Escobar Román, S.; Sasse, R.; Meseguer, J. (2012). Folding variant narrowing and optimal variant termination. Journal of Logic and Algebraic Programming. 81(7):898-928. doi:10.1016/j.jlap.2012.01.002.

Folding Variant Narrowing and Optimal Variant Termination

Santiago Escobar[a], Ralf Sasse[b], José Meseguer[b]

[a]*DSIC-ELP, Universitat Politècnica de València, Spain*
[b]*Department of Computer Science, University of Illinois at Urbana-Champaign*

Abstract

Automated reasoning modulo an equational theory $\mathcal{E}$ is a fundamental technique in many applications. If $\mathcal{E}$ can be split as a disjoint union $E \cup Ax$ in such a way that E is confluent, terminating, sort-decreasing, and coherent modulo a set of equational axioms Ax, narrowing with E modulo Ax provides a complete $\mathcal{E}$-unification algorithm. However, except for the hopelessly inefficient case of full narrowing, little 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. Narrowing with equations E modulo axioms Ax can be turned into a practical automated reasoning technique by systematically exploiting the notion of E, Ax*-variants* of a term. After reviewing such a notion, originally proposed by Comon-Lundh and Delaune, and giving various necessary and/or sufficient conditions for it, we explain how narrowing strategies can be used to obtain narrowing algorithms modulo axioms that are: (i) *variant-complete* (generate a complete set of variants for any input term), (ii) *minimal* (such a set does not have redundant variants), and (iii) *optimally variant-terminating* (the strategy will terminate for an input term t iff t has a finite complete set of variants). We define a strategy called *folding variant narrowing* that satisfies above properties (i)–(iii); in particular, when $E \cup Ax$ has the *finite variant property*, that is, when any term t has a finite complete set of variants, this strategy terminates on any input term and provides a *finitary* $E \cup Ax$-unification algorithm. We also explain how folding variant narrowing has a number of interesting applications in areas such as unification theory, cryptographic protocol verification, and proofs of termination, confluence and coherence of a set of rewrite rules R modulo an equational theory E.

Keywords: Narrowing modulo, Terminating Narrowing Strategy, Variants, Equational Unification

1. Introduction

Narrowing is a fundamental rewriting technique useful for many purposes, including equational unification and equational theorem proving [32], combinations of functional and logic programming [27, 28, 39], partial evaluation [4], symbolic reachability analysis of rewrite theories understood as transition systems [37], and symbolic model checking [18].

Email addresses: sescobar@dsic.upv.es (Santiago Escobar), rsasse@illinois.edu (Ralf Sasse), meseguer@illinois.edu (José Meseguer)

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 [32]). 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 [32] 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 [32, 3] 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. However, the extensive literature on lazy narrowing strategies [43, 7, 21] is mainly focused on efficient evaluation strategies (efficient in the number of narrowing steps or the generality of computed substitutions to reach a term that cannot be narrowed any more) whereas we are interested in narrowing strategies that are terminating and complete for variant generation. The topic of efficient evaluation strategies is outside the scope of the paper and can be complementary to the narrowing strategies for variant generation developed here. See [6, 30] for references on lazy narrowing strategies. On the other hand, lazy narrowing strategies are demand-driven and we are not aware of demand-driven strategies for the modulo case, or even of a notion of needed (or demanded) evaluation 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 [33], 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. That is because 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., [44].

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 [33, 48], we are not aware of any studies about narrowing strategies in the modulo case. Furthermore, as work in [11, 48] 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. *[11] Consider the equational theory* $(\Sigma, E \cup Ax)$ *where* E *contains the following*

equations and Ax contains associativity[1] *and commutativity (AC) for +:*

$$\begin{array}{lllll} a+a & = & 0 & (1) & a+a+X = X \ (3) \\ b+b & = & 0 & (2) & b+b+X = X \ (4) \end{array} \qquad 0+X = X \quad (5)$$

The set E is terminating, AC-confluent, 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 into basic narrowing sequences (see [38]). That is, given a term t and a (normalized) 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* $t\sigma$*:* $(a + b) + (a + b) \rightarrow_{E,AC} b + b \rightarrow_{E,AC} 0$*. As further explained in Example 6 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* $t\sigma$ *into a more general basic narrowing sequence, 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* (FV) in the sense of [11], we proposed in [20] 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 [19] we gave a method that can be used to check if $E \cup Ax$ is FV. However, FV is a quite strong restriction. What can be done for *any* confluent, terminating and coherent theory modulo axioms Ax?

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, sort-decreasing and coherent modulo Ax, and under minimal requirements on Ax, such as having a finitary Ax-unification algorithm. It turns out that the general notion of *variant*, which makes sense for any such theory $E \cup Ax$ and does not depend on FV, 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. In [22] we proposed such a general and effective strategy, called *folding variant narrowing*, which can be applied to any theory $E \cup Ax$, with E confluent, terminating, sort-decreasing, and coherent modulo Ax, and showed that it is both *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 – and *optimally variant-terminating* – in the sense that it will terminate for an

[1] We use AC operators many times in the paper and we often write terms using AC symbols in its varyadic form, e.g., given an AC symbol +, we write $a + a + X$ or $+(a, a, X)$ instead of $a + (a + X)$, $+(a, +(a, X))$, $(a + X) + a$, or $+(+(a, X), a)$.

input term t if and only if t has a finite, complete set of variants. To the best of our knowledge, folding variant narrowing is the only practical, yet complete, general narrowing strategy modulo a set of axioms Ax; in particular the only such one for the AC case. Furthermore, we showed in [22] that there is no other such complete strategy that can terminate on an input term when folding variant narrowing does not. It transforms the, up to now theoretically possible but practically hopeless, mechanism of narrowing modulo axioms Ax into a practically usable automated deduction method, which has already been exploited in a wide range of applications as explained in Section 9.

This paper extends and unifies within a common theoretical framework our earlier contributions in [20, 19, 22]. Our goal is to provide the most complete and accessible reference to this general body of ideas by developing in detail its mathematical foundations and its fundamental algorithms. The plan of the paper, and its main contributions, can be summarized as follows:

1. Comon-Lundh and Delaune's notion of *variant* [11] is the fundamental notion underlying the entire approach. After some preliminaries in Section 2, in Section 3 we further refine this notion by formalizing the E, Ax-variants of a term t as *pairs* (t', θ), with θ a substitution and t' an E, Ax-canonical form for $t\theta$, and making explicit the preorder relation of generalization that holds between such pairs and the corresponding notion of most general variants in such a preorder.
2. We then give, in Section 4, general notions of narrowing strategy and precise definitions of what it means for a strategy to be: (i) *variant complete*, i.e., it computes a complete set of variants (and possibly also *minimal*, in the sense of the preorder relation of generalization explained above), and (ii) *optimally variant-terminating*, i.e., it will terminate iff there is a finite complete set of variants. Note that we are not interested in efficient narrowing evaluation strategies (as widely studied in the literature of narrowing) and not even on the standard completeness results for narrowing strategies, so we define variant completeness and variant termination notions. These are the essential requirements that will guide us in the search for the desired strategy. To illustrate how tight these essential requirements are, so that none of the known strategies satisfy them, we show that basic narrowing, *both* in the free case ($Ax = \emptyset$) and in the AC case, fails to satisfy properties (i) and/or (ii).
3. A key contribution is the *parametric* notion of *folding narrowing* of Section 5. The essential idea is to associate to any narrowing strategy $\mathcal{S}$ a corresponding "folding" version of it. That is, $\mathcal{S}$ is a local strategy, i.e., in the sense of which narrowing steps are allowed from a term, whereas $\mathcal{S}^{\circlearrowleft}$ is a global strategy, i.e., in the sense of tracking variants and avoiding repeated generation of variants. We prove that for any complete strategy $\mathcal{S}$, its folding version $\mathcal{S}^{\circlearrowleft}$ is always variant complete, which is property (i) in (2) above. The presentation of folding narrowing in [22] has been improved in this paper.
4. What about minimality, and about the termination property (ii) in (2)? Another key contribution is the *variant narrowing strategy* (VN), which takes into account properties of confluence, termination and coherence of the rules E modulo the axioms Ax to restrict the narrowing steps from each term. We prove that VN is variant complete. However, although VN is not variant-terminating, we show that its folding version $VN^{\circlearrowleft}$ is variant complete and optimally variant-terminating, thus variant minimal. The variant narrowing of [20] has been completely redesigned in this paper.
5. Although all the above results hold for any theory $E \cup Ax$ with E confluent, terminating, sort-decreasing, and coherent modulo Ax, the case when $E \cup Ax$ has the *finite variant property* (FV) in the sense of [11], that is, when any term t has a finite, complete set

of variants, is of particular interest, since then the folding variant narrowing strategy is guaranteed to terminate and to compute a complete and minimal set of variants for *any* input term t. This case is studied in detail in Section 6. In particular, we study a number of sufficient and/or necessary conditions for $E \cup Ax$ to enjoy FV.

