Folding Variant Narrowing and Optimal Variant Termination⋆

Santiago Escobar[1], Ralf Sasse[2] and José Meseguer[2]

[1] DSIC-ELP, Universidad Politécnica de Valencia, Spain. `sescobar@dsic.upv.es`
[2] University of Illinois at Urbana-Champaign, USA.
{`rsasse,meseguer`}`@illinois.edu`

Abstract. If a set of equations $E \cup Ax$ is such that E is confluent, terminating, and coherent modulo Ax, narrowing with E modulo Ax provides a complete $E \cup Ax$-unification algorithm. However, except for the hopelessly inefficient case of full narrowing, nothing seems to be known about effective narrowing strategies in the general modulo case beyond the quite depressing observation that basic narrowing is *incomplete* modulo AC. In this work we propose an effective strategy based on the idea of the $E \cup Ax$-variants of a term that we call *folding variant narrowing*. This strategy is *complete*, both for computing $E \cup Ax$-unifiers and for computing a minimal complete set of variants for any input term. And it is *optimally variant terminating* in the sense of terminating for an input term t iff t has a finite, complete set of variants. The applications of folding variant narrowing go beyond providing a complete $E \cup Ax$-unification algorithm: computing the $E \cup Ax$-variants of a term may be just as important as computing $E \cup Ax$-unifiers in recent applications of folding variant narrowing such as termination methods modulo axioms, and checking confluence and coherence of rules modulo axioms.

1 Introduction

Narrowing is a fundamental rewriting technique useful for many purposes, including equational unification and equational theorem proving [15], combinations of functional and logic programming [12,13], partial evaluation [2], symbolic reachability analysis of rewrite theories understood as transition systems [19], and symbolic model checking [7].

Narrowing with confluent and terminating equations E enjoys key completeness results, including the generation of a complete set of E-unifiers and the covering of all rewrite sequences starting at an instance of term t by a normalized substitution, see [15]. However, full narrowing (i.e., narrowing at all non-variable term positions) can be quite inefficient both in space and time. Therefore, much work has been devoted to *narrowing strategies* that, while remaining complete,

---

⋆

can have a much smaller search space. For instance, the *basic narrowing* strategy [15] was shown to be complete w.r.t. a complete set of E-unifiers for confluent and terminating equations E.

Termination aspects are another important potential benefit of narrowing strategies, since they can sometimes *terminate*, generating a finite search tree when narrowing an input term t, while full narrowing may generate an infinite search tree on the same input term. For example, works such as [15,1] investigate conditions under which basic narrowing, one of the most fully studied strategies for termination purposes, terminates. Similarly, so-called lazy narrowing strategies also seek to both reduce the search space and to increase the chances of termination [10], but we are not aware of lazy narrowing strategies for the modulo case.

By decomposing an equational theory $\mathcal{E}$ into a set of rules E and a set of equational axioms Ax for which a finite and complete Ax-unification algorithm exists, and imposing natural requirements such as confluence, termination and coherence of the rules E *modulo* Ax, narrowing can be generalized to narrowing *modulo* axioms Ax. As known since the original study [16], the good completeness properties of standard narrowing extend naturally to similar completeness properties for narrowing modulo Ax. This generalization of narrowing to the modulo case has many applications. It is, to begin with, a key component of theorem proving systems that often reason modulo axioms such as associativity–commutativity, and greatly improves the efficiency of general paramodulation. It is, furthermore, very important for adding functional-logical features to algebraic functional languages supporting rewriting modulo combinations of equational axioms. Yet another recent area with many applications is cryptographic protocol analysis, where there is strong interest in analyzing protocol security *modulo* the algebraic theory $\mathcal{E}$ of a protocol's cryptographic functions, since protocols deemed to be secure under the standard Dolev-Yao model, which treats the underlying cryptography as a black box, can sometimes be broken by clever use of algebraic properties, e.g., [22].

However, very little is known at present about effective narrowing strategies in the modulo case, and some of the known anomalies ring a cautionary note, to the effect that the naive extensions of standard narrowing strategies can fail rather badly in the modulo case. Indeed, except for [16,24], we are not aware of any studies about narrowing strategies in the modulo case. Furthermore, as work in [4,24] shows, narrowing modulo axioms such as associativity-commutativity (AC) can very easily lead to non-terminating behavior and, what is worse, as shown in the Example 1 below, due to Comon-Lundh and Delaune, basic narrowing modulo AC is *not* complete.

Example 1. [4] Consider the equational theory $(\Sigma, E \uplus Ax)$ where E contains the following equations and Ax contains associativity and commutativity for $+$:

$$a + a = 0 \quad (1) \qquad a + a + X = X \quad (3) \qquad 0 + X = X \quad (5)$$
$$b + b = 0 \quad (2) \qquad b + b + X = X \quad (4)$$

2

The set E is terminating, AC-convergent, and AC-coherent. Consider now the unification problem $X_1 + X_2 \stackrel{?}{=} 0$ and one of the possible solutions $\sigma = \{X_1 \mapsto a+b; X_2 \mapsto a+b\}$, which is a normalized solution. It is well-known that in the free case (when $Ax = \emptyset$) basic narrowing is complete for unification in the sense of lifting all innermost rewriting sequences (see [20]). That is, given a term t and a substitution σ, every innermost rewriting sequence starting from $t\sigma$ can be *lifted* to a basic narrowing sequence from t computing a substitution more general than σ. This completeness property fails for basic narrowing modulo AC as shown by the above example when we consider the term $t = X_1 + X_2$ instantiated with σ and the following *innermost rewriting sequence modulo AC* from $t\sigma$ (we underline the redex at each step): $\underline{(a+b)+(a+b)} \rightarrow_{E,AC} \underline{b+b} \rightarrow_{E,AC} 0$. As further explained in Example 3 below, basic narrowing modulo AC, i.e., the extension of basic narrowing to AC where we just replace syntactic unification by AC-unification, cannot lift the above innermost sequence for $t\sigma$, because it is necessary to narrow inside the term generated by instantiation. Therefore, basic narrowing modulo AC is incomplete in the sense of *not* providing a complete $E \cup AC$-unification algorithm, even though E may be confluent, terminating, and coherent modulo AC.

It seems clear that full narrowing, although complete, is hopelessly inefficient in the free case, and even more so modulo a set Ax of axioms. The above example shows that known efficient strategies like basic narrowing can totally fail to enjoy the desired completeness properties modulo axioms. What can be done? For equational theories of the form $E \cup Ax$, where E is confluent, terminating, and coherent modulo Ax, and such that $E \cup Ax$ has the *finite variant property* (FVP) in the sense of [4], we proposed in [9] a narrowing strategy that is complete in the sense of generating a complete set of most general $E \cup Ax$-unifiers, and *terminates* for any input term computing its complete set of variants. And in [8] we gave a method that can be used to check if $E \cup Ax$ is FVP. However, FVP is a quite strong restriction. To the best of our knowledge, except for the hopelessly inefficient case of full narrowing, nothing is known at present about a *general* narrowing strategy that is effective and complete in an adequate sense, including being complete for computing $E \cup Ax$-unifiers, for *any* theory $E \cup Ax$ under the minimum requirements that E is confluent, terminating, and coherent modulo Ax. It turns out that the notion of *variant*, which makes sense for any such theory $E \cup Ax$ and does not depend on FVP, provides the key to obtaining a strategy meeting these requirements, and sheds considerable light on the very process of computing $E \cup Ax$-unifiers by narrowing.

Our contributions. In this paper, for any theory $E \cup Ax$ with E confluent, terminating, and coherent modulo Ax, we propose *folding variant narrowing* as such a general and effective strategy satisfying the following properties:

1. It is *complete*, both in the sense of computing a complete set of $E \cup Ax$-unifiers, and of computing a minimal and complete set of variants for any input term t.

