, then, relative to the unique choice of $\underline{\alpha} \in [\alpha]_{\simeq_B}$ in Definition 4.12 , there is a unique $\rightsquigarrow_{\underline{\Delta},B}$-narrowing sequence from t such that $t \overset{id}{\rightsquigarrow}{}^*_{\underline{\Delta},B} t{\downarrow_{\Delta,B}}$.*

The following result ensures that variant narrowing is complete.

Theorem 4.15 (Completeness of Variant Narrowing) *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties (i)–(vi). If $t \overset{\sigma}{\rightsquigarrow}{}^*_{\Delta,B} (t\sigma){\downarrow_{\Delta,B}}$ with $\sigma|_{Var(t)}$ Δ, B-normalized, and there are no substitutions ρ, ρ' such that ρ' is not a renaming, $t \overset{\rho}{\rightsquigarrow}{}^*_{\Delta,B} (t\rho){\downarrow_{\Delta,B}}$, $\sigma|_{Var(t)} =_B (\rho\rho')|_{Var(t)}$, and $(t\sigma){\downarrow_{\Delta,B}} =_B ((t\rho){\downarrow_{\Delta,B}})\rho'$, then $t \overset{\sigma}{\rightsquigarrow}{}^*_{\underline{\Delta},B} (t\sigma){\downarrow_{\Delta,B}}$.*

Note that the previous theorem is only valid when Δ is confluent modulo B, instead of just *ground confluent* [21] modulo B, as shown by the following example.

Example 4.16 Let us consider the following rewrite theory, which is terminating and ground confluent but not confluent:

$$f(x) = 0 \qquad f(x) = g(x) \qquad g(0) = 0 \qquad g(s(x)) = g(x)$$

If we consider the term $f(x)$ and the narrowing step taking the first equation, then we compute the most general substitution. However, if we consider $f(x)$ and the narrowing step that takes the second equation, we will compute an infinite number of substitutions, and no one of the them is more general than the identity substitution, computed with the first equation.

[6] By definition, $Ran(\sigma_1) \cap Var(t) = \emptyset$ and $Ran(\sigma_2) \cap Var(t) = \emptyset$. Therefore, if $\sigma_1|_{Var(t)} \leq_B \sigma_2|_{Var(t)}$ (i.e., $\exists \tau$ s.t. $(\sigma_1|_{Var(t)})\tau =_B \sigma_2|_{Var(t)}$), then $Dom(\tau) \cap Var(t) = \emptyset$. In the case $\sigma_1 = id$ and $\sigma_2 \neq id$ we can assume, without any loss of generality, that σ_1 is a renaming satisfying $Ran(\sigma_1) \cap Var(t) = \emptyset$ and, therefore, there exists a substitution τ such that $(\sigma_1|_{Var(t)})\tau =_B \sigma_2|_{Var(t)}$.

Note that the relation $\leadsto^*_{\Delta,B}$ can still have many infinite narrowing derivations, e.g., for term $t = A \oplus B$ in Example 4.2, we have $A \oplus B \overset{\sigma}{\leadsto}_{\Delta,B} A' \oplus B'$ using rule (3) and substitution $\sigma = \{A \mapsto X \oplus A', B \mapsto X \oplus B'\}$. However, if (Δ, B) has the finite variant property, those infinite derivations can be safely discarded.

Theorem 4.17 (Computing the Finite Variants II) *Let (Δ, B) be a finite variant decomposition of an order-sorted equational theory (Σ, E). Let $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and $\#_{\Delta,B}(t) = n$. Then $(s, \sigma) \in FV_{\Delta,B}(t)$ if and only if there is a narrowing derivation $t \overset{\sigma'}{\leadsto}{}^{\leq n}_{\Delta,B} s$ such that s is $\to_{\Delta,B}$-irreducible, $\sigma'|_{Var(t)}$ is $\to_{\Delta,B}$-normalized, and $\sigma'|_{Var(t)} \simeq_E \sigma$.*

Even without assuming the finite variant property, another possibility is combining $\leadsto^*_{\Delta,B}$ with narrowing strategies that can avoid useless infinite narrowing derivations such as natural narrowing [11] or finite representations of an infinite search space [8]. This is left for future work.