6. A related practical question is: given $E \cup Ax$, how can we check whether it has the finite variant property? Under appropriate assumptions on $E \cup Ax$, we give an algorithm in Section 7 that can be used to check FV. The key idea is to view FV as a generalized termination property. Our algorithm extends and adapts to the variant generation case ideas from the dependency pairs method, which is a well-known technique for proving termination of rewriting (modulo axioms). Note that we do not really extend the dependency pairs technique to narrowing and we simply reuse the dependency pairs technique to approximate that there are no infinite variant-preserving narrowing sequences. The same methods can also be used for *disproving* FV for a given theory $E \cup Ax$. The algorithm of [19] has been improved in this paper, since we were computing bounds for the depth of the narrowing tree in [19] that are not necessary in this paper.
7. Section 8 studies in detail one key application of folding variant narrowing, namely, to provide a *finitary* unification algorithm when $E \cup Ax$ enjoys FV. This is very useful for many applications, for example in the analysis of cryptographic protocols. Also, in practice, if $E \cup Ax$ and $E' \cup Ax'$ both enjoy FV, their union $E \cup E' \cup Ax \cup Ax'$ is often FV, either because of disjointness, or because it is quite easy to show it by checking the required conditions. That is, variant-based unification is a quite modular approach, although we do not discuss modularity issues in this paper.
8. Section 9 discusses a number of applications of folding variant narrowing and of variant-based unification, including: (i) cryptographic protocol verification modulo equational properties; (ii) proof techniques for termination of rewriting modulo axioms; and (iii) proof techniques for proving confluence and coherence of rewrite rules modulo axioms. Finally, Section 10 presents some concluding remarks.

2. Preliminaries

We follow the classical notation and terminology from [46] for term rewriting, and from [35] for rewriting logic and order-sorted notions. We assume an order-sorted signature $\mathbf{\Sigma} = (\mathsf{S}, \leq, \Sigma)$ with poset of sorts $(\mathsf{S}, \leq)$ and such that for each sort $\mathsf{s} \in \mathsf{S}$ the connected component of s in $(\mathsf{S}, \leq)$ has a top sort, denoted $[\mathsf{s}]$, and all $f : \mathsf{s}_1 \cdots \mathsf{s}_n \to \mathsf{s}$ with $n \geq 1$ have a top sort overloading $f : [\mathsf{s}_1] \cdots [\mathsf{s}_n] \to [\mathsf{s}]$. 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, $Var(t)$ denotes the set of all variables in t.

Positions are represented by sequences of natural numbers denoting an access path in the term when viewed as a tree. The top or root position is denoted by the empty sequence $\wedge$. We define the relation $p \leq q$ between positions as $p \leq p$ for any p; and $p \leq p.q$ for any p and q. Given $U \subseteq \Sigma \cup \mathcal{X}$, $Pos_U(t)$ denotes the set of positions of a term t that are rooted by symbols or variables in U. The set of positions of a term t is written $Pos(t)$, and the set of non-variable positions $Pos_\Sigma(t)$. 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 $\mathcal{X}$ to $\mathcal{T}_\Sigma(\mathcal{X})$. Substitutions are written as $\sigma = \{X_1 \mapsto t_1, \ldots, X_n \mapsto t_n\}$ where the domain of σ is $Dom(\sigma) =$

$\{X_1, \ldots, X_n\}$ and the set of variables introduced by terms $t_1, \ldots, t_n$ is written $Ran(\sigma)$. 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., σ satisfies $Dom(\sigma) \cap Ran(\sigma) = \emptyset$. 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 $\sigma\sigma'$. Combination of two substitutions is denoted by $\sigma \cup \sigma'$. We call an idempotent substitution σ a variable *renaming* if there is another idempotent substitution σ^{-1} such that $(\sigma\sigma^{-1})|_{Dom(\sigma)} = id$.

A Σ-*equation* is an unoriented pair $t = t'$, where $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ for some sort $\mathsf{s} \in \mathsf{S}$. Given Σ and a set $\mathcal{E}$ of Σ-equations, order-sorted equational logic induces a congruence relation $=_\mathcal{E}$ on terms $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ (see [36]). Throughout this paper we assume that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s, because this affords a simpler deduction system. 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 just $\sqsubseteq$ 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 $t\theta =_\mathcal{E} t'$. We write $t \sqsubset_\mathcal{E} t'$ if $t \sqsubseteq_\mathcal{E} t'$ and $t \not\approx_\mathcal{E} t'$. Relations $\approx_\mathcal{E}$ and $\sqsubset_\mathcal{E}$ are extended to substitutions in a similar way. 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 $(\sigma\eta)|_V =_\mathcal{E} \rho|_V$. We write $\sigma \sqsubset_\mathcal{E} \sigma'$ if $\sigma \sqsubseteq_\mathcal{E} \sigma'$ and $\sigma \not\approx_\mathcal{E} \sigma'$.

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 $CSU^W_\mathcal{E}(t = t')$ is said to be a *complete* set of unifiers for the equation $t = t'$ modulo $\mathcal{E}$ away from W iff: (i) each $\sigma \in CSU^W_\mathcal{E}(t = t')$ is an $\mathcal{E}$-unifier of $t = t'$; (ii) for any $\mathcal{E}$-unifier ρ of $t = t'$ there is a $\sigma \in CSU^W_\mathcal{E}(t = t')$ such that $\rho|_W \sqsubseteq_\mathcal{E} \sigma|_W$; (iii) for all $\sigma \in CSU^W_\mathcal{E}(t = t')$, $Dom(\sigma) \subseteq (Var(t) \cup Var(t'))$ and $Ran(\sigma) \cap W = \emptyset$. If the set of variables W is irrelevant or is understood from the context, we write $CSU_\mathcal{E}(t = t')$ instead of $CSU^W_\mathcal{E}(t = t')$. 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, i.e., for any two unifiers $\rho_1, \rho_2 \in CSU^W_\mathcal{E}(t = t')$ such that $\rho_1|_W \neq_\mathcal{E} \rho_2|_W$, we have that $\rho_1|_W \not\sqsubseteq_\mathcal{E} \rho_2|_W$ and $\rho_2|_W \not\sqsubseteq_\mathcal{E} \rho_1|_W$.

A *rewrite rule* is an oriented pair $l \to r$, where $Var(r) \subseteq Var(l)$ 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 (resp. transitive and reflexive) closure of $\to_{R/Ax}$ is denoted $\to^+_{R/Ax}$ (resp. $\to^*_{R/Ax}$). 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 a rewrite rule $l \to r$, we say that it is *sort-decreasing* if for each substitution σ, we have $r\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ implies $l\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$. We say a rewrite theory (Σ, Ax, R) is sort-decreasing if all rules in R are. For a Σ-equation $t = t'$, we say that it is *regular* if $Var(t) = Var(t')$, and it is *sort-preserving* if for each substitution σ, we have $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ implies $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ and vice

versa. We say an equational theory $(\Sigma, \mathcal{E})$ is regular or sort-preserving if all equations in $\mathcal{E}$ are.

For substitutions σ, ρ and a set of variables V we define $\sigma|_V \rightarrow_{R/Ax} \rho|_V$ if there is $x \in V$ such that $x\sigma \rightarrow_{R/Ax} x\rho$ 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 $\rightarrow_{R/Ax}$ is *terminating* if there is no infinite sequence $t_1 \rightarrow_{R/Ax} t_2 \rightarrow_{R/Ax} \cdots t_n \rightarrow_{R/Ax} t_{n+1} \cdots$. We say that the relation $\rightarrow_{R/Ax}$ is *confluent* if whenever $t \rightarrow^*_{R/Ax} t'$ and $t \rightarrow^*_{R/Ax} t''$, there exists a term t''' such that $t' \rightarrow^*_{R/Ax} t'''$ and $t'' \rightarrow^*_{R/Ax} t'''$. An order-sorted rewrite theory (Σ, Ax, R) is confluent (resp. terminating) if the relation $\rightarrow_{R/Ax}$ is confluent (resp. terminating). In a confluent, terminating, sort-decreasing, 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 $t \rightarrow^!_{R/Ax} t'$, 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 [33] by R, Ax-rewriting. We assume the following properties on R and Ax:

1. Ax is regular and sort-preserving; furthermore, for each equation $t = t'$ in Ax, all variables in $Var(t)$ have a top sort.
2. Ax has a finitary and complete unification algorithm.
3. The rewrite rules R are sort-decreasing, confluent, and terminating.

Definition 1 (Rewriting modulo). [49] *Let (Σ, Ax, R) be an order-sorted rewrite theory satisfying properties* (1)–(3)*. 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 non-variable position $p \in Pos_\Sigma(t)$, a rule $l \rightarrow r$ in R, and a 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 sort-decreasing, confluent, and terminating, i.e., the relation $\rightarrow_{R/Ax}$ is confluent and terminating, and $\rightarrow_{R,Ax} \subseteq \rightarrow_{R/Ax}$, 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 in general. 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 [24, 49, 34] for coherence completion algorithms.

4. $\rightarrow_{R,Ax}$ is Ax-*coherent* [33], 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 $t_4 =_{Ax} t_5$. See Figure 1 for a graphical illustration.

Let us explain in detail the practical meaning of Ax-coherence, at least for the common associative-commutative (AC) case. The best way to illustrate it is by its *absence*. Consider Example 1 where symbol $\_+\_$ is declared AC. Now consider the equation $b+b = 0$. This equation, if not completed by another equation, is *not* coherent modulo AC. What this means is that there will be term *contexts* in which the equation *should* be applied, but it cannot be applied. Consider, for example, the term $b + (a + b)$. Intuitively, we should be able to apply to it the above equation to simplify it to the term $a + 0$ in one step. However, since we are using the weaker rewrite relation $\rightarrow_{E,Ax}$ instead of the stronger but much harder to implement relation $\rightarrow_{E/Ax}$, we cannot! The problem is that the equation cannot be applied (even if we match modulo AC) to either the

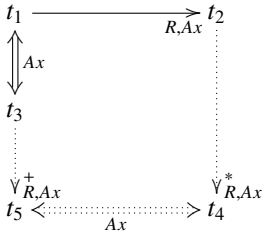


Figure 1: Ax-coherence

top term $b + (a + b)$ or the subterm $a + b$. We can however make our equation *coherent* modulo AC by adding the extra equation $b + b + Y = 0 + Y$, which, using also the equation $X + 0 = X$, we can slightly simplify to the equation $b + b + Y = Y$. This extended version of our equation will now apply to the term $b + (a + b)$, giving the simplification $b + (a + b) \longrightarrow_{E,Ax} a$. Technically, what coherence means is that the weaker relation $\rightarrow_{E,Ax}$ becomes semantically equivalent to the stronger relation $\rightarrow_{E/Ax}$.