3

2. It is *optimal variant terminating*, in the sense that it will terminate for an input term t if and only if t has a finite, complete set of variants (in particular, it will terminate for *any* term t iff $E \cup Ax$ is FVP).

Furthermore, we show that basic narrowing, *both* in the free case ($Ax = \emptyset$) and in the AC case, fails to satisfy properties (1) and/or (2).

The rest of the paper is organized as follows. After some preliminaries in Section 2, we present in Section 3 the notion of variant of a term w.r.t. an order-sorted equational theory and its application to equational unification. Then, we study in Section 4 how to effectively compute the set of variants of a term and provide the folding variant narrowing strategy. In Section 5 we describe future work and conclude the paper.

2   Preliminaries

We follow the classical notation and terminology from [23] for term rewriting and from [18] for rewriting logic and order-sorted notions. We assume an order-sorted signature $\mathbf{\Sigma} = (S, \leq, \Sigma)$ with poset of sorts $(S, \leq)$ and for each sort $s \in S$ where the connected component of s in $(S, \leq)$ has a top sort, denoted $[s]$, and all $f : s_1 \cdots s_n \to s$ with $n \geq 1$ have a top sort overloading $f : [s_1] \cdots [s_n] \to [s]$. We also assume an S-sorted family $\mathcal{X} = \{\mathcal{X}_\mathsf{s}\}_{\mathsf{s} \in \mathsf{S}}$ of 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 order-sorted term algebras.

For a term t we write $Var(t)$ for the set of all variables in t. The set of positions of a term t is written $Pos(t)$, and the set of non-variable positions $Pos_\Sigma(t)$. The root position 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* $\sigma \in \mathcal{S}ubst(\Sigma, \mathcal{X})$ is a sorted mapping from a finite subset of $\mathcal{X}$, written $Dom(\sigma)$, to $\mathcal{T}_\Sigma(\mathcal{X})$. The set of variables introduced by σ is $Ran(\sigma)$. 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 $t\sigma$. For simplicity, we assume that every substitution is idempotent, i.e., for σ, $Dom(\sigma) \cap Ran(\sigma) = \emptyset$. Substitution idempotency ensures $t\sigma = (t\sigma)\sigma$. The restriction of σ to a set of variables V is $\sigma|_V$; sometimes we write $\sigma|_{t_1,\ldots,t_n}$ to denote $\sigma|_V$ where $V = Var(t_1) \cup \cdots \cup Var(t_n)$. Composition of two substitutions is denoted by $\sigma\sigma'$. We call an idempotent substitution σ a variable *renaming* if there is another substitution σ^{-1} such that $(\sigma\sigma^{-1})|_{Dom(\sigma)} = id$.

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

The $\mathcal{E}$-*subsumption* preorder $\sqsubseteq_\mathcal{E}$ (or $\sqsubseteq$ if $\mathcal{E}$ is understood) holds between $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$, denoted $t \sqsubseteq_\mathcal{E} t'$ (meaning that t' is *more general* than t modulo

$\mathcal{E}$), if there is a substitution σ such that $t =_{\mathcal{E}} t'\sigma$; such a substitution σ is said to be an $\mathcal{E}$-*match* from t to t'. The $\mathcal{E}$-renaming equivalence $t \approx_{\mathcal{E}} t'$, holds if there is a variable renaming θ such that $t\theta =_{\mathcal{E}} t'\theta$. For substitutions σ, ρ and a set of variables V we define $\sigma|_V =_{\mathcal{E}} \rho|_V$ if $x\sigma =_{\mathcal{E}} x\rho$ for all $x \in V$; $\sigma|_V \sqsubseteq_{\mathcal{E}} \rho|_V$ if there is a substitution η such that $\sigma|_V =_{\mathcal{E}} (\rho\eta)|_V$; and $\sigma|_V \approx_{\mathcal{E}} \rho|_V$ if there is a renaming η such that $(\sigma\eta)|_V =_{\mathcal{E}} \rho|_V$.

An $\mathcal{E}$-*unifier* for a Σ-equation $t = t'$ is a substitution σ such that $t\sigma =_{\mathcal{E}} t'\sigma$. For $Var(t) \cup Var(t') \subseteq W$, a set of substitutions $CSU_{\mathcal{E}}^W(t = t')$ is said to be a *complete* set of unifiers of the equation $t =_{\mathcal{E}} t'$ away from W if: (i) each $\sigma \in CSU_{\mathcal{E}}^W(t = t')$ is an $\mathcal{E}$-unifier of $t =_{\mathcal{E}} t'$; (ii) for any $\mathcal{E}$-unifier ρ of $t =_{\mathcal{E}} t'$ there is a $\sigma \in CSU_{\mathcal{E}}^W(t = t')$ such that $\rho|_W \sqsubseteq_{\mathcal{E}} \sigma|_W$; (iii) for all $\sigma \in CSU_{\mathcal{E}}^W(t = t')$, $Dom(\sigma) \subseteq (Var(t) \cup Var(t'))$ and $Ran(\sigma) \cap W = \emptyset$. If the set of variables W is irrelevant or understood from the context, we write $CSU_{\mathcal{E}}(t = t')$ instead of $CSU_{\mathcal{E}}^W(t = t')$. An $\mathcal{E}$-unification algorithm is *complete* if for any equation $t = t'$ it generates a complete set of $\mathcal{E}$-unifiers. Note that this set needs not be finite. A unification algorithm is said to be *finitary* and complete if it always terminates after generating a finite and complete set of solutions. A unification algorithm is said to be *minimal* if it always provides a maximal (w.r.t. $\sqsubseteq_{\mathcal{E}}$) set of unifiers.

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 (Σ, Ax, R) with Σ an order-sorted signature, Ax 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 $t \to_{p,R} t'$ holds between t and t' iff there exist $p \in Pos_{\Sigma}(t)$, $l \to r \in R$ and a substitution σ, such that $t|_p = l\sigma$, and $t' = t[r\sigma]_p$. The subterm $t|_p$ is called a *redex*. The relation $\to_{R/Ax}$ on $\mathcal{T}_{\Sigma}(\mathcal{X})$ is $=_{Ax}; \to_R; =_{Ax}$. Note that $\to_{R/Ax}$ on $\mathcal{T}_{\Sigma}(\mathcal{X})$ induces a relation $\to_{R/Ax}$ on the free (Σ, Ax)-algebra $\mathcal{T}_{\Sigma/Ax}(\mathcal{X})$ by $[t]_{Ax} \to_{R/Ax} [t']_{Ax}$ iff $t \to_{R/Ax} t'$. The transitive closure of $\to_{R/Ax}$ is denoted by $\to_{R/Ax}^+$ and the transitive and reflexive closure of $\to_{R/Ax}$ is denoted by $\to_{R/Ax}^*$. We say that a term t is $\to_{R/Ax}$-irreducible (or just R/Ax-irreducible) if there is no term t' such that $t \to_{R/Ax} t'$.

For substitutions σ, ρ and a set of variables V we define $\sigma|_V \to_{R/Ax} \rho|_V$ if there is $x \in V$ such that $x\sigma \to_{R/Ax} x\rho$ and for all other $y \in V$ we have $y\sigma =_{Ax} y\rho$. A substitution σ is called R/Ax-*normalized* (or normalized) if $x\sigma$ is R/Ax-irreducible for all $x \in V$.

We say that the relation $\to_{R/Ax}$ is *terminating* if there is no infinite sequence $t_1 \to_{R/Ax} t_2 \to_{R/Ax} \cdots t_n \to_{R/Ax} t_{n+1} \cdots$. We say that the relation $\to_{R/Ax}$ is *confluent* if whenever $t \to_{R/Ax}^* t'$ and $t \to_{R/Ax}^* t''$, there exists a term t''' such that $t' \to_{R/Ax}^* t'''$ and $t'' \to_{R/Ax}^* t'''$. An order-sorted rewrite theory (Σ, Ax, R) is confluent (resp. terminating) if the relation $\to_{R/Ax}$ is confluent (resp. terminating). In a confluent, terminating, order-sorted rewrite theory, for each term $t \in \mathcal{T}_{\Sigma}(\mathcal{X})$, there is a unique (up to Ax-equivalence) R/Ax-irreducible term t' obtained from t by rewriting to canonical form, which is denoted by $t \to_{R/Ax}^! t'$ or $t\downarrow_{R/Ax}$ (when t' is not relevant).