5 Variant Narrowing and Equational Unification

Variant narrowing provides a complete equational unification procedure.

Theorem 5.1 (Variant-narrowing Unification Procedure) *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties (i)–(vi). Let t, t' be two terms. Then, the set of substitutions $\sigma|_{Var(t,t')}$ such that $(t \approx t') \overset{\sigma}{\leadsto}{}^*_{\widehat{\Delta},B} \mathtt{tt}$ (recall the definition of $\widehat{\Delta}$ in Theorem 3.5) is a minimal and complete set of $R \uplus E$-unifiers for $t = t'$.*

In the case that a rewrite theory has the boundedness property, then we can compute a bound on the number of narrowing steps needed to compute a complete set of unifiers.

Corollary 5.2 (Bounded Variant-narrowing Unification Procedure) *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties (i)–(vi) that also has the boundedness property. Let t, t' be two terms. We can put a bound on the number of steps in a narrowing sequence of the form $(t \approx t') \overset{\sigma}{\leadsto}{}^*_{\widehat{\Delta},B} \mathtt{tt}$. The bound is $\#_{\Delta,B}(t \approx t') = \#_{\Delta,B}(t) + \#_{\Delta,B}(t') + 1$. Then, let $n = \#_{\Delta,B}(t \approx t')$, the set of substitutions $\sigma|_{Var(t,t')}$ such that $(t \approx t') \overset{\sigma}{\leadsto}{}^{\leq n}_{\widehat{\Delta},B} \mathtt{tt}$ is a minimal, finite, and complete set of $R \uplus E$-unifiers for $t = t'$.*

The procedure of Corollary 5.2 for equational unification is unsatisfactory in practice, because a bigger bound allows more useless narrowing sequences up to such a bound. Thus, for a finite variant decomposition (Δ, B) of an equational theory E, the unification problem $CSU_{\Delta \uplus B}(t = t')$ is solved using the variants as in Theorem 5.3. The meet $\sigma \cap_B \sigma'$ of two substitutions σ, σ' is the set of most general substitutions τ such that there are minimal ρ and ρ' such that $\sigma\rho =_B \sigma'\rho'$, and $\tau = \sigma\rho$.

Theorem 5.3 (Finite Variant Unification Procedure) *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties (i)–(vi) that has also the boundedness property. Let t, t' be two terms. Let $FV_{\Delta \uplus B}(t) = \{(t_1, \sigma_1), \ldots, (t_n, \sigma_n)\}$*

and $FV_{\Delta \uplus B}(t') = \{(t'_1, \sigma'_1), \ldots, (t'_m, \sigma'_m)\}$, the set of substitutions $(\rho\rho')|_{Var(t,t')}$ such that there are $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$ such that $\rho \in (\sigma_i \cap_B \sigma'_j)$ and $\rho' \in CSU_B(t_i = t'_j)$ is a finite and complete set of $R \uplus E$-unifiers for $t = t'$.