Coherence can be handled implicitly or explicitly, i.e., either the matching mechanism is modified to take care of this issue or the rules are explicitly extended, which is the option shown above; see [47] for a comparison between implicit and explicit extensions. For rewriting, implicit extensions are sufficient in many cases, as the implicit Ax-coherence completion provided by the Maude tool [10] for any combination of associativity (A), commutativity (C), and identity (U) axioms. For narrowing, implicit extension is more complicated and it is sufficient in common cases such as combinations of C, AC, and ACU axioms to consider explicit single-variable extensions, i.e., given an equation $s = t$ one considers $s + x = t + x$ where x is a new variable. The method is as follows for AC. For any symbol f which is AC, and for any equation of the form $f(u, v) = w$ in E, we add also the equation $f(f(u, v), X) = f(w, X)$, where X is a new variable not appearing in u, v, w. In an order-sorted setting, we should give to X *the biggest sort possible*, so that it will apply in all generality. As an additional optimization, note that some equations may already be coherent modulo AC, so that we need not add the extra equation. For example, if the variable X has the biggest possible sort it could have, then the equation $X + 0 = X$ of Example 1 is already coherent, since X will match "the rest of the +-expression," regardless of how big or complex that expression might be, and of where in the expression a constant 0 occurs.

The following theorem in [33, Proposition 1] that generalizes ideas in [42] and has an easy extension to order-sorted theories, links $\rightarrow_{R/Ax}$ with $\rightarrow_{R,Ax}$.

Theorem 1 (Correspondence). [42, 33] *Let* (Σ, Ax, R) *be an order-sorted rewrite theory satisfying properties* (1)–(4). *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). [20] *Let* $(\Sigma, \mathcal{E})$ *be an order-sorted equational theory. We call* (Σ, Ax, E) *a* decomposition *of* $(\Sigma, \mathcal{E})$ *if* $\mathcal{E} = E \cup Ax$ *and* (Σ, Ax, E) *is an order-sorted rewrite theory satisfying properties* (1)–(4) *above.*

Note that we abuse notation and call (Σ, Ax, E) a decomposition of an order-sorted equational theory $(\Sigma, \mathcal{E})$ even if $\mathcal{E} \neq E \cup Ax$ but E is the explicitly extended Ax-coherent version of a set E' such that $\mathcal{E} = E' \cup Ax$.

3. Variants

Given an equational theory $\mathcal{E}$, *the $\mathcal{E}$-variants* of a term t are pairs (t', θ) such that $t\theta =_{\mathcal{E}} t'$. This notion can be very useful for reasoning about t modulo $\mathcal{E}$, e.g., unification modulo $\mathcal{E}$ of two terms t and t' can be understood as an appropriate intersection of sets of $\mathcal{E}$-variants for t and t' (as shown in Section 8).

Definition 3 (Variants). [11] *Given a term t and an order-sorted equational theory $(\Sigma, \mathcal{E})$, we say that (t', θ) is an* $\mathcal{E}$-variant *of t if $t\theta =_{\mathcal{E}} t'$, where $Dom(\theta) \subseteq Var(t)$ and $Ran(\theta) \cap Var(t) = \emptyset$.*

Example 2. *Let us consider the following equational theory for both the exclusive-or operator and the cancellation equations for public encryption and decryption. The exclusive-or symbol is $\oplus$ and the symbols pk and sk are used for public and private key encryption, respectively. This equational theory is useful for protocol verification (see [37]) and it is relevant here because there are no unification procedures available in the literature which are directly applicable to it, e.g., unification algorithms for exclusive-or such as [5] do not directly apply when extra equations are added.*

$$\begin{array}{rclcrclcrcl} X \oplus Y & = & Y \oplus X & & X \oplus 0 & = & X & & pk(K, sk(K, M)) & = & M \\ X \oplus (Y \oplus Z) & = & (X \oplus Y) \oplus Z & & X \oplus X & = & 0 & & sk(K, pk(K, M)) & = & M \end{array}$$

Given the term $M \oplus M$, we have that: (i) $(0, id)$, (ii) $(0, \{M \mapsto pk(K, sk(K, M'))\})$, and (iii) $(0, \{M \mapsto M' \oplus M' \oplus M''\})$ are some of its variants. Given the term $X \oplus Y$, we have that: (i) $(X \oplus Y, id)$, (ii) $(0, \{X \mapsto U, Y \mapsto U\})$, (iii) $(Z, \{X \mapsto 0, Y \mapsto Z\})$, and (iv) $(Z, \{X \mapsto Z, Y \mapsto 0\})$ are some of its variants.

Suppose that a rewrite theory (Σ, Ax, E) is a decomposition of $(\Sigma, \mathcal{E})$. Given a term t, we can obtain a tighter notion of variant of t (also called an *E,Ax-variant* of t) as a pair (t', θ) with t' an E,Ax-canonical form of the term $t\theta$. That is, the variants of a term now give us all the irreducible *patterns* that instances of t can reduce to.

Definition 4 (Complete set of variants). [11] *Let (Σ, Ax, E) be a decomposition of an order-sorted equational theory $(\Sigma, \mathcal{E})$. A* complete set of E, Ax-variants *(up to renaming) of a term t is a subset V of $\mathcal{E}$-variants of t such that, for each substitution σ, there is a variant $(t', \theta) \in V$ and a substitution ρ such that: (i) t' is E, Ax-irreducible, (ii) $(t\sigma)\downarrow_{E,Ax} =_{Ax} t'\rho$, and (iii) $(\sigma\downarrow_{E,Ax})|_{Var(t)} =_{Ax} (\theta\rho)|_{Var(t)}$.*

Example 3. *The equational theory $(\Sigma, \mathcal{E})$ of Example 2 has a decomposition into E consisting of the oriented equations below, and Ax the associativity and commutativity (AC) axioms for $\oplus$:*

$$\begin{array}{rclcl} X \oplus 0 & = & X & & (6) \\ X \oplus X & = & 0 & & (7) \\ X \oplus X \oplus Y & = & Y & & (8) \\ pk(K, sk(K, M)) & = & M & & (9) \\ sk(K, pk(K, M)) & = & M & & (10) \end{array}$$

Note that equations (6)–(7) are not AC-coherent, but adding equation (8) is sufficient to recover that property (see [49, 15]). For term $t = M \oplus M$, the set $\{(0, id)\}$ provides a complete set of E, Ax-variants, since any possible variant of t is an instance of $(0, id)$.

The following characterization of variants in terms of a variant semantics for decompositions is useful in various applications discussed later in the paper.

Definition 5 (Variant Semantics). *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$ *and* t *be a* Σ*-term. We define the set of (normalized)* E, Ax*-variants of* t *as*

$$[\![t]\!]^{\star}_{E,Ax} = \{(t', \theta) \mid \theta \in \mathcal{S}ubst(\Sigma, \mathcal{X}), t\theta \rightarrow^{!}_{E,Ax} t'', \text{ and } t'' =_{Ax} t'\}.$$

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. 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 θ, the less E,Ax rewrite steps, the better.

Definition 6 (Variant Preordering). *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$ *and* t *be a* Σ*-term. Given two variants* $(t_1, \theta_1), (t_2, \theta_2) \in [\![t]\!]^{\star}_{E,Ax}$*, 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* $(\theta_1{\downarrow_{E,Ax}})|_{Var(t)} =_{Ax} (\theta_2\rho)|_{Var(t)}$*. We write* $(t_1, \theta_1) \sqsubset_{E,Ax} (t_2, \theta_2)$ *iff* $(t_1, \theta_1) \sqsubseteq_{E,Ax} (t_2, \theta_2)$ *and for every substitution* ρ *such that* $t_1 =_{Ax} t_2\rho$ *and* $(\theta_1{\downarrow_{E,Ax}})|_{Var(t)} =_{Ax} (\theta_2\rho)|_{Var(t)}$*,* ρ *is not a renaming.*

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

Definition 7 (Variant Equality). *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$ *and* t *be a* Σ*-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, we write $(t_1, \theta_1) =_{Ax} (t_2, \theta_2)$ to denote that $t_1 =_{Ax} t_2$ and $\theta_1 =_{Ax} \theta_2$, and we provide a notion of equality of variants up to renaming. Both relations $=_{Ax}$ and $\approx_{Ax}$ will be useful.

Definition 8 (Ax-Equality). *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$ *and* t *be a* Σ*-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* $(\theta_1\rho)|_{Var(t)} =_{Ax} (\theta_2\rho)|_{Var(t)}$*. 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 6 allows us to define a most general and complete set of variants that encompasses (modulo Ax and modulo renaming) all the variants for a term t.