2.1 R, Ax-rewriting

Since Ax-congruence classes can be infinite, $\rightarrow_{R/Ax}$-reducibility is undecidable in general. Therefore, R/Ax-rewriting is usually implemented [16] by R, Ax-rewriting. We assume the following properties on R and Ax:

1. Ax is *regular*, i.e., for each $t = t'$ in Ax, we have $Var(t) = Var(t')$, and *sort-preserving*, i.e., for each substitution σ, we have $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$ iff $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$; furthermore all variables in $Var(t)$ have a top sort.
2. Ax has a finitary and complete unification algorithm.
3. For each $t \rightarrow t'$ in R we have $Var(t') \subseteq Var(t)$.
4. R is *sort-decreasing*, i.e., for each $t \rightarrow t'$ in R, each $\mathsf{s} \in \mathsf{S}$, and each substitution σ, $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$ implies $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_{\mathsf{s}}$.
5. The rewrite rules R are *confluent and terminating modulo Ax*, i.e., the relation $\rightarrow_{R/Ax}$ is confluent and terminating.

Definition 1 (Rewriting modulo [25]). *Let (Σ, Ax, R) be an order-sorted rewrite theory satisfying properties (1)–(5). We define the relation $\rightarrow_{R,Ax}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ by $t \rightarrow_{p,R,Ax} t'$ (or just $t \rightarrow_{R,Ax} t'$) iff there is a $p \in Pos_\Sigma(t)$, $l \rightarrow r$ in R and substitution σ such that $t|_p =_{Ax} l\sigma$ and $t' = t[r\sigma]_p$.*

Note that, since Ax-matching is decidable, $\rightarrow_{R,Ax}$ is decidable. Notions such as confluence, termination, irreducible terms, and normalized substitution, are defined in a straightforward manner for $\rightarrow_{R,Ax}$. Note that since R is confluent and terminating modulo Ax, the relation $\rightarrow^!_{R,Ax}$ is decidable, i.e., it terminates and produces a unique term (up to Ax-equivalence) for each initial term t, denoted by $t\downarrow_{R,Ax}$. Of course $t \rightarrow_{R,Ax} t'$ implies $t \rightarrow_{R/Ax} t'$, but the converse does not need to hold. To prove completeness of $\rightarrow_{R,Ax}$ w.r.t. $\rightarrow_{R/Ax}$ we need the following additional *coherence* assumption; we refer the reader to [11,25,17] for coherence completion algorithms.

6. $\rightarrow_{R,Ax}$ is *Ax-coherent* [16], i.e., $\forall t_1, t_2, t_3$ we have $t_1 \rightarrow_{R,Ax} t_2$ and $t_1 =_{Ax} t_3$ implies $\exists t_4, t_5$ such that $t_2 \rightarrow^*_{R,Ax} t_4$, $t_3 \rightarrow^+_{R,Ax} t_5$, and $t_4 =_{Ax} t_5$.

The following theorem in [16, Proposition 1] that generalizes ideas in [21] and has an easy extension to order-sorted theories, links $\rightarrow_{R/Ax}$ with $\rightarrow_{R,Ax}$.

Theorem 1 (Correspondence [21,16]). *Let (Σ, Ax, R) be an order-sorted rewrite theory satisfying properties (1)–(6). Then $t_1 \rightarrow^!_{R/Ax} t_2$ iff $t_1 \rightarrow^!_{R,Ax} t_3$, where $t_2 =_{Ax} t_3$.*

Finally, we provide the notion of decomposition of an equational theory into rules and axioms.

Definition 2 (Decomposition [9]). *Let $(\Sigma, \mathcal{E})$ be an order-sorted equational theory. We call (Σ, Ax, E) a decomposition of $(\Sigma, \mathcal{E})$ if $\mathcal{E} = E \uplus Ax$ and (Σ, Ax, E) is an order-sorted rewrite theory satisfying properties (1)–(6).*

3 Variants & Equational Unification

Suppose that an equational theory $\mathcal{E}$ is decomposed into a set of rules E and a set of equational axioms Ax such that a finite and complete Ax-unification algorithm exists, and the rules E are confluent, terminating, sort-decreasing, and coherent *modulo* Ax. Given a term t, an E,Ax-*variant* of t is a pair (t', θ) with t' an E,Ax-canonical form of the term $t\theta$. That is, the variants of a term intuitively give us all the irreducible *patterns* that instances of t can reduce to. Of course, some variants are *more general* than others, that is, there is a natural preorder $(t', \theta') \sqsubseteq_{E,Ax} (t'', \theta'')$ defining when variant (t'', θ'') is *more general* than variant (t', θ'). This is important, because even though the set of E,Ax-variants of a term t may be infinite, the set of *most general variants* (that is maximal elements in the generalization preorder up to Ax-equivalence and variable renaming) may be finite.

The intimate connection of variants with $\mathcal{E}$-unification is then as follows. Suppose that we add to our theory decomposition $E \uplus Ax$ a binary equality predicate eq, a new constant tt[3] and for each top sort $[s]$ and x of sort $[s]$ an extra rule $eq(x, x) \rightarrow tt$. Then, given any two terms t, t', if θ is a $\mathcal{E}$-unifier of t and t', then the E,Ax canonical forms of $t\theta$ and $t'\theta$ must be Ax-equal and therefore the pair (tt, θ) must be a variant of the term $eq(t, t')$. Furthermore, if the term $eq(t, t')$ has a finite set of most general variants, then we are *guaranteed* that the set of most general $\mathcal{E}$-unifiers of t and t' is *finite*.

We characterize a notion of variant semantics for equational theories.

Definition 3 (Variant Semantics). *Let (Σ, Ax, E) be a decomposition of an equational theory and t be a term. We define the set of variants of t as $[\![t]\!]^{\star}_{E,Ax} = \{(t', \theta) \mid \theta \in \mathcal{S}ubst(\Sigma, \mathcal{X}), t\theta \rightarrow^{!}_{E,Ax} t'', \text{ and } t'' =_{Ax} t'\}$.*

Let us make explicit the relation between variants and $\mathcal{E}$-unification.

Proposition 1 (Variant-based Unification). *Let (Σ, Ax, E) be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. Let t_1, t_2 be two terms. Then, ρ is a $\mathcal{E}$-unifier of t_1 and t_2 iff $\exists (t', \rho) \in [\![t_1]\!]^{\star}_{E,Ax} \cap [\![t_2]\!]^{\star}_{E,Ax}$.*

Some variants are more general than others. We write $(t_1, \theta_1) \sqsubseteq_{E,Ax} (t_2, \theta_2)$ to denote that variant (t_2, θ_2) is *more general* than variant (t_1, θ_1). Our notion of being more general takes into account not only the instantiation relation between the two substitutions θ_1 and θ_2 and the two normal forms t_1 and t_2 of a term t, but also whether θ_2 is already an E,Ax-normalized substitution, since, for a substitution, the less E,Ax rewrite steps, the better.

Definition 4 (Variant Preordering). *Let (Σ, Ax, E) be a decomposition of an equational theory and t be a term. Given two variants $(t_1, \theta_1), (t_2, \theta_2) \in$*

---

[3] 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 $\mathtt{eq} : [s] \times [s] \rightarrow$ Truth.