Example 5.4 Using the equational theory given in Example 4.2 with $E = \Delta \uplus B$ and the E-variants found in Example 4.6 we have that for $t = M \oplus sk(K, pk(K, M))$ the set consisting of only one element, $(0, id)$, is a minimal and complete set of E-variants. For $t' = 0$ we have that $\{(0, id)\}$ is a minimal and complete set of E-variants. Then we can answer the E-unification question for $t =_{\Delta \uplus B} t'$ by considering $0 =_B 0$ which has a positive answer with substitution id. Therefore we have that $id\,id\,id = id$ is an E-unifier of t and t'.
For the term $s = X \oplus sk(K, pk(K, Y))$ we have the E-variants as shown in Example 4.6. Considering $s' = a \oplus b$ with a, b constants, we have that $(a \oplus b, id)$ is a minimal and complete set of E-variants for s'. Then the E-unification question of $s =_E s'$ can be answered by considering the following combination of E-variants. First, $0 =_B a \oplus b$ has no solution. Second, $X \oplus Y =_B a \oplus b$ has two solutions $\{X \mapsto a, Y \mapsto b\}$ and $\{X \mapsto b, Y \mapsto a\}$. Third, $Z =_B a \oplus b$ has only one solution $\{Z \mapsto a \oplus b\}$ so we get four solutions by combining it with the one in the variants, namely $\{X \mapsto 0, Y \mapsto a \oplus b\}$, $\{X \mapsto a \oplus b, Y \mapsto 0\}$, $\{X \mapsto a \oplus b \oplus U, Y \mapsto U\}$, and $\{X \mapsto U, Y \mapsto a \oplus b \oplus U\}$. Fourth, $Z_1 \oplus Z_2 =_B a \oplus b$ has the two solutions $\{Z_1 \mapsto a, Z_2 \mapsto b\}$ and $\{Z_1 \mapsto b, Z_2 \mapsto a\}$ and by combination we get $\{X \mapsto U \oplus a, Y \mapsto U \oplus b\})$ and $\{X \mapsto U \oplus b, Y \mapsto U \oplus a\})$.

6 Variant Narrowing in the Maude-NPA

Maude-NPA [6] uses backwards search from an insecure state to find attacks or to prove unreachability. This is implemented using backwards narrowing with the protocol rules *modulo* the equational theory $E = \Delta \uplus B$, which represents the algebraic properties of the underlying cryptographic theory. There are two ways to do this. One is to use built-in unification algorithms for each equational theory and combination of equational theories. The other is to use a hybrid approach, for example to use built-in algorithms for B, and a generic algorithm, such as our variant narrowing modulo B, for Δ. We have chosen the second approach for the Maude-NPA tool, as being more readily extensible to different theories with the finite variant property. That is, narrowing is used at two levels in Maude-NPA using a rewrite theory $(\Sigma, \Delta \uplus B, R)$, where the algebraic properties of the protocol's cryptographic functions are axiomatized by the equations $\Delta \uplus B$, and the protocol's transitions are axiomatized by R. At a first level, narrowing with the rules R "in reverse" modulo $\Delta \uplus B$ performs backwards search from an insecure state to an initial state. At a second level, narrowing with the oriented equations Δ modulo B computes the $\Delta \uplus B$-unifiers needed for the first level.

An important technical aspect for this approach has been the use of *order-sorted* theories. In order-sorted theories, narrowing will terminate, providing a finitary unification algorithm, in many cases in which unsorted narrowing will not. Furthermore, even in the case in which both terminate, order-sorted narrowing will often produce a smaller search space. Two interesting examples of this use of order-sorted theories to obtain finitary unification algorithms are the approximate theory for associativity in [7] and the Diffie-Hellman exponentiation theory of [5]. In both cases, narrowing with the corresponding unsorted theories is non-terminating, whereas narrowing with the order-sorted theories does terminate.