Definition 9 (Most General and Complete Variant Semantics). *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$ *and* t *be a* Σ*-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* $(t_2, \theta_2) \in [\![t]\!]_{E,Ax} \setminus \{(t_1, \theta_1)\}$ *s.t.* $(t_1, \theta_1) \sqsubseteq_{E,Ax} (t_2, \theta_2)$*.*

For any term t, $[\![t]\!]_{E,Ax}$ characterizes the set of *maximal elements* of the preorder $([\![t]\!]^{\star}_{E,Ax}, \sqsubseteq_{E,Ax})$. The set $[\![t]\!]_{E,Ax}$ is unique up to $\approx_{Ax}$-equivalence. By definition, $[\![t]\!]_{E,Ax} \subset [\![t]\!]^{\star}_{E,Ax}$ and all the substitutions in $[\![t]\!]_{E,Ax}$ are E,Ax-normalized.

Example 4. *In the equational theory of Example 3, for terms* $t = M \oplus sk(K, pk(K, M))$ *and* $s = X \oplus sk(K, pk(K, Y))$*, we have that* $[\![t]\!]_{E,Ax} = \{(0, id)\}$ *and*

$$
\begin{array}{lll}
[\![s]\!]_{E,Ax} = \{ & (X \oplus Y, id), & \\
& (Z, \{X \mapsto 0, Y \mapsto Z\}), & (Z, \{X \mapsto Z, Y \mapsto 0\}), \\
& (Z, \{X \mapsto Z \oplus U, Y \mapsto U\}), & (Z, \{X \mapsto U, Y \mapsto Z \oplus U\}), \\
& (0, \{X \mapsto U, Y \mapsto U\}), & (Z_1 \oplus Z_2, \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\})\}
\end{array}
$$

These two sets are the most general ones w.r.t. $\sqsubseteq_{E,Ax}$.

In the next section, we study how to compute the variants of a term.

4. Narrowing Strategies and Optimal Variant Termination

In this section, we introduce narrowing, narrowing strategies and their use for variant generation. As already mentioned, we are not interested in optimal evaluation narrowing strategies [6, 30], which is an extensive topic in the literature on functional logic programming, and not even on the standard completeness results for narrowing strategies. We are interested in narrowing strategies that are terminating and complete for computing variants. A comparison of the *folding variant narrowing strategy*, defined in this paper, with the related literature on optimal evaluation narrowing strategies is outside the scope of this paper.

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 10 (Narrowing modulo). [33, 37] *Let* $\mathcal{R} = (\Sigma, Ax, R)$ *be an order-sorted rewrite theory. Let* $CSU_{Ax}(u = u')$ *be a finite and complete set of* Ax*-unifiers for any pair of terms* u, u' *with the same top sort. Let* t *be a* Σ*-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* $t \rightsquigarrow_{p,\sigma,R,Ax} t'$ *(*$\rightsquigarrow_{\sigma,R,Ax}$ *if* p *is understood,* $\rightsquigarrow_\sigma$ *if* R, Ax *are also understood, and* $\rightsquigarrow$ *if* σ *is also understood) if there is a non-variable position* $p \in Pos_\Sigma(t)$*, a rule* $l \to r \in R$ *properly renamed s.t.* $Var(l) \cap W = \emptyset$*, and a unifier* $\sigma \in CSU_{Ax}^{W'}(t|_p = l)$ *for* $W' = W \cup Var(l)$*, such that* $t' = (t[r]_p)\sigma$.

For convenience, in each narrowing step $t \rightsquigarrow_\sigma t'$ we only specify the part of σ that binds variables of t. The transitive (resp. transitive and reflexive) closure of $\rightsquigarrow$ is denoted by $\rightsquigarrow^+$ (resp. $\rightsquigarrow^*$). We may write $t \rightsquigarrow_\sigma^k t'$ if there are $u_1, \ldots, u_{k-1}$ and substitutions $\rho_1, \ldots, \rho_k$ such that $t \rightsquigarrow_{\rho_1} u_1 \cdots u_{k-1} \rightsquigarrow_{\rho_k} t'$, $k \geq 0$, and $\sigma = \rho_1 \cdots \rho_k$.

Example 5. *Consider Example 3. Given the term* $t = X \oplus Y$*, there are several narrowing steps that can be performed*

$X \oplus Y \rightsquigarrow_{\phi_1,E,Ax} Z$ *using* $\phi_1 = \{X \mapsto 0, Y \mapsto Z\}$ *and Equation* (6)
$X \oplus Y \rightsquigarrow_{\phi_2,E,Ax} Z$ *using* $\phi_2 = \{X \mapsto Z, Y \mapsto 0\}$ *and Equation* (6)
$X \oplus Y \rightsquigarrow_{\phi_3,E,Ax} Z$ *using* $\phi_3 = \{X \mapsto Z \oplus U, Y \mapsto U\}$ *and Equation* (8)
$X \oplus Y \rightsquigarrow_{\phi_4,E,Ax} Z$ *using* $\phi_4 = \{X \mapsto U, Y \mapsto Z \oplus U\}$ *and Equation* (8)
$X \oplus Y \rightsquigarrow_{\phi_5,E,Ax} 0$ *using* $\phi_5 = \{X \mapsto U, Y \mapsto U\}$ *and Equation* (7)
$X \oplus Y \rightsquigarrow_{\phi_6,E,Ax} Z_1 \oplus Z_2$ *using* $\phi_6 = \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\}$ *and Equation* (8)

And some redundant narrowing steps with non-normalized substitutions due to the prolific AC-unification such as

$$X \oplus Y \rightsquigarrow_{\phi_7,E,Ax} Z_1 \oplus Z_2 \quad \textit{using } \phi_7 = \{X \mapsto Z_1 \oplus 0, Y \mapsto Z_2\} \textit{ and Equation } (6)$$
$$X \oplus Y \rightsquigarrow_{\phi_8,E,Ax} Z_1 \oplus Z_2 \quad \textit{using } \phi_8 = \{X \mapsto Z_1, Y \mapsto 0 \oplus Z_2\} \textit{ and Equation } (6)$$
$$X \oplus Y \rightsquigarrow_{\phi_9,E,Ax} Z \quad \textit{using } \phi_9 = \{X \mapsto U \oplus U, Y \mapsto Z\} \textit{ and Equation } (8)$$
$$X \oplus Y \rightsquigarrow_{\phi_{10},E,Ax} Z \quad \textit{using } \phi_{10} = \{X \mapsto Z, Y \mapsto U \oplus U\} \textit{ and Equation } (8)$$
$$X \oplus Y \rightsquigarrow_{\phi_{11},E,Ax} Z_1 \oplus Z_2 \quad \textit{using } \phi_{11} = \{X \mapsto U \oplus U \oplus Z_1, Y \mapsto Z_2\} \textit{ and Equation } (8)$$
$$X \oplus Y \rightsquigarrow_{\phi_{12},E,Ax} Z_1 \oplus Z_2 \quad \textit{using } \phi_{12} = \{X \mapsto Z_1, Y \mapsto U \oplus U \oplus Z_2\} \textit{ and Equation } (8)$$

Indeed, the narrowing `search` *command of Maude [9] computes* 124 *different narrowing steps from term t. When we consider narrowing sequences instead of single steps, we can easily get a combinatorial explosion, since after any of the narrowing steps:* $X \oplus Y \rightsquigarrow_{\phi_6,E,Ax} Z_1 \oplus Z_2$, $X \oplus Y \rightsquigarrow_{\phi_8,E,Ax} Z_1 \oplus Z_2$, *or* $X \oplus Y \rightsquigarrow_{\phi_{11},E,Ax} Z_1 \oplus Z_2$, *we have another* 124 *different narrowing steps. Also, there are clearly many infinite narrowing sequences, such as the one repeating substitution* ϕ_6 *again and again:* $X \oplus Y \rightsquigarrow_{\phi_6,E,Ax} Z_1 \oplus Z_2 \rightsquigarrow_{\phi'_6,E,Ax} Z'_1 \oplus Z'_2 \rightsquigarrow_{\phi''_6,E,Ax} Z''_1 \oplus Z''_2 \rightsquigarrow_{E,Ax} \cdots$ *where* $\phi'_6 = \{Z_1 \mapsto U' \oplus Z'_1, Z_2 \mapsto U' \oplus Z'_2\}$ *and* $\phi''_6 = \{Z'_1 \mapsto U'' \oplus Z''_1, Z'_2 \mapsto U'' \oplus Z''_2\}$. *Clearly, strategies that dramatically reduce this search space, yet are complete, are surely needed.*

4.1. Completeness of Narrowing w.r.t. Rewriting

Several notions of completeness of narrowing w.r.t. rewriting have been given in the literature (e.g., [32, 33, 37]).

Theorem 2 (Completeness of Full Narrowing Modulo). [33] *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$. *Let* t_1 *be a* Σ*-term and* σ *be an* E,Ax*-normalized substitution. If* $t_1\sigma \rightarrow_{E,Ax} t_2 \rightarrow_{E,Ax} \cdots \rightarrow_{E,Ax} t_n$ *such that* $t_n = (t_1\sigma)\downarrow_{E,Ax}$, *then there exist terms* $t'_2, \ldots, t'_n$ *and* E,Ax*-normalized substitutions* $\theta_1, \ldots, \theta_n$ *and* ρ *s.t.* $t_1 \rightsquigarrow_{\theta_1,E,Ax} t'_2 \rightsquigarrow_{\theta_2,E,Ax} \cdots \rightsquigarrow_{\theta_n,E,Ax} t'_n$, $\sigma|_{Var(t_1)} =_{Ax} (\theta_1 \cdots \theta_n\rho)|_{Var(t_1)}$, *and* $t_i =_{Ax} t'_i\rho$ *for* $1 \leq i \leq n$.