$[\![t]\!]^{\star}_{E,Ax}$, *we write* $(t_1, \theta_1) \sqsubseteq_{E,Ax} (t_2, \theta_2)$, *meaning* (t_2, θ_2) *is* more general *than* (t_1, θ_1), *iff there is a substitution* ρ *such that* $t_1 =_{Ax} t_2\rho$ *and* $\theta_1{\downarrow}_{E,Ax} =_{Ax} \theta_2\rho$. *We write* $(t_1, \theta_1) \sqsubset_{E,Ax} (t_2, \theta_2)$ *if for every substitution* ρ *such that* $t_1 =_{Ax} t_2\rho$ *and* $\theta_1{\downarrow}_{E,Ax} =_{Ax} \theta_2\rho$, *then* ρ *is not a renaming.*

We are, indeed, interested in equivalence classes for variant semantics and provide a notion of semantic equality, written $\simeq_{E,Ax}$, based on $\sqsubseteq_{E,Ax}$.

Definition 5 (Variant Equality). *Let* (Σ, Ax, E) *be a decomposition of an equational theory and t be a term. For $S_1, S_2 \subseteq [\![t]\!]^{\star}_{E,Ax}$, we write $S_1 \sqsubseteq_{E,Ax} S_2$ iff for each $(t_1, \theta_1) \in S_1$, there exists $(t_2, \theta_2) \in S_2$ s.t. $(t_1, \theta_1) \sqsubseteq_{E,Ax} (t_2, \theta_2)$. We write $S_1 \simeq_{E,Ax} S_2$ iff $S_1 \sqsubseteq_{E,Ax} S_2$ and $S_2 \sqsubseteq_{E,Ax} S_1$.*

Despite the previous semantic notion of equivalence, the following, more syntactic notion of equality of variants up to renaming is useful.

Definition 6 (Ax-Equality). *Let* (Σ, Ax, E) *be a decomposition of an equational theory and t be a term. For $(t_1, \theta_1), (t_2, \theta_2) \in [\![t]\!]^{\star}_{E,Ax}$, we write $(t_1, \theta_1) \approx_{Ax} (t_2, \theta_2)$ if there is a renaming ρ such that $t_1\rho =_{Ax} t_2\rho$ and $\theta_1\rho =_{Ax} \theta_2\rho$. For $S_1, S_2 \subseteq [\![t]\!]^{\star}_{E,Ax}$, we write $S_1 \approx_{Ax} S_2$ if for each $(t_1, \theta_1) \in S_1$, there exists $(t_2, \theta_2) \in S_2$ s.t. $(t_1, \theta_1) \approx_{Ax} (t_2, \theta_2)$, and for each $(t_2, \theta_2) \in S_2$, there exists $(t_1, \theta_1) \in S_1$ s.t. $(t_2, \theta_2) \approx_{Ax} (t_1, \theta_1)$.*

The preorder of Definition 4 allows us to provide a most general and complete set of variants that encompasses all the variants for a term t.

Definition 7 (Most General and Complete Variant Semantics). *Let* (Σ, Ax, E) *be a decomposition of an equational theory and t be a term. A* most general and complete variant semantics *of t, denoted $[\![t]\!]_{E,Ax}$, is a subset $[\![t]\!]_{E,Ax} \subseteq [\![t]\!]^{\star}_{E,Ax}$ such that: (i) $[\![t]\!]^{\star}_{E,Ax} \sqsubseteq_{E,Ax} [\![t]\!]_{E,Ax}$, and (ii) for each $(t_1, \theta_1) \in [\![t]\!]_{E,Ax}$, there is no $(t_2, \theta_2) \in [\![t]\!]_{E,Ax}$ s.t. $(t_1, \theta_1) \not\approx_{Ax} (t_2, \theta_2)$ and $(t_1, \theta_1) \sqsubseteq_{E,Ax} (t_2, \theta_2)$.*

Note that, for any term t, $[\![t]\!]^{\star}_{E,Ax} \simeq_{E,Ax} [\![t]\!]_{E,Ax}$ but, in general, $[\![t]\!]^{\star}_{E,Ax} \not\approx_{Ax} [\![t]\!]_{E,Ax}$. Also, by definition, all the substitutions in $[\![t]\!]_{E,Ax}$ are E,Ax-normalized. Moreover, $[\![t]\!]_{E,Ax}$ is unique up to $\approx_{Ax}$ and provides a very succinct description of $[\![t]\!]^{\star}_{E,Ax}$. Indeed, up to Ax-equality, $[\![t]\!]_{E,Ax}$ characterizes the set of *maximal elements* (therefore, most general variants) of the preorder $([\![t]\!]_{E,Ax}, \sqsubseteq_{E,Ax})$.

Again, let us make explicit the relation between variants and $\mathcal{E}$-unification.

Proposition 2 (Minimal and Complete $\mathcal{E}$-unification). *Let* (Σ, Ax, E) *be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. Let t, t' be two terms. Then, $S = \{\theta \mid (\texttt{tt}, \theta) \in [\![\texttt{eq}(t, t')]\!]_{\widehat{E},Ax}\}$ is a minimal and complete set of $\mathcal{E}$-unifiers for $t = t'$, where $\texttt{eq}$ and $\texttt{tt}$ are new symbols defined in Footnote 3 and $\widehat{E} = E \cup \{\texttt{eq}(X, X) \rightarrow \texttt{tt}\}$.*

Example 2. Let us consider the following equational theory for the exclusive or operator and the cancellation equations for public encryption/decryption, which is actually useful for protocol verification (see [19]). This equational theory is

relevant because there are no unification procedures directly applicable to it, e.g. unification algorithms for exclusive-or such as [3] do not directly apply if extra equations are added. 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 equational theory $(\Sigma, \mathcal{E})$ has a decomposition into E containing the following oriented equations and Ax containing associativity and commutativity for $\oplus$:

$$X \oplus 0 = X \quad (6) \qquad X \oplus X = 0 \quad (7) \qquad pk(K, sk(K, M)) = M \quad (9)$$

$$X \oplus X \oplus Y = Y \quad (8) \qquad sk(K, pk(K, M)) = M \quad (10)$$

Note that equations (6)–(7) are not AC-coherent, but adding equation (8) is sufficient to recover that property. For $t = M \oplus sk(K, pk(K, M))$ and $s = X \oplus sk(K, pk(K, Y))$, we have that $[\![t]\!]_{E,Ax} = \{(0, id)\}$ and $[\![s]\!]_{E,Ax} = \{(X \oplus Y, id), (Z, \{X \mapsto 0, Y \mapsto Z\}), (Z, \{X \mapsto Z, Y \mapsto 0\}), (Z, \{X \mapsto Z \oplus U, Y \mapsto U\}), (Z, \{X \mapsto U, Y \mapsto Z \oplus U\}), (0, \{X \mapsto U, Y \mapsto U\}), (Z_1 \oplus Z_2, \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\})\}$. This set is the most general one w.r.t. $\sqsubseteq_{E,Ax}$.

The *finite variant property* defined by Comon-Lundh and Delaune [4], provides a useful sufficient condition for finitary $\mathcal{E}$-unification. Essentially, it determines whether every term has a finite number of most general variants.

Definition 8 (Finite variant property [4]). *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$. *Then* $(\Sigma, \mathcal{E})$, *and thus* (Σ, Ax, E), *has the finite variant property iff for each term* t, *the set* $[\![t]\!]_{E,Ax}$ *is finite. We will call* (Σ, Ax, E) *a* finite variant decomposition *of* $(\Sigma, \mathcal{E})$ *iff* (Σ, Ax, E) *has the finite variant property.*

In [8] we developed a technique to check whether an equational theory has the finite variant property. Using our technique it is easy to check that Example 2 has the finite variant property, as every right–hand side is a constant symbol or a variable.

Finally, it is clear that when we consider a finite variant decomposition, we have a decidable unification algorithm.