In order to demonstrate the use of associativity and commutivity (AC) in the Maude-NPA tool [6], an example involving the well-known Diffie-Hellman key agreement protocol was used in [5]. This protocol uses exponentiation in order to generate a shared secret between two parties, and is the basis for most existing key agreement protocols today. The order-sorted signature Σ is defined as $g :\ \to \mathsf{Gen}$, $exp : \mathsf{Gen{\vee}Exp} \times \mathsf{NeNonceSet} \to \mathsf{Exp}$, $exp : \mathsf{Gen} \times \mathsf{NeNonceSet} \to \mathsf{Exp}$, and $\_{*}\_ : \mathsf{NeNonceSet} \times \mathsf{NeNonceSet} \to \mathsf{NeNonceSet}$, together with the following subsort relations $\mathsf{Nonce} < \mathsf{NeNonceSet}$, and $\mathsf{Gen}\ \mathsf{Exp} < \mathsf{Gen{\vee}Exp}$. The equational theory underlying such protocol is described as the oriented equations $\Delta = \{\ exp(exp(W, Y), Z) = exp(W, Y * Z)\ \}$ and the axioms $B = \{\ (X * Y) * Z = X * (Y * Z),\ (X * Y) = Y * X\ \}$, where W is a variable of sort Gen and X, Y, Z are variables of sort $\mathsf{NeNonceSet}$. This equational theory satisfies the finite variant property according to the class of equational theories presented in [9]. The key point is that the term $exp(W, Y * Z)$ cannot be narrowed with the left-hand side $exp(exp(W, Y), Z)$ because the variable W is of sort Gen, although it can be narrowed in the unsorted sense. In our case, exp is an overloaded function symbol, for which the typing $exp : \mathsf{Gen} \times \mathsf{NeNonceSet} \to \mathsf{Exp}$ does not have any applicable equation in Δ.

The order-sorted unification in Maude-NPA at the time when [5] was written was based on full narrowing. We have implemented the unification algorithm of Theorem 5.3 in the Maude-NPA tool for the case when the bound n of Definition 4.8 is 1, and have successfully tested it on several examples, including this Diffie-Hellman example, demonstrating the feasibility of our approach.

7 Related Work and Conclusions

E-unification is a well studied topic that has been addressed in different ways and we do not attempt to cover the vast related work area. For a general survey on E-unification, see [1]. The use of the basic narrowing strategy of [13] for unification modulo an equational theory (Σ, E) that can be decomposed into $(\emptyset, \Delta)$ is the earliest work. Although it might seem that the basic narrowing strategy is subsumed into our variant strategy, this is *not* the case. Intuitively, variant narrowing and basic narrowing are both restrictions of ordinary narrowing that avoid sequences with non-normalized substitutions. Basic narrowing avoids any narrowing step performed within non-normalized computed substitutions, whereas variant narrowing discards them when found. The following example shows that basic narrowing may be non-terminating in cases when variant narrowing does terminate.

Example 7.1 Consider the rewrite theory $(\Sigma, \emptyset, \Delta)$, the set of convergent rules $\Delta = \{f(x) \to x, f(f(x)) \to f(x)\}$, and the term $t = f(x)$. Basic narrowing performs the following two narrowing steps (i) $f(x) \overset{id}{\rightsquigarrow}_{\Delta} x$ and (ii) $f(x) \overset{\sigma}{\rightsquigarrow}_{\Delta} f(x')$ with $\sigma = \{x/f(x')\}$. However, the second narrowing step leads to the following non-terminating basic narrowing sequence

$$f(x) \leadsto_{\{x/f(x')\},\Delta} f(x') \leadsto_{\{x'/f(x'')\},\Delta} f(x'') \cdots$$

Variant narrowing will perform only the first narrowing step, since the second contains a non-normalized substitution, and thus it does not produce the non-terminating narrowing sequence.

However, since the variant narrowing strategy does not carry any history of computed terms or substitutions, it is not able to avoid some useless narrowing sequences, whereas basic narrowing will avoid any of those sequences from the very beginning by avoiding narrowing inside the substitutions. The following example shows that variant narrowing may be non-terminating in cases when basic narrowing does terminate.

Example 7.2 Now, consider the rewrite theory $(\Sigma, \emptyset, \Delta)$, the set of convergent rules $\Delta = \{f(f(x)) \to x\}$, and the term $t = c(f(x), x)$ where $c \in \Sigma$. Basic narrowing performs only $c(f(x), x) \overset{\sigma}{\leadsto}_{\Delta} c(x', f(x'))$ with $\sigma = \{x/f(x')\}$ and it stops, since the term $f(x')$ is introduced by a substitution. However, our variant narrowing will perform the following non-terminating narrowing sequence

$$c(f(x), x) \overset{\theta_1}{\leadsto}_{\Delta} c(x_1, f(x_1)) \overset{\theta_2}{\leadsto}_{\Delta} c(f(x_2), x_2) \cdots$$

with $\theta_1 = \{x/f(x_1)\}$, $\theta_{i+1} = \{x_i/f(x_{i+1})\}$, since every of the individual unifiers is normalized, though the composition $\theta_1 \cdots \theta_{i+1}$ is non-normalized.