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

Lemma 1 (Completeness). *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$. *Let* t_1 *be a* Σ*-term and* θ *be any substitution. If* $t_1\theta \rightarrow^{!}_{E,Ax} t_2$, *then there exists a term* t'_2 *and two* E, Ax*-normalized substitutions* σ *and* ρ *s.t.* $t_1 \rightsquigarrow^{*}_{\sigma,E,Ax} t'_2$, $(\theta\downarrow_{E,Ax})|_{Var(t_1)} =_{Ax} (\sigma\rho)|_{Var(t_1)}$, *and* $t_2 =_{Ax} t'_2\rho$.

Proof. *Let* $\bar{\theta} = \theta\downarrow_{E,Ax}$. *By coherence, confluence and termination of* $\rightarrow_{E,Ax}$, $t_1\theta \rightarrow^{!}_{E,Ax} t_2$ *implies* $\exists t_3 : t_1\bar{\theta} \rightarrow^{!}_{E,Ax} t_3$ *and* $t_3 =_{Ax} t_2$. *By Theorem 2, there exists a term* t'_3 *and two* E, Ax*-normalized substitutions* σ *and* ρ *s.t.* $t_1 \rightsquigarrow^{*}_{\sigma,R,E} t'_3$, $\bar{\theta}|_{Var(t_1)} =_{Ax} (\sigma\rho)|_{Var(t_1)}$, *and* $t_3 =_{Ax} t'_3\rho$. □

As a direct consequence of Lemma 1 we obtain the following result.

Corollary 1 (Complete Variant Semantics by Full Narrowing). *Let* (Σ, Ax, E) *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$. *Then for each term t, the set*

$$[\![t]\!]^{Full}_{E,Ax} = \{(t', \theta) \mid t \rightsquigarrow^{*}_{\theta,E,Ax} t' \wedge t' = t'\downarrow_{E,Ax}\}$$

is a complete set of variants, i.e., $[\![t]\!]^{\star}_{E,Ax} \sqsubseteq_{E,Ax} [\![t]\!]^{Full}_{E,Ax}$.

Note that, although $[\![t]\!]^{\star}_{E,Ax} \sqsubseteq_{E,Ax} [\![t]\!]^{Full}_{E,Ax}$, not all $(t', \theta) \in [\![t]\!]^{Full}_{E,Ax}$ need to be most general, i.e., $[\![t]\!]^{Full}_{E,Ax}$ is not necessarily a most general complete set of variants as shown by Example 5. Therefore, full narrowing gives us a way of computing a *complete variant semantics*, $[\![t]\!]^{Full}_{E,Ax}$, from which we would like to obtain a subset $S \subseteq [\![t]\!]^{Full}_{E,Ax}$ such that S is a *most general and complete variant semantics*, i.e., $S = [\![t]\!]_{E,Ax}$. The key question, then, is:

Can we compute the set $[\![t]\!]_{E,Ax}$ of most general $\mathcal{E}$-variants of a term t effectively?

This is not entirely obvious. Full (i.e., unrestricted) E,Ax-narrowing may never terminate and the set $[\![t]\!]^{Full}_{E,Ax}$ can 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 if $[\![t]\!]_{E,Ax}$ is *finite*, then the narrowing strategy will *terminate* and will compute $[\![t]\!]_{E,Ax}$.

4.2. Narrowing Strategies and Their Properties

In order to obtain an appropriate narrowing strategy that enjoys better properties than full E,Ax-narrowing and allows to compute $[\![t]\!]_{E,Ax}$, 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 $\alpha : (t_0 \rightsquigarrow_{p_0,\sigma_0,R,Ax} t_1 \cdots \rightsquigarrow_{p_{n-1},\sigma_{n-1},R,Ax} t_n)$, we denote by α_i the narrowing sequence $\alpha_i : (t_0 \rightsquigarrow_{p_0,\sigma_0,R,Ax} t_1 \cdots \rightsquigarrow_{p_{i-1},\sigma_{i-1},R,Ax} t_i)$ which is a prefix of α. Given an order-sorted rewrite theory $\mathcal{R}$, we denote by $Full_{\mathcal{R}}(t)$ the (possibly infinite) set of all narrowing sequences starting at term t.

Definition 11 (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 $\alpha \in \mathcal{S}_{\mathcal{R}}(t)$ of length n, and each $i \in \{1, \ldots, n\}$, we also have $\alpha_i \in \mathcal{S}_{\mathcal{R}}(t)$.*

Note that this definition of a narrowing strategy is very general and does not consider any aspect about efficient narrowing strategies at all, see [6] for efficient narrowing strategies.

Each narrowing strategy is trivially sound w.r.t. rewriting. We say that a narrowing strategy $\mathcal{S}$ is *complete* w.r.t. rewriting if it satisfies Theorem 2 above, concretized as follows.

Definition 12 (Completeness of a Narrowing Strategy). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. A narrowing strategy $\mathcal{S}_{\mathcal{R}}$ is called* complete *iff for each pair of terms t_1 and t_2 and each E,Ax-normalized substitution θ such that $t_1\theta \rightarrow^{!}_{E,Ax} t_2$, there exists a term t'_2 and two E,Ax-normalized substitutions σ and ρ s.t. $(t_1 \rightsquigarrow^{*}_{\sigma,E,Ax} t'_2) \in \mathcal{S}_{\mathcal{R}}(t)$, $\theta|_{Var(t_1)} =_{Ax} (\sigma\rho)|_{Var(t_1)}$, and $t_2 =_{Ax} t'_2\rho$.*

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 strategies and consider only narrowing sequences to normalized terms.

Definition 13 (Narrowing Variant Semantics). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$ and $\mathcal{S}_{\mathcal{R}}$ be a narrowing strategy. We define the set of* narrowing variants *of a term t w.r.t. $\mathcal{S}_{\mathcal{R}}$ as $[\![t]\!]^{\mathcal{S}_{\mathcal{R}}}_{E,Ax} = \{(t', \theta) \mid (t \rightsquigarrow^{*}_{\theta,E,Ax} t') \in \mathcal{S}_{\mathcal{R}}(t) \text{ and } t' = t'{\downarrow_{E,Ax}}\}$.*

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

Definition 14 (Variant Completeness and Minimality). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. A narrowing strategy $\mathcal{S}_\mathcal{R}$ is called E, Ax-*variant-complete *(or just variant-complete) iff for any Σ-term t we have that $[\![t]\!]_{E,Ax} \simeq_{E,Ax} [\![t]\!]^{\mathcal{S}_\mathcal{R}}_{E,Ax}$. The narrowing strategy $\mathcal{S}_\mathcal{R}$ is called E, Ax-*variant-minimal *(or just variant-minimal) iff, in addition, for any Σ-term t we have that $[\![t]\!]_{E,Ax} \approx_{Ax} [\![t]\!]^{\mathcal{S}_\mathcal{R}}_{E,Ax}$ and for each pair of variants $(t_1, \theta_1), (t_2, \theta_2) \in [\![t]\!]^{\mathcal{S}_\mathcal{R}}_{E,Ax}$ such that $(t_1, \theta_1) \neq_{Ax} (t_2, \theta_2)$, we have that $(t_1, \theta_1) \not\approx_{Ax} (t_2, \theta_2)$.*

In practice, the set $\mathcal{S}_\mathcal{R}(t)$ of narrowing sequences from a term t will be generated by an *algorithm* $\mathcal{A}_{\mathcal{S}_\mathcal{R}}$. That is, $\mathcal{A}_{\mathcal{S}_\mathcal{R}}$ is a computable function such that, given a pair $(\mathcal{R}, t)$, it enumerates the set $\mathcal{S}_\mathcal{R}(t)$. Even when $\mathcal{R} = (\Sigma, Ax, E)$ is a decomposition of an equational theory, the strategy $\mathcal{S}_\mathcal{R}$ is variant-complete, and $[\![t]\!]_{E,Ax}$ is finite on an input term t, it may happen that $[\![t]\!]^{\mathcal{S}_\mathcal{R}}_{E,Ax}$ is not finite. Furthermore, even if $[\![t]\!]^{\mathcal{S}_\mathcal{R}}_{E,Ax}$ is finite, its enumeration using the algorithm $\mathcal{A}_{\mathcal{S}_\mathcal{R}}$ may 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. 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 15 (Optimal Variant Termination). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$ and $\mathcal{S}_\mathcal{R}$ be an E, Ax-variant-complete narrowing strategy. An algorithm $\mathcal{A}_{\mathcal{S}_\mathcal{R}}$ for computing $\mathcal{S}_\mathcal{R}$ is* variant-terminating *iff $\mathcal{A}_{\mathcal{S}_\mathcal{R}}(t)$ terminates on input $(\mathcal{R}, t)$ iff $[\![t]\!]^{\mathcal{S}_\mathcal{R}}_{E,Ax}$ is finite. An algorithm $\mathcal{A}_{\mathcal{S}_\mathcal{R}}$ is* optimally variant-terminating *iff both $\mathcal{A}_{\mathcal{S}_\mathcal{R}}$ is variant-terminating and $[\![t]\!]^{\mathcal{S}_\mathcal{R}}_{E,Ax}$ is variant-minimal for every Σ-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.