Corollary 1 (Finitary $\mathcal{E}$-unification). *Let* (Σ, Ax, E) *be a finite variant decomposition of an equational theory* $(\Sigma, \mathcal{E})$. *Then, for any two given terms* t, t', $S = \{\theta \mid (\mathtt{tt}, \theta) \in [\![\mathtt{eq}(t, t')]\!]_{\widehat{E},Ax}\}$ *is a* finite, minimal, *and* complete *set of* $\mathcal{E}$*-unifiers for* $t = t'$, *where* $\widehat{E}$, $\mathtt{eq}$, *and* $\mathtt{tt}$ *are defined as in Proposition 2.*

Note that the opposite does not hold: given two terms t, t' that have a finite, minimal, and complete set of $\mathcal{E}$-unifiers, the equational theory $(\Sigma, \mathcal{E})$ may not have a finite variant decomposition (Σ, Ax, E). An example is the unification under homomorphism (or one-side distributivity), where there is a finite number of unifiers of two terms but the theory does not satisfy the finite variant property (see [4,8]); the key idea is that the term $\mathtt{eq}(t, t')$ may have an infinite number of variants even though there is only a finite set of most general variants of the form $(\mathtt{tt}, \theta)$.

Once we have clarified the intimate relation between variants and equational unification, we consider in the next section how to compute a complete set of variants of a term.

4 Variants and Narrowing-based Equational Unification

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 with variables.

Definition 9 (Narrowing modulo [16,19]). *Let (Σ, Ax, R) be an order-sorted rewrite theory. Let $CSU_{Ax}(u = u')$ provide a finitary and complete set of Ax-unifiers for any pair of terms u, u' with the same top sort. Let t be a term and W be a set of variables such that $Var(t) \subseteq W$. The R, Ax-narrowing relation on $\mathcal{T}_\Sigma(\mathcal{X})$ is defined as $t \leadsto_{p,\sigma,R,Ax} t'$ ($\leadsto_{\sigma,R,Ax}$ if p is understood, and $\leadsto$ if σ, R, Ax are understood) if there is $p \in Pos_\Sigma(t)$, a rule $l \to r \in R$ properly renamed s.t. $Var(l) \cap W = \emptyset$, and $\sigma \in CSU_{Ax}^{W'}(t|_p = l)$ for $W' = W \cup Var(l)$ such that $t' = (t[r]_p)\sigma$.*

For convenience, in each narrowing step $t \leadsto_\sigma t'$ we only provide the part of σ that binds variables of t. The transitive closure of $\leadsto$ is denoted by $\leadsto^+$ and the transitive and reflexive closure by $\leadsto^*$. We may write $t \leadsto_\sigma^* t'$ instead of $t \leadsto^* t'$ if there are $s_1, \ldots, s_{k-1}$ and substitutions $\rho_1, \ldots, \rho_k$ such that $t \leadsto_{\rho_1} s_1 \cdots s_{k-1} \leadsto_{\rho_k} t'$, $k \geq 0$, and $\sigma = \rho_1 \cdots \rho_k$. Several notions of completeness of narrowing w.r.t. rewriting have been given in the literature (e.g. [15,16,19]).

Theorem 2 (Completeness of Full Narrowing Modulo [16]). *Let (Σ, Ax, E) be a decomposition of an equational theory. Let t_1 be a term and θ be an E, Ax-normalized substitution. If $t_1\theta \to_{E,Ax}^! t_2$, then there exists a term t_2' and two E, Ax-normalized substitutions θ' and ρ s.t. $t_1 \leadsto_{\theta',E,Ax}^* t_2'$, $\theta|_{Var(t_1)} =_{Ax} (\theta'\rho)|_{Var(t_1)}$, and $t_2 =_{Ax} t_2'\rho$. Furthermore, the rewriting sequence and the narrowing sequence have the same number of steps, with the same rules and at the same positions.*

Narrowing completeness ensures complete generation of all the variants of a term and, thus, an $\mathcal{E}$-unification algorithm: if the term $eq(t, t')$ has a finite set of most general variants, then we are *guaranteed* that the set of most general substitutions *computed* by E, Ax-narrowing is *finite* and provides the set of most general $\mathcal{E}$-unifiers of t and t'. However, can we compute the set of most general $\mathcal{E}$-unifiers of t and t' *effectively*? This is not entirely obvious. Full E, Ax-narrowing may never terminate, since it will compute a complete set of variants of the form (tt, θ) for the term $eq(t, t')$, but that set may easily be infinite, even though a finite set of most general elements for it exists. The solution, of course, is that we should look for adequate narrowing *strategies* that have better properties than full E, Ax-narrowing so that, in the end, we can obtain a *terminating* narrowing-based $\mathcal{E}$-unification *algorithm* to unify t and t' whenever any term $eq(t, t')$ has a finite set of most general variants.

4.1 Narrowing Strategies and Their Properties

In order to provide an appropriate narrowing strategy that enjoys better properties than full E,Ax-narrowing, we need to characterize what a narrowing strategy is and which properties it must satisfy. E.g., the notion of variant–completeness rather than the standard full narrowing completeness becomes essential.

First, we define the notion of a narrowing strategy and several useful properties. Given a narrowing sequence $\alpha : (t_0 \leadsto_{\sigma_0,p_0,R,Ax} t_1 \cdots \leadsto_{\sigma_{n-1},p_{n-1},R,Ax} t_n)$, we denote by α_i the narrowing sequence $\alpha_i : (t_0 \leadsto_{\sigma_0,p_0,R,Ax} t_1 \cdots \leadsto_{\sigma_{i-1},p_{i-1},R,Ax} t_i)$ which is a prefix of α. We denote by $Full_{\mathcal{R}}(t)$ the set of all narrowing sequences starting at term t.

Definition 10 (Narrowing Strategy). *A narrowing strategy $\mathcal{S}$ is a function of two arguments, namely, a rewrite theory $\mathcal{R} = (\Sigma, Ax, R)$ and a term $t \in \mathcal{T}_\Sigma(\mathcal{X})$, which we denote by $\mathcal{S}_{\mathcal{R}}(t)$, such that $\mathcal{S}_{\mathcal{R}}(t) \subseteq Full_{\mathcal{R}}(t)$. We require $\mathcal{S}_{\mathcal{R}}(t)$ to be prefix closed, i.e., for each narrowing sequence $\alpha \in \mathcal{S}_{\mathcal{R}}(t)$, and each $i \in \{1, \ldots, n\}$, we also have $\alpha_i \in \mathcal{S}_{\mathcal{R}}(t)$.*

We say a narrowing strategy $\mathcal{S}$ is *complete* if it satisfies Theorem 2. In this paper we are interested in a notion of completeness of a narrowing strategy slightly different than previous notions, which we call *variant-completeness*. First, we extend the variant semantics to narrowing and consider only narrowing sequences to normalized terms.

Definition 11 (Narrowing Semantics). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$ and $\mathcal{S}$ be a narrowing strategy. We define the set of* narrowing variants *of a term t w.r.t. $\mathcal{S}$ as $[\![t]\!]^{\mathcal{S}}_{E,Ax} = \{(t', \theta) \mid (t \leadsto^*_{\theta,E,Ax} t') \in \mathcal{S}_{\mathcal{R}}(t) \text{ and } t' = t'\!\downarrow_{E,Ax}\}$.*

Now, we can define our notion of variant–completeness.

Definition 12 (Variant Completeness and Minimality). *Let (Σ, Ax, E) be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. A narrowing strategy $\mathcal{S}$ is called $\mathcal{E}$-variant–complete (or just variant–complete) iff for any term t $[\![t]\!]_{E,Ax} \simeq_{E,Ax} [\![t]\!]^{\mathcal{S}}_{E,Ax}$. The narrowing strategy $\mathcal{S}$ is called $\mathcal{E}$-variant–minimal (or just variant–minimal) iff, in addition, we have that for any term t $[\![t]\!]_{E,Ax} \approx_{Ax} [\![t]\!]^{\mathcal{S}}_{E,Ax}$ and for each pair of variants $(t_1, \theta_1), (t_2, \theta_2) \in [\![t]\!]^{\mathcal{S}}_{E,Ax}$ such that $(t_1, \theta_1) \neq_{Ax} (t_2, \theta_2)$, we have that $(t_1, \theta_1) \not\approx_{Ax} (t_2, \theta_2)$.*

This minimality property motivates the following corollary.