However, our argument (as well as others [2,22]) is that basic narrowing is too restrictive and indeed it can fail to be sound and complete when $B \neq \emptyset$, whereas variant narrowing is complete modulo axioms.

Example 7.3 Consider the following rewrite theory (Σ, B, Δ) from [2] where B contains associativity and commutativity of the operator $\times$ and $\Delta = \{a \times a \to 0, b \times b \to 0, a \times a \times Z \to Z, b \times b \times Z \to Z, 0 \times Z \to Z\}$. Given the term $X \times Y$, AC-basic narrowing is not able to provide the narrowing sequence $X \times Y \overset{\sigma}{\leadsto}_{\Delta,B} X' \times Y' \overset{\sigma'}{\leadsto}_{\Delta,B} 0$ with $\sigma = \{X/a \times X', Y/a \times Y'\}$ and $\sigma' = \{X'/b, Y'/b\}$, since the term $X' \times Y'$ comes from the application of the unifier σ to the right-hand side Z of the rule $a \times a \times Z \to Z$. However, our variant narrowing is able to provide this narrowing sequence, since no non-normalized substitution is generated at any step.

The repaired basic AC-narrowing strategy of [22] considers implicit extensions instead of explicit extensions to overcome incompleteness. However, [22] considers only associativity and commutativity, whereas we extend our results to more general equational axioms. On the other hand, there is much literature about (efficient) narrowing strategies. However, the related literature does not consider the case of narrowing modulo axioms.

7.1 Conclusions

We have proposed variant narrowing as a narrowing modulo B procedure that achieves efficiency, in terms of having a potentially much smaller search space than full narrowing, without losing completeness. We have also shown how, when a theory E has the finite variant property, variant narrowing specializes to algorithms for both computing the finite variant and for computing a complete and minimal set of E-unifiers. We have also explained how, under the finite variant assumption, variant narrowing can be used as a key component of a symbolic reachability analysis method for concurrent systems specified as rewrite theories, and in particular for cryptographic protocols specified this way.

Much work remains ahead. One important topic is giving sufficient conditions on an equational theory E guaranteeing the finite variant property and giving an algorithm to compute the corresponding bound for each term, which has been addressed in [10]. We have developed a prototype implementation of variant narrowing that is used as a key component in the Maude-NPA tool, and has been shown effective in analyzing and finding attacks in various cryptographic protocols. One important practical research direction is developing more optimized versions of the variant narrowing unification algorithm. Finally, modularity results, allowing us to know when modular combinations of theories enjoying the finite variant property also enjoy the same property is a topic worth investigating, since it will support modular combinations of the corresponding unification algorithms.

Acknowledgements. S. Escobar has been partially supported by the EU (FEDER) and the Spanish MEC under grant TIN2007-68093-C02-02, and Integrated Action HA 2006-0007. J. Meseguer and R. Sasse have been partially supported by the ONR Grant N00014-02-1-0715, and by the NSF Grants IIS 07-20482 and CNS 07-16638.

References

[1] F. Baader and W. Snyder. Unification theory. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume 1 of *Volume*, chapter 8, pages 445–532. Elsevier Science, 2001.

[2] H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In J. Giesl, editor, *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2005.

[3] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science, Vol. B*, pages 243–320. North-Holland, 1990.

[4] N. Dershowitz, S. Mitra, and G. Sivakumar. Decidable matching for convergent systems (preliminary version). In D. Kapur, editor, *CADE*, volume 607 of *Lecture Notes in Computer Science*, pages 589–602. Springer, 1992.