Proposition 1. *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. Let $\mathcal{S}_\mathcal{R}$ be an E, Ax-variant-complete narrowing strategy and $\mathcal{S}'_\mathcal{R}$ be an optimally variant-terminating narrowing strategy. Then, for each Σ-term t such that $\mathcal{S}_\mathcal{R}(t)$ terminates, then $\mathcal{S}'_\mathcal{R}(t)$ also terminates.*

Proof. *If $\mathcal{S}_\mathcal{R}(t)$ terminates, then $[\![t]\!]^{\mathcal{S}_\mathcal{R}}_{E,Ax}$ is necessarily finite. Therefore, $[\![t]\!]^{\mathcal{S}'_\mathcal{R}}_{E,Ax}$ is also necessarily finite, since $\mathcal{S}'_\mathcal{R}$ is variant-minimal. Therefore, $\mathcal{S}'_\mathcal{R}(t)$ also terminates.* □

Therefore, if a variant-complete narrowing strategy $\mathcal{S}_\mathcal{R}$ is optimally variant-terminating, then whenever any other narrowing strategy $\mathcal{S}'_\mathcal{R}$ enjoying the same variant-completeness property terminates on a term t, $\mathcal{S}_\mathcal{R}$ is guaranteed to terminate on t as well. Such an optimally variant-terminating strategy would be a powerful tool, improving over many narrowing strategies defined previously in the literature, as shown in the next section. Later, in Sections 5 and 6 below, we introduce a narrowing strategy that is optimally variant-terminating under some conditions.

4.3. 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 [31] to the modulo case.

Definition 16 (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 step modulo Ax for $\langle t, \rho\rangle$ is defined by $\langle t, \rho\rangle \overset{b}{\leadsto}_{p,\theta,R,Ax} \langle t', \rho'\rangle$ iff there is $p \in Pos_\Sigma(t)$, a rule $l \to r \in R$ properly renamed s.t. $Var(l) \cap W = \emptyset$, and $\theta \in CSU_{Ax}^{W'}(t|_p\rho = l)$ 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* [48] despite its completeness in the free case [38], i.e., there are innermost rewriting sequences modulo *AC* that are not lifted to basic narrowing sequences modulo Ax. In particular, basic narrowing modulo *AC* is not variant-complete.

Example 6. *The following full narrowing sequence relevant for the unification problem $X_1 + X_2 \stackrel{?}{=} 0$ of Example 1:*

$$X_1 + X_2 \leadsto_{\rho_1,E,Ax} X' + X''$$
$$\text{using } \rho_1 = \{X_1 \mapsto a + X', X_2 \mapsto a + X''\} \text{ and rule (3)}$$
$$X' + X'' \leadsto_{\rho_2,E,Ax} 0$$
$$\text{using } \rho_2 = \{X' \mapsto b, X'' \mapsto b\} \text{ and rule (2)}$$

is not a basic narrowing sequence modulo AC, since after the first step it results in a variable X and no further basic narrowing step modulo AC is possible:

$$\langle X_1 + X_2, id\rangle \overset{b}{\leadsto}_{\tau_1,E,Ax} \langle X, \tau_1\rangle$$
$$\text{using } \tau_1 = \{X_1 \mapsto a + X', X_2 \mapsto a + X'', X \mapsto X' + X''\} \text{ and rule (3)}$$

Since the pair $(0, \rho_1\rho_2)$ is a variant of $X_1 + X_2$ not subsumed by any basic narrowing sequence generated from $X_1 + X_2$, basic narrowing modulo AC is not variant-complete.

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

Example 7. *Consider the rewrite theory $\mathcal{R} = (\Sigma, \emptyset, E)$ where E is the set of confluent and terminating 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 Example 15 in Section 6, or also [19]). 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:

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

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

In the next section we define a variant-complete narrowing strategy.

5. Folding Variant Narrowing

In order to compute the variants of a term, we can simply keep track of all the variants generated so far by narrowing, since we know that for any decomposition there is a (possibly infinite) set of most general variants (modulo axioms and modulo renaming) and sooner or later full narrowing will generate those most general variants, thanks to Corollary 1. In this section, we define a narrowing strategy called *folding narrowing*, which works in this way and achieves variant-completeness. Note that the folding narrowing strategy is parametric on another complete narrowing strategy, which will allow us later to define more concise narrowing strategies for obtaining the variants. Also note that only when a term has a finite number of most general variants, a narrowing strategy can be optimally variant-terminating for that term; this is studied in detail in Section 6 below.

First, we need to introduce the notion of variant preordering with normalization, which is very close to Definition 6, in order to capture when a newly generated variant is subsumed by a previously generated one.

Definition 17 (Normalized Variant Preordering). *Let (Σ, Ax, E) be a decomposition of an equational theory $(\Sigma, \mathcal{E})$ and t be a Σ-term. Given two variants $(t_1, \theta_1), (t_2, \theta_2) \in [\![t]\!]^{\star}_{E,Ax}$, we write $(t_1, \theta_1) \sqsubseteq^{!}_{E,Ax} (t_2, \theta_2)$, meaning (t_2, θ_2) is a more general variant of t than (t_1, θ_1), iff $(t_1{\downarrow_{E,Ax}}, \theta_1) \sqsubseteq_{E,Ax} (t_2, \theta_2)$.*

We define in Definition 18 below the folding narrowing strategy, which is based on the different levels of reachable states, denoted as $Frontier_{\sqsubseteq^{!}_{E,Ax}}(I)_i$, and the relation $\sqsubseteq^{!}_{E,Ax}$ for identifying variants subsumed by previously generated ones. We are presenting a specialized version of the folding reachable transition system of [18] rolled together with our folding narrowing strategy. Given a decomposition $\mathcal{R} = (\Sigma, Ax, E)$ of an equational theory $(\Sigma, \mathcal{E})$ and a narrowing strategy $\mathcal{S}_{\mathcal{R}}$, we extend $\mathcal{S}_{\mathcal{R}}$ to variants as follows: given a term t and a substitution ρ, $\mathcal{S}_{\mathcal{R}}((t, \rho)) = \{(t, \rho) \rightsquigarrow^{*}_{\sigma,E,Ax} (t', \rho\sigma) \mid (t \rightsquigarrow^{*}_{\sigma,E,Ax} t') \in \mathcal{S}_{\mathcal{R}}(t)\}$.

Definition 18 (Folding Narrowing Strategy). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$ and $\mathcal{S}_{\mathcal{R}}$ a narrowing strategy. Let t be a Σ-term. The frontier from $I = (t, id)$ with folding $\sqsubseteq^{!}_{E,Ax}$ is defined as*

$$
\begin{aligned}
&Frontier_{\sqsubseteq^{!}_{E,Ax}}(I)_0 = I,\\
&Frontier_{\sqsubseteq^{!}_{E,Ax}}(I)_{n+1} = \{(y, \rho\sigma) \mid (\exists (z, \rho) \in Frontier_{\sqsubseteq^{!}_{E,Ax}}(I)_n : (z, \rho) \rightsquigarrow_{\sigma,E,Ax} (y, \rho\sigma)) \wedge\\
&\qquad\qquad (\nexists k \leq n, (w, \tau) \in Frontier_{\sqsubseteq^{!}_{E,Ax}}(I)_k : (y, \rho\sigma) \ \sqsubseteq^{!}_{E,Ax} \ (w, \tau))\}
\end{aligned}
$$

The folding $\mathcal{S}_{\mathcal{R}}$-narrowing strategy, denoted by $\mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t)$, is defined as

$$
\mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t) = \{t \rightsquigarrow^{k}_{\sigma,E,Ax} t' \mid ((t, id) \rightsquigarrow^{k}_{\sigma,E,Ax} (t', \sigma)) \in \mathcal{S}_{\mathcal{R}}(t) \wedge (t', \sigma) \in Frontier_{\sqsubseteq^{!}_{E,Ax}}(I)_k\}
$$

We write $Full^{\circlearrowleft}_{\mathcal{R}}$ to denote the folding version of the full narrowing strategy $Full_{\mathcal{R}}$. The following example shows the advantages of folding full-narrowing for computing variants, for instance w.r.t. basic narrowing modulo AC.

Example 8. *Considering Example 7. Using the $Full^{\circlearrowleft}_{\mathcal{R}}$ strategy, we only get step (i), since step (ii) is subsumed by step (i). That is, $(f(x'), \{x \mapsto f(x')\}) \sqsubseteq^{!}_{E,\emptyset} (x', \{x \mapsto x'\})$, since $f(x'){\downarrow_{E,Ax}} = x'$. So even though basic narrowing does not terminate for this equational theory, $Full^{\circlearrowleft}_{\mathcal{R}}$ does.*

The following example shows what steps are performed by $Full^{\circlearrowleft}_{\mathcal{R}}$ and its termination on our running example.