Corollary 2. *Let (Σ, Ax, E) be a decomposition of an equational theory $(\Sigma, \mathcal{E})$ and $\mathcal{S}$ be an $\mathcal{E}$-variant-complete narrowing strategy. For any two terms t, t' with the same top sort, the set $S = \{\theta \mid (\mathtt{tt}, \theta) \in [\![\mathtt{eq}(t, t')]\!]^{\mathcal{S}}_{\widehat{E},Ax}\}$ is a complete set of $\mathcal{E}$-unifiers for $t = t'$, where $\widehat{E}$, $\mathtt{eq}$, and $\mathtt{tt}$ are defined as in Proposition 2. If, in addition, $\mathcal{S}$ is a $\mathcal{E}$-variant-minimal narrowing strategy, then the set S is a minimal set of $\mathcal{E}$-unifiers for $t = t'$.*

In practice, the set $\mathcal{S}_\mathcal{R}(t)$ of narrowing sequences from a term t will be generated by an *algorithm* $\mathcal{A}_\mathcal{S}$. That is, $\mathcal{A}_\mathcal{S}$ is a computable function such that, given a pair $(\mathcal{R}, t)$, enumerates the set $\mathcal{S}_\mathcal{R}(t)$. If $\mathcal{E} = (\Sigma, Ax, E)$ is a decomposition of an equational theory, the strategy $\mathcal{S}_\mathcal{E}$ is variant–complete, and $[\![t]\!]_{E,Ax}$ is finite on an input term t, then $[\![t]\!]^\mathcal{S}_{E,Ax}$ may not be finite. Furthermore, even if $[\![t]\!]^\mathcal{S}_{E,Ax}$ is finite, its enumeration using the algorithm $\mathcal{A}_\mathcal{S}$ might not terminate. We are of course interested in variant–complete narrowing strategies that will *always* terminate on an input term t whenever $[\![t]\!]_{E,Ax}$ is finite, since by Corollary 2 such strategies will provide a finitary $\mathcal{E}$-unification algorithm whenever $\mathcal{E}$ has the finite variant property. This leads to the following notion of variant–termination for an algorithm $\mathcal{A}_\mathcal{S}$ restricting the class of algorithms we are interested in.

Definition 13 (Optimal Variant Termination). *Let (Σ, Ax, E) be a decomposition of an equational theory $(\Sigma, \mathcal{E})$ and $\mathcal{S}$ be an $\mathcal{E}$-variant-complete narrowing strategy. An algorithm $\mathcal{A}_\mathcal{S}$ is* variant terminating *iff $\mathcal{A}_\mathcal{S}(\mathcal{E}, t)$ terminates on input $(\mathcal{E}, t)$ iff $[\![t]\!]^\mathcal{S}_{E,Ax}$ is finite. An algorithm $\mathcal{A}_\mathcal{S}$ is* optimally variant terminating *iff $\mathcal{A}_\mathcal{S}$ is variant terminating and $[\![t]\!]^\mathcal{S}_{E,Ax}$ is variant–minimal for every term t.*

By abuse of language, we say that a narrowing strategy $\mathcal{S}$ is variant terminating (resp. optimally variant terminating) whenever $\mathcal{A}_\mathcal{S}$ is. The term "optimally variant terminating" is justified as follows.

Corollary 3. *Let $\mathcal{E} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. Let $\mathcal{S}$ be a $\mathcal{E}$-variant–complete narrowing strategy and $\mathcal{S}'$ be an optimally variant terminating narrowing strategy. Then, for each term t such that $\mathcal{S}_\mathcal{E}(t)$ is finite, then $\mathcal{S}'_\mathcal{E}(t)$ is also finite.*

4.2 Basic Narrowing Modulo is neither Variant–Complete nor Optimally Variant–Terminating

In this section we show that basic narrowing modulo AC is not variant–complete. Furthermore, we show that even basic narrowing without axioms is not optimally variant–terminating, thus motivating that there is room for improvement even in the free case. We extend the standard definition of basic narrowing given in [14] to the modulo case.

Definition 14 (Basic Narrowing modulo Ax). *Let (Σ, Ax, R) be an order-sorted rewrite theory. Given a term $t \in \mathcal{T}_\Sigma(\mathcal{X})$, a substitution ρ, and a set W of variables such that $Var(t) \subseteq W$ and $Var(\rho) \subseteq W$, a basic narrowing modulo Ax step for $\langle t, \rho \rangle$ is defined by $\langle t, \rho \rangle \overset{b}{\rightsquigarrow}_{p,\theta,R,Ax} \langle t', \rho' \rangle$ if there is $p \in Pos_\Sigma(t)$, a rule $l \to r \in R$ properly renamed s.t. $Var(l) \cap W = \emptyset$, and $\theta \in CSU^{W'}_{Ax}(t|_p\rho = l)$ for $W' = W \cup Var(l)$ such that $t' = t[r]_p$, and $\rho' = \rho\theta$.*

Basic narrowing modulo AC is incomplete w.r.t. innermost rewriting modulo AC despite the free case [20], i.e., there are innermost rewriting sequences modulo AC that are not lifted to basic narrowing modulo Ax. And, therefore, basic narrowing modulo AC is not variant–complete.

Example 3. The narrowing sequence shown in Example 1 is not a basic narrowing sequence modulo AC, as after the first step it results in $\langle X, \rho_1 \rangle$ and no further basic narrowing modulo AC step is possible:

$\langle X_1 + X_2, id \rangle \overset{b}{\leadsto}_{\Lambda, \rho_1, E, Ax} \langle X, \rho_1 \rangle$
using $\rho_1 = \{X_1 \mapsto a + X', X_2 \mapsto a + X'', X \mapsto X' + X''\}$ and rule (3)

Therefore, basic narrowing modulo AC is *not variant–complete*, since the pair $(0, \sigma)$ is a variant of t. The (full or unrestricted) narrowing sequence associated to the unification problem $X_1 + X_2 \overset{?}{=} 0$ in the extended equational theory $\widehat{E}$ defined in Proposition 2 is:

$\mathsf{eq}(\underline{X_1 + X_2}, 0) \leadsto_{\rho_1, \widehat{E}, Ax} \mathsf{eq}(X' + X'', 0)$
using $\rho_1 = \{X_1 \mapsto a + X', X_2 \mapsto a + X''\}$ and rule (3)

$\mathsf{eq}(\underline{X' + X''}, 0) \leadsto_{\rho_2, \widehat{E}, Ax} \mathsf{eq}(0, 0)$ using $\rho_2 = \{X' \mapsto b, X'' \mapsto b\}$ and rule (2)

$\underline{\mathsf{eq}(0, 0)} \leadsto_{id, \widehat{E}, Ax} \mathtt{tt}$ using rule $\mathsf{eq}(X, X) \to \mathtt{tt}$

Furthermore, if we add a new equation $0+0+X = 0+X$ basic narrowing modulo AC does not terminate though the number of variants does not change at all, due to the following always available narrowing step $0 + X_2 \leadsto_{\theta_1, E, Ax} 0 + X_2'$ using $\theta_1 = \{X_2 \mapsto 0 + X_2', X \mapsto X_2'\}$.

Moreover, basic narrowing in the free case is not optimally variant–terminating, as shown by the following example.