[5] S. Escobar, J. Hendrix, , C. Meadows, and J. Meseguer. Diffie-Hellman cryptographic reasoning in the Maude-NRL Protocol Analyzer. In *Proc. of the Second International Workshop on Security and Rewriting Techniques (SecReT 2007)*, 2007.

[6] S. Escobar, C. Meadows, and J. Meseguer. A rewriting-based inference system for the NRL protocol analyzer and its meta-logical properties. *Theor. Comput. Sci.*, 367(1-2):162–202, 2006.

[7] S. Escobar, C. Meadows, and J. Meseguer. Equational cryptographic reasoning in the Maude-NRL Protocol Analyzer. *Electronic Notes in Theoretical Computer Science*, 171(4):23–36, 2007.

[8] S. Escobar and J. Meseguer. Symbolic model checking of infinite-state systems using narrowing. In F. Baader, editor, *RTA*, volume 4533 of *Lecture Notes in Computer Science*, pages 153–168. Springer, 2007.

[9] S. Escobar, J. Meseguer, and R. Sasse. Variant narrowing and equational unification. Technical Report UIUCDCS-R-2007-2910, Department of Computer Science - University of Illinois at Urbana-Champaign, October 2007.

[10] S. Escobar, J. Meseguer, and R. Sasse. Effectively checking the finite variant property. In A. Voronkov, editor, *Rewriting Techniques and Applications, 19th International Conference, RTA 2008, Hagenberg, Austria, July 15-17, 2008, Proceedings*, volume 5117 of *Lecture Notes in Computer Science*, pages 79–93. Springer, 2008.

[11] S. Escobar, J. Meseguer, and P. Thati. Natural narrowing for general term rewriting systems. In J. Giesl, editor, *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings*, volume 3467 of *Lecture Notes in Computer Science*, pages 279–293. Springer, 2005.

[12] M. Hanus. Lazy narrowing with simplification. *Journal of Computer Languages*, 23(2-4):61–85, 1997.

[13] J.-M. Hullot. Canonical forms and unification. In W. Bibel and R. A. Kowalski, editors, *CADE*, volume 87 of *Lecture Notes in Computer Science*, pages 318–334. Springer, 1980.

[14] J.-P. Jouannaud, C. Kirchner, and H. Kirchner. Incremental construction of unification algorithms in equational theories. In J. Díaz, editor, *ICALP*, volume 154 of *Lecture Notes in Computer Science*, pages 361–373. Springer, 1983.

[15] D. Kapur and P. Narendran. Matching, Unification and Complexity. *ACM SIGSAM Bulletin*, 21(4):6–9, 1987.

[16] J. Meseguer. Conditioned rewriting logic as a united model of concurrency. *Theor. Comput. Sci.*, 96(1):73–155, 1992.

[17] J. Meseguer. Membership algebra as a logical framework for equational specification. In F. Parisi-Presicce, editor, *WADT*, volume 1376 of *Lecture Notes in Computer Science*, pages 18–61. Springer, 1997.

[18] J. Meseguer and P. Thati. Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols. *Higher-Order and Symbolic Computation*, 20(1–2):123–160, 2007.

[19] S. Mitra. *Semantic Unification for Convergent Rewrite Systems.* PhD thesis, University Illinois at Urbana-Champaign, 1994.

[20] G. E. Peterson and M. E. Stickel. Complete sets of reductions for some equational theories. *J. ACM*, 28(2):233–264, 1981.

[21] TeReSe, editor. *Term Rewriting Systems.* Cambridge University Press, Cambridge, 2003.

[22] E. Viola. E-unifiability via narrowing. In A. Restivo, S. R. D. Rocca, and L. Roversi, editors, *ICTCS*, volume 2202 of *Lecture Notes in Computer Science*, pages 426–438. Springer, 2001.

[23] P. Viry. Equational rules for rewriting logic. *Theor. Comput. Sci.*, 285(2):487–517, 2002.