Example 9. *Using the theory from Example 3, for $t = X \oplus Y$ we get the following $Full^{\circlearrowleft}_{\mathcal{R}}$ steps. First, we show the narrowing steps with normalized substitutions.*

(i) $(X \oplus Y, id) \rightsquigarrow_{\phi_1} (Z, \phi_1)$*, using Equation* (6) *and substitution* $\phi_1 = \{X \mapsto 0, Y \mapsto Z\}$*,*
(ii) $(X \oplus Y, id) \rightsquigarrow_{\phi_2} (Z, \phi_2)$*, using Equation* (6) *and substitution* $\phi_2 = \{X \mapsto Z, Y \mapsto 0\}$*,*
(iii) $(X \oplus Y, id) \rightsquigarrow_{\phi_3} (Z, \phi_3)$*, using Equation* (8) *and substitution* $\phi_3 = \{X \mapsto Z \oplus U, Y \mapsto U\}$*,*
(iv) $(X \oplus Y, id) \rightsquigarrow_{\phi_4} (Z, \phi_4)$*, using Equation* (8) *and substitution* $\phi_4 = \{X \mapsto U, Y \mapsto Z \oplus U\}$*,*
(v) $(X \oplus Y, id) \rightsquigarrow_{\phi_5} (0, \phi_5)$*, using Equation* (7) *and substitution* $\phi_5 = \{X \mapsto U, Y \mapsto U\}$*,*
(vi) $(X \oplus Y, id) \rightsquigarrow_{\phi_6} (Z_1 \oplus Z_2, \phi_6)$*, using Equation* (8) *and* $\phi_6 = \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\}$*.*

Non-normalized narrowing steps such as

$$(X \oplus Y, id) \rightsquigarrow_{\phi_6} (Z, \phi_7)\text{, using Equation } (8) \text{ and } \phi_7 = \{X \mapsto U \oplus U, Y \mapsto Z\}$$

are also computed by $Full^{\circlearrowleft}_{\mathcal{R}}$ but all are finally subsumed by a variant with the normalized version of the same substitution, e.g., $(Z, \phi_7) \sqsubseteq_{E,Ax} (Z, \phi_1)$. Note that $Full^{\circlearrowleft}_{\mathcal{R}}$ terminates after generating all narrowing steps above:

1. *There are no further steps possible from (i)-(iv), since any instantiation of Z for which a narrowing step is possible would mean that the computed substitution is not normalized.*
2. *There is no further step possible from (v), since* 0 *is a normal form.*
3. *There are no further steps possible from (vi), since we are back at the beginning, i.e, $(Z_1 \oplus Z_2, \phi_6) \sqsubseteq^{!}_{E,Ax} (t, id)$, and can repeat all of the steps possible from (t, id), but all of the results are subsumed by the same step we already have from (t, id).*

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 $\mathcal{S}^{\circlearrowleft}$ is *variant-complete* provided the given narrowing strategy $\mathcal{S}$ that is restricted by folding is *complete* according to Definition 12. First, we provide two auxiliary definitions and an auxiliary result.

Definition 19. *Given a decomposition (Σ, Ax, E), a term t, and two narrowing sequences $\alpha_1 : t \rightsquigarrow^{*}_{\sigma_1,E,Ax} t_1$ and $\alpha_2 : t \rightsquigarrow^{*}_{\sigma_2,E,Ax} t_2$, we write $\alpha_1 \sqsubseteq_{E,Ax} \alpha_2$ if there is a substitution θ such that $(\sigma_1 \downarrow_{E,Ax})|_{Var(t)} =_{Ax} (\sigma_2\theta)|_{Var(t)}$ and $t_1 =_{Ax} t_2\theta$. We write $\alpha_1 \approx_{Ax} \alpha_2$ if there is a renaming substitution ρ such that $\sigma_1|_{Var(t)} =_{Ax} (\sigma_2\rho)|_{Var(t)}$ and $t_1 =_{Ax} t_2\rho$.*

Definition 20 (Most General Narrowing Sequence). *Given a decomposition (Σ, Ax, E), a narrowing sequence $\alpha : t \rightsquigarrow^{*}_{\theta,E,Ax} (t\theta)\downarrow_{E,Ax}$ is called a* most general *narrowing sequence if for any narrowing sequence $\alpha' : t \rightsquigarrow^{*}_{\theta',E,Ax} (t\theta')\downarrow_{E,Ax}$ such that $\alpha \sqsubseteq_{E,Ax} \alpha'$, then $\alpha \approx_{Ax} \alpha'$.*

Lemma 2. *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. Let $\mathcal{S}_{\mathcal{R}}$ be a complete narrowing strategy. If $\alpha : t \rightsquigarrow^{*}_{\sigma,E,Ax} (t\sigma)\downarrow_{E,Ax}$ and α is most general, then there is a narrowing sequence $\alpha' : t \rightsquigarrow^{*}_{\sigma',E,Ax} (t\sigma')\downarrow_{E,Ax}$ such that $\alpha' \in \mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t)$ and $\alpha \approx_{Ax} \alpha'$.*

Proof. *By contradiction. Let* $\alpha : t \rightsquigarrow_{\sigma_1,E,Ax} t_1 \cdots t_{k-1} \rightsquigarrow_{\sigma_k,E,Ax} t_k = (t\sigma)\downarrow_{E,Ax}$. *Since there is no narrowing sequence* $\alpha' : t \rightsquigarrow^*_{\sigma',E,Ax} (t\sigma')\downarrow_{E,Ax}$ *such that* $\alpha' \in \mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t)$ *and* $\alpha' \approx_{Ax} \alpha$, *by completeness of* $\mathcal{S}_{\mathcal{R}}$ *there is an alternative narrowing sequence* $\beta : t \rightsquigarrow_{\theta_1,E,Ax} u_1 \cdots u_{n-1} \rightsquigarrow_{\theta_n,E,Ax} u_n = (t\theta)\downarrow_{E,Ax}$ *in* $\mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t)$ *with* $\theta = \theta_1 \cdots \theta_n$ *and* $n \leq k$ *such that* $(t_n, \sigma_1 \cdots \sigma_n) \sqsubseteq^!_{E,Ax} (u_n, \theta_1 \cdots \theta_n)$, *i.e., there is a substitution* ρ *such that* $t_n\downarrow_{E,Ax} =_{Ax} u_n\rho$ *and* $((\sigma_1 \cdots \sigma_n)\downarrow_{E,Ax})|_{Var(t)} =_{Ax} (\theta_1 \cdots \theta_n\rho)|_{Var(t)}$. *Note that* ρ *cannot be a renaming, since* ρ *being a renaming implies* $\beta \approx_{Ax} \alpha$. *Then, by confluence, there is a rewriting sequence starting from* u_n *that reaches* $t\sigma\downarrow_{E,Ax}$, *i.e.,* $(u_n\rho\sigma_{n+1} \cdots \sigma_k) \rightarrow^*_{E,Ax} (t\sigma)\downarrow_{E,Ax}$. *But this rewriting sequence can be lifted to a narrowing sequence, i.e., by completeness of* $\mathcal{S}_{\mathcal{R}}$ *there is a narrowing sequence* $\beta' : u_n \rightsquigarrow^*_{\tau,E,Ax} t''$ *and a substitution* ρ' *such that* $(\sigma_{n+1} \cdots \sigma_k)\downarrow_{E,Ax}|_{Var(u_n)} =_{Ax} (\tau\rho')|_{Var(u_n)}$ *and* $(t\sigma)\downarrow_{E,Ax} =_{Ax} t''\rho'$. *Then, we can concatenate both narrowing sequences* $\beta;\beta' : t \rightsquigarrow^*_{\theta,E,Ax} u_n \rightsquigarrow^*_{\tau,E,Ax} t''$ *such that* $(\sigma_1 \cdots \sigma_n\sigma_{n+1} \cdots \sigma_k)\downarrow_{E,Ax}|_{Var(t)} =_{Ax} (\theta_1 \cdots \theta_n\rho\tau\rho')|_{Var(t)}$ *and* $(t\theta)\downarrow_{E,Ax} =_{Ax} t''\rho'\rho$. *Since* ρ *is not a renaming, the narrowing sequence* $\beta;\beta'$ *is more general than* α. *But this contradicts that* α *is a most general narrowing sequence and, thus, the conclusion follows.* □

Theorem 3 (Variant Completeness of Folding Narrowing). *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$. *Let* t_1 *be a* Σ*-term and* θ *be an* E,Ax*-normalized substitution. Let* $\mathcal{S}_{\mathcal{R}}$ *be a complete narrowing strategy. If* $t_1\theta \rightarrow^!_{E,Ax} t_2$ *then there exist a term* t'_2 *and two* E,Ax*-normalized substitutions* σ *and* ρ *s.t.* $(t_1 \rightsquigarrow^*_{\sigma,E,Ax} t'_2) \in \mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t_1)$, $\theta|_{Var(t_1)} =_{Ax} (\sigma\rho)|_{Var(t_1)}$, *and* $t_2 =_{Ax} t'_2\rho$.

Proof. *Given* $t_1\theta \rightarrow^!_{E,Ax} t_2$, *by completeness of narrowing (Theorem 2), there exist a term* t'_2 *and two* E,Ax*-normalized substitutions* σ *and* ρ *such that* $(\alpha : t_1 \rightsquigarrow^*_{\sigma,E,Ax} t'_2) \in \mathcal{S}_{\mathcal{R}}(t_1)$, $\theta|_{Var(t_1)} =_{Ax} (\sigma\rho)|_{Var(t_1)}$, *and* $t_2 =_{Ax} t'_2\rho$. *Let us assume that* α *is most general, since there is always at least one most general narrowing sequence. Then, by Lemma 2, there exists* $(\beta : t_1 \rightsquigarrow^*_{\phi,E,Ax} u) \in \mathcal{S}_{\mathcal{R}}(t_1)$ *such that* $\alpha \approx_{Ax} \beta$ *and the conclusion follows.* □

We can effectively compute a complete set of variants by folding narrowing in the following way.

Corollary 2 (Computing the Variants). *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$. *Let* t *be a* Σ*-term. Let* $\mathcal{S}_{\mathcal{R}}$ *be a complete narrowing strategy. If* $(t', \sigma) \in [\![t]\!]_{E,Ax}$, *then there are* t'', σ', *and* ρ *such that* $(t \rightsquigarrow^*_{\sigma',E,Ax} t'') \in \mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t)$, t'' *is* $\rightarrow_{E,Ax}$*-irreducible,* σ' *is* $\rightarrow_{E,Ax}$*-normalized,* ρ *is a renaming,* $t' =_{Ax} t''\rho$, *and* $\sigma|_{Var(t)} =_{Ax} (\sigma'\rho)|_{Var(t)}$.

We can conclude that the folding full-narrowing strategy is a variant-complete narrowing strategy.

Corollary 3. *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$. *The folding full-narrowing strategy* $Full^{\circlearrowleft}_{\mathcal{R}}$ *is* variant-complete, *i.e., for each* Σ*-term* t, $[\![t]\!]_{E,Ax} \simeq_{E,Ax} [\![t]\!]^{Full^{\circlearrowleft}_{\mathcal{R}}}_{E,Ax}$.

Note that folding full-narrowing is not variant-minimal (and thus not optimally variant-terminating).

Example 10. *Consider the following decomposition without axioms*

$$f(s(X)) = g(X) \qquad g(s(X)) = 0 \qquad f(s(s(0))) = 0.$$

For term $f(X)$, *we have that* $\{(f(X), id), (g(X'), \{X \mapsto s(X')\}), (0, \{X \mapsto s(s(X''))\})\}$ *is the set of most general variants. However, folding full-narrowing will generate those three variants plus* $(0, \{X \mapsto s(s(0))\})$, *which is subsumed by variant* $(0, \{X \mapsto s(s(X''))\})$*:*

1. *The variant* $(f(X), id)$ *without any narrowing step.*
2. *Variants with one narrowing step:* $(g(X'), \{X \mapsto s(X')\})$ *and* $(0, \{X \mapsto s(s(0))\})$*, i.e.,* $(f(X) \rightsquigarrow_{\{X \mapsto s(X')\},E,Ax} g(X')) \in Full_{\mathcal{R}}^{\circlearrowleft}$ *and* $(f(X) \rightsquigarrow_{\{X \mapsto s(s(0))\},E,Ax} 0) \in Full_{\mathcal{R}}^{\circlearrowleft}$.
3. *The variant* $(0, \{X \mapsto s(s(X''))\})$ *with two narrowing steps:*

$$(f(X) \rightsquigarrow_{\{X \mapsto s(X')\},E,Ax} g(X') \rightsquigarrow_{\{X' \mapsto s(X'')\},E,Ax} 0) \in Full_{\mathcal{R}}^{\circlearrowleft}$$

In the next section, we refine the folding narrowing strategies and improve over the folding full-narrowing strategy for computing variants.

5.1. Variant Narrowing Strategy

We have shown that the folding full-narrowing strategy $Full_{\mathcal{R}}^{\circlearrowleft}$ is variant-complete. However, there is another interesting aspect about narrowing strategies:

> *Are there strategies more effective than full-narrowing which can be extended to folding narrowing in order to compute variants?*

We answered this question in the positive in our paper [20] with the notion of *variant narrowing strategy*, but we improve the presentation here.

Let us first motivate with two ideas why a narrowing strategy which is an alternative to full narrowing can be very useful for a decomposition. First, the completeness of a narrowing strategy w.r.t. a decomposition is restricted to normalized substitutions. Therefore, we are interested in narrowing strategies that provide only narrowing sequences with normalized substitutions. Basic narrowing was an attempt at this but, as we show in Example 6, it is incomplete for the modulo case as well as (possibly) non-terminating for computing variants, as shown in Example 7. Here we present a narrowing strategy that computes *only* normalized substitutions without losing completeness. Second, applying narrowing $\rightsquigarrow_{E,Ax}$ to perform $(E \cup Ax)$-unification without any restriction, as done in $Full_{\mathcal{R}}$, is very wasteful, because as soon as a rewrite step $\rightarrow_{E,Ax}$ is enabled in a term that has also narrowing steps $\rightsquigarrow_{E,Ax}$, such a rewrite step should always be taken before any further narrowing steps are applied, thanks to confluence and coherence modulo Ax. This idea is consistent with the implementation of rewriting logic [49] and, therefore, the relation $\rightarrow_{E,Ax}^{!}; \rightsquigarrow_{E,Ax}$ makes sense as an optimization of $\rightsquigarrow_{E,Ax}$ (see [29] for discussion about this idea in a context without axioms). 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, for a decomposition $\mathcal{R} = (\Sigma, Ax, E)$, if two narrowing steps $t \rightsquigarrow_{\sigma_1,E,Ax} t_1$ and $t \rightsquigarrow_{\sigma_2,E,Ax} t_2$ are possible and we have that $\sigma_1 \sqsubseteq_{Ax} \sigma_2$ (i.e., σ_2 is more general than σ_1), then it is enough to take only the narrowing step using σ_2. These improvements are formalized as follows. First, we introduce a partial order between narrowing steps, defining when a narrowing step is more general than another narrowing step.

Definition 21 (Preorder and equivalence of narrowing steps). *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of* $(\Sigma, \mathcal{E})$*. Let us consider two narrowing steps* $\alpha_1 : t \rightsquigarrow_{\sigma_1,E,Ax} s_1$ *and* $\alpha_2 : t \rightsquigarrow_{\sigma_2,E,Ax} s_2$*. We write* $\alpha_1 \preceq_{Ax} \alpha_2$ *if* $\sigma_1|_{Var(t)} \sqsubseteq_{Ax} \sigma_2|_{Var(t)}$ *and* $\alpha_1 \prec_{Ax} \alpha_2$ *if* $\sigma_1|_{Var(t)} \sqsubset_{Ax} \sigma_2|_{Var(t)}$ *(i.e.,* σ_2 *is strictly more general than* σ_1*). We write* $\alpha_1 \simeq_{Ax} \alpha_2$ *if* $\sigma_1|_{Var(t)} \simeq_{Ax} \sigma_2|_{Var(t)}$*. The relation* $\alpha_1 \simeq_{Ax} \alpha_2$ *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 representative* $\underline{\alpha} \in [\alpha]_{\simeq_{Ax}}$ *in each equivalence class of narrowing steps from* t*. Therefore,* $\underline{\alpha}$ *will always denote a chosen unique representative* $\underline{\alpha} \in [\alpha]_{\simeq_{Ax}}$.

The relation $\preceq_{Ax}$ provides an improvement on narrowing executions, since narrowing steps with more general computed substitutions will be selected instead of narrowing steps with more instantiated computed substitutions. Also, this relation ensures that, when both a rewriting step and a narrowing step are available, the rewriting step will always be chosen. Finally, the relation $\simeq_{Ax}$ provides another improvement, since only one narrowing (or rewriting) step is chosen in each equivalence class, reducing the width of the narrowing tree even more. The very last improvement is to restrict to normalized computed substitutions, as motivated at the beginning of this section.

Definition 22 (Variant Narrowing). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of $(\Sigma, \mathcal{E})$. Given a Σ-term t, we define the variant narrowing strategy $VN_{\mathcal{R}}(t) = \{t \rightsquigarrow^*_{\sigma,\underline{E},Ax} s\}$, where: (i) $\sigma|_{Var(t)}$ is E, Ax-normalized and (ii) each narrowing step $u \rightsquigarrow_{\rho,\underline{E},Ax} v$ is defined as the narrowing step $\underline{\alpha}$: $u \rightsquigarrow_{\rho,E,Ax} v$ such that $\underline{\alpha}$ is maximal w.r.t. the order $\preceq_{Ax}$, and $\underline{\alpha}$ is the chosen unique representative of its $\simeq_{Ax}$-equivalence class.*

Example 11. *Consider Example 3. For the term $t = X \oplus Y \oplus X \oplus Y$, there are nearly* 150 *full narrowing steps, since subterm $X \oplus Y$ had* 124 *narrowing steps as explained in Example 5 and there are even more combinations. However, variant narrowing recognizes that this term is not yet normalized, i.e., $X \oplus Y \oplus X \oplus Y \rightarrow 0$, and such a rewriting step is more general than any narrowing step. Thus, variant narrowing performs only a rewriting step and avoids such an exceptionally large number of narrowing steps. Note that there are two other rewrite steps $X \oplus Y \oplus X \oplus Y \rightarrow Y \oplus Y$ and $X \oplus Y \oplus X \oplus Y \rightarrow X \oplus X$ and variant narrowing will choose one of these three as the unique representative of the $\simeq_{AC}$-equivalence class of rewrite steps.*

We denote the extended folding version of variant narrowing, i.e., *folding variant narrowing*, by $VN^{\circlearrowleft}_{\mathcal{R}}$. The condition in Definition 22 that $\sigma|_{Var(t)}$ is E, Ax-normalized (in contrast to σ being E, Ax-normalized) is essential for a correct behavior of the strategy, as shown below.

Example 12. *Consider the following decomposition $(\Sigma, \emptyset, E)$ where E contains $f(a, b, X) \rightarrow f(a, b)$, symbol f is AC, and X is a variable. Consider the term $t = f(a, a, a, b, b, b)$, whose normal form is $f(a, b)$, i.e., $f(a, a, a, b, b, b) \rightarrow_{E,Ax} f(a, b)$. Any rewriting sequence leading to its normal form does not consider a normalized substitution, i.e., the first rewriting step of any rewriting sequence will use substitution $\{X \mapsto f(a, a, b, b)\}$. Therefore, we cannot restrict ourselves to normalized substitution w.r.t. rewriting steps.*

On the other hand, consider now the term $s = f(Y_1, Y_2)$ and the narrowing step $f(Y_1, Y_2) \rightsquigarrow_{\rho_2,E,Ax} f(a, b)$ with $\rho_2 = \{Y_1 \mapsto f(a, b, Y_3), X \mapsto f(Y_2, Y_3)\}$. The unifier ρ_2 is not normalized, since $f(a, b, Y_3)\downarrow_{E,Ax} = f(a, b)$. Note