Example 4. Consider the rewrite theory $\mathcal{R} = (\Sigma, \emptyset, E)$ where E is the set of convergent rules $E = \{f(x) \to x, f(f(x)) \to f(x)\}$ and Σ contains only the unary symbol f and a constant a. The term $t = f(x)$ has only one variant: $[\![f(x)]\!]_{E, Ax} = \{(x, id)\}$. Indeed, the theory has the finite variant property (see [8]). Basic narrowing performs the following two narrowing steps:

(i) $\langle f(x), id \rangle \overset{b}{\leadsto}_{\{x \mapsto x'\}, E} \langle x', \{x \mapsto x'\} \rangle$ and

(ii) $\langle f(x), id \rangle \overset{b}{\leadsto}_{\{x \mapsto f(x')\}, E} \langle f(x'), \{x \mapsto f(x')\} \rangle$.

However, the second narrowing step leads to the following non-terminating basic narrowing sequence:

$\langle f(x), id \rangle \overset{b}{\leadsto}_{\{x \mapsto f(x')\}, E} \langle f(x'), \{x \mapsto f(x')\} \rangle$
$\overset{b}{\leadsto}_{\{x' \mapsto f(x'')\}, E} \langle f(x''), \{x \mapsto f(f(x'')), x' \mapsto f(x'')\} \rangle$
$\dots$

and basic narrowing is unable to terminate and provide the finite number of variants associated to the term t.

In the following section we provide a narrowing strategy to compute the variants of a term that is variant–complete, variant–minimal, and optimally variant–terminating.

4.3 An Optimally Variant–Terminating, and Variant–Minimal Narrowing Strategy for Finite Variant Decompositions

For a finite variant decomposition, we achieve optimal variant termination by simply keeping track of all the variants generated so far, since we know that there is a finite set of more general variants and sooner or later narrowing will generate all the most general variants. We have developed in [7] a way of detecting such repetitions.

Definition 15 (Transition System). *[7] A transition system is written $\mathcal{A} = (A, \rightarrow)$, where A is a set of states, and $\rightarrow$ is a transition relation between states, i.e., $\rightarrow \subseteq A \times A$. We write $\mathcal{A} = (A, \rightarrow, I)$ when $I \subseteq A$ is a set of initial states.*

Intuitively, we define a global strategy that keeps track of previously computed variants and discards narrowing steps that compute a previously met variant.

Definition 16 (Folding Reachable Transition Subsystem [7]). *Given a transition system $\mathcal{A} = (A, \rightarrow, I)$ and a relation $G \subseteq A \times A$, the reachable subsystem from I in A with folding G is written $\mathcal{R}each_{\mathcal{A}}^{G}(I) = (Reach_{\rightarrow}^{G}(I), \rightarrow^{G}, I)$, where $Reach_{\rightarrow}^{G}(I) = \bigcup_{n \in \mathbb{N}} Frontier_{\rightarrow}^{G}(I)_n$ and*

$$Frontier_{\rightarrow}^{G}(I)_0 = I,$$
$$Frontier_{\rightarrow}^{G}(I)_{n+1} = \{y \in A \mid (\exists z \in Frontier_{\rightarrow}^{G}(I)_n : z \rightarrow y) \wedge$$
$$(\nexists k \leq n, w \in Frontier_{\rightarrow}^{G}(I)_k : y \; G \; w)\},$$

$$\rightarrow^{G} = \bigcup_{n \in \mathbb{N}} \rightarrow_{n+1}^{G},$$

$$x \rightarrow_{n+1}^{G} y \begin{cases} \textit{if } x \in Frontier_{\rightarrow}^{G}(I)_n, y \in Frontier_{\rightarrow}^{G}(I)_{n+1}, \\ \quad x \rightarrow y; \\ \textit{if } x \in Frontier_{\rightarrow}^{G}(I)_n, y \notin Frontier_{\rightarrow}^{G}(I)_{n+1}, \\ \quad \exists k \leq n : y \in Frontier_{\rightarrow}^{G}(I)_k, \exists w : (x \rightarrow w \wedge w \; G \; y) \end{cases}$$

Note that, the more general relation G, the greater the chances of $\mathcal{R}each_{\mathcal{A}}^{G}(I)$ being a finite transition system. In [7], we study different relations G such as $\sqsubseteq_{Ax}$ or $\approx_{Ax}$ and its properties. For computing the variants, G is just the preorder $\sqsubseteq_{E,Ax}$ between variants. Given a decomposition (Σ, Ax, E) of an equational theory $(\Sigma, \mathcal{E})$ and a narrowing strategy $\mathcal{S}_{\mathcal{E}}$, we extend $\mathcal{S}_{\mathcal{E}}$ to variants as follows: given a term t and a substitution ρ s.t. $t\rho =_{Ax} t$, $\mathcal{S}_{\mathcal{E}}((t, \rho)) = \{(t, \rho) \rightsquigarrow_{\sigma, E, Ax}^{k} (t', \rho\sigma) \mid (t \rightsquigarrow_{\sigma, E, Ax}^{k} t') \in \mathcal{S}_{\mathcal{E}}(t)\}$. Given a narrowing strategy $\mathcal{S}_{\mathcal{R}}$, we write $\mathcal{S}_{\mathcal{R}}^{1}$ to denote narrowing derivations produced by $\mathcal{S}_{\mathcal{R}}$ of length exactly 1.

Definition 17 (Folding Narrowing Strategy). *Let (Σ, Ax, E) be a decomposition of an equational theory $(\Sigma, \mathcal{E})$ and $\mathcal{S}_{\mathcal{E}}$ a narrowing strategy. Let t be a term. Let us consider the transition system $(\mathcal{T}_{\Sigma}(\mathcal{X}) \times \mathcal{S}ubst(\Sigma, \mathcal{X}), \mathcal{S}_{\mathcal{E}}^{1}, I)$ for variants with the one-step version of the strategy $\mathcal{S}_{\mathcal{E}}$ and the initial state $I = (t, id)$. The folding $\mathcal{S}_{\mathcal{E}}$–narrowing strategy, denoted by $\mathcal{S}_{\mathcal{E}}^{\circlearrowleft}(t)$, is defined as*

$$\mathcal{S}_{\mathcal{E}}^{\circlearrowleft}(t) = \{t \rightsquigarrow_{\sigma, E, Ax}^{k} t' \mid ((t, id) \rightsquigarrow_{\sigma, E, Ax}^{k} (t', \sigma)) \in \mathcal{S}_{\mathcal{E}}(t) \wedge$$
$$(t', \sigma) \in Frontier_{\mathcal{S}_{\mathcal{E}}^{1}}^{\sqsubseteq_{E,Ax}}(I)_k\}$$

We write $Full_{\mathcal{R}}^{\circlearrowleft}$ for the folding version of the full narrowing strategy.

The following example shows that basic narrowing may be non-terminating in cases when variant narrowing does terminate.

Example 5. Considering Example 4 and using the $Full_{\mathcal{R}}^{\circlearrowleft}$ strategy we only get step (i). Step (ii) is subsumed as $(f(x'), \{x \mapsto f(x')\}) \sqsubseteq_{E,\emptyset} (x', \{x \mapsto x'\})$. So even though basic narrowing does not terminate in this case, $Full_{\mathcal{R}}^{\circlearrowleft}$ does.

The following example shows what steps can be done by $Full_{\mathcal{R}}^{\circlearrowleft}$ and termination of it on the given example.

Example 6. Using the theory from Example 2, for $t = X \oplus Y$ we get the following $Full_{\mathcal{R}}^{\circlearrowleft}$ steps. Note that we only need to consider steps with normalized substitutions as otherwise the resulting variant would be subsumed by the variant reachable using the normalized form of the same substitution.

(i) $(t, id) \rightsquigarrow_{\phi_1} (Z, \phi_1)$, with $\phi_1 = \{X \mapsto 0, Y \mapsto Z\}$,
(ii) $(t, id) \rightsquigarrow_{\phi_2} (Z, \phi_2)$, with $\phi_2 = \{X \mapsto Z, Y \mapsto 0\}$,
(iii) $(t, id) \rightsquigarrow_{\phi_3} (Z, \phi_3)$, with $\phi_3 = \{X \mapsto Z \oplus U, Y \mapsto U\}$,
(iv) $(t, id) \rightsquigarrow_{\phi_4} (Z, \phi_4)$, with $\phi_4 = \{X \mapsto U, Y \mapsto Z \oplus U\}$,
(v) $(t, id) \rightsquigarrow_{\phi_5} (0, \phi_5)$, with $\phi_5 = \{X \mapsto U, Y \mapsto U\}$,
(vi) $(t, id) \rightsquigarrow_{\phi_6} (Z_1 \oplus Z_2, \phi_6)$, with $\phi_6 = \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\}$.

There are no further steps possible from (i)-(v) as any instantiation of Z for which a narrowing step is possible would mean that the substitution is not normalized, and 0 is a normal form without variables. For the result of (vi), $(Z_1 \oplus Z_2, \phi_6)$, we are back at the beginning and can repeat all of the steps possible for (t, id), but all of the results are subsumed by the same step we already have from (t, id). So, $Full_{\mathcal{R}}^{\circlearrowleft}$ terminates for t.

Note that by the use of the folding definition we get only the shortest paths to each possible term (depending on the substitution), since the longer paths are simply subsumed by shorter ones using $\sqsubseteq_{E,Ax}$. Any folding narrowing strategy is sound as it is a further restriction of the narrowing strategy. We prove that any folding narrowing strategy is variant–complete provided the given narrowing strategy is complete according to Theorem 2.

Theorem 3 (Variant Completeness of Folding Narrowing). *Let (Σ, Ax, E) be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. Let t_1 be a term and θ be an E,Ax-normalized substitution. Let $\mathcal{S}_{\mathcal{E}}$ be a complete narrowing strategy. If $t_1\theta \rightarrow_{E,Ax}^{!} t_2$ then there exists a term t_2' and two E,Ax-normalized substitutions θ' and ρ s.t. $(t_1 \rightsquigarrow_{\theta',E,Ax}^{*} t_2') \in \mathcal{S}_{\mathcal{E}}^{\circlearrowleft}(t)$, $\theta|_{Var(t_1)} =_{Ax} (\theta'\rho)|_{Var(t_1)}$, and $t_2 =_{Ax} t_2'\rho$.*

The following corollary establishes that folding full-narrowing is an optimally variant–terminating, and variant–minimal narrowing strategy for finite variant decompositions.

Corollary 4. *Let (Σ, Ax, E) be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. The folding full–narrowing $Full_{\mathcal{E}}^{\circlearrowleft}$ is* variant–complete *and* variant–minimal, *i.e., for any term t, $[\![t]\!]_{E,Ax} \approx_{Ax} [\![t]\!]_{E,Ax}^{Full_{\mathcal{E}}^{\circlearrowleft}}$. Moreover, if (Σ, Ax, E) is a finite variant decomposition of $(\Sigma, \mathcal{E})$, then $Full_{\mathcal{E}}^{\circlearrowleft}$ is also optimally variant–terminating.*

5 Conclusions

To the best our knowledge, the general problem of finding effective strategies for narrowing modulo axioms that avoid the hopeless inefficiency of full narrowing and the incompleteness in general of basic narrowing for the modulo case, has remained unsolved up to now. We have presented *folding variant narrowing* as an effective strategy that, by computing exactly and only a mimimal complete set of variants for a term t, is optimally variant terminating, and complete both for unification purposes and for computing variants. Besides yielding in particular a new finitary unification algorithm for FVP equational theories that improves upon the variant algorithm presented in [9], and does not require anymore prior checking of FVP as described in [8], by being applicable to *any* equational theory modulo under minimal assumptions of confluence, termination, and coherence, many more applications than just cryptographic protocol analysis modulo algebraic properties in the style of the Maude-NPA [6] are opened up. In fact, several such applications, to termination methods modulo axioms [5], and to the most recent Maude CRC and ChC tools modulo axioms (see http://maude.lcc.uma.es/CRChC/), are already exploiting the general power of folding variant narrowing.

As always, however, much work remains ahead, particularly in the two closely-related areas of refining and optimizing the folding variant narrowing strategy, and of developing an efficient implementation. There is already an existing implementation in Maude of variant narrowing under the FVP assumption that has been shown effective in formally analyzing a good number of cryptographic protocols modulo a variety of algebraic theories describing their cryptographic infrastructure (see [6] and references there). We expect that a good part of the infrastructure of the current FVP variant narrowing strategy will be easily extensible to an optimized form of the folding variant narrowing strategy; but this will require substantial new work in design, implementation, and experimentation.

References

1. M. Alpuente, S. Escobar, and J. Iborra. Modular termination of basic narrowing. In A. Voronkov, editor, *RTA*, volume 5117 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2008.
2. M. Alpuente, M. Falaschi, and G. Vidal. Partial Evaluation of Functional Logic Programs. *ACM Transactions on Programming Languages and Systems*, 20(4):768–844, 1998.
3. S. Anantharaman, P. Narendran, and M. Rusinowitch. Unification modulo *cui* plus distributivity axioms. *J. Autom. Reasoning*, 33(1):1–28, 2004.
4. H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In J. Giesl, editor, *RTA*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2005.
5. F. Durán, S. Lucas, and J. Meseguer. Termination modulo combinations of equational theories. In *Frontiers of Combining Systems, 7th International Symposium, FroCoS 2009, Trento, Italy, September 16-18, 2009. Proceedings*, volume 5749 of *Lecture Notes in Computer Science*, pages 246–262. Springer, 2009.

6. S. Escobar, C. Meadows, and J. 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.

7. 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.

8. S. Escobar, J. Meseguer, and R. Sasse. Effectively checking the finite variant property. In A. Voronkov, editor, *RTA*, volume 5117 of *Lecture Notes in Computer Science*, pages 79–93. Springer, 2008.

9. S. Escobar, J. Meseguer, and R. Sasse. Variant narrowing and equational unification. In *Electr. Notes Theor. Comput. Sci.*, 238(3):103-119, 2009.

10. S. Escobar, J. Meseguer, and P. Thati. Natural narrowing for general term rewriting systems. In J. Giesl, editor, *RTA*, volume 3467 of *Lecture Notes in Computer Science*, pages 279–293. Springer, 2005.

11. J. Giesl and D. Kapur. Dependency pairs for equational rewriting. In A. Middeldorp, editor, *RTA*, volume 2051 of *Lecture Notes in Computer Science*, pages 93–108. Springer, 2001.

12. J. A. Goguen and J. Meseguer. Equality, types, modules, and (why not ?) generics for logic programming. *J. Log. Program.*, 1(2):179–210, 1984.

13. M. Hanus. The Integration of Functions into Logic Programming: From Theory to Practice. *Journal of Logic Programming*, 19&20:583–628, 1994.

14. S. Hölldobler. *Foundations of Equational Logic Programming*, volume 353 of *Lecture Notes in Artificial Intelligence*. Springer-Verlag, Berlin, 1989.

15. 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.

16. 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.

17. J.-P. Jouannaud and H. Kirchner. Completion of a set of rules modulo a set of equations. *SIAM J. Comput.*, 15(4):1155–1194, 1986.

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

19. 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.

20. A. Middeldorp and E. Hamoen. Completeness results for basic narrowing. *Journal of Applicable Algebra in Engineering, Communication, and Computing*, 5:213–253, 1994.

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

22. P. Y. A. Ryan and S. A. Schneider. An attack on a recursive authentication protocol. a cautionary tale. *Inf. Process. Lett.*, 65(1):7–10, 1998.

23. TeReSe, editor. *Term Rewriting Systems.* Cambridge University Press, Cambridge, 2003.

24. 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.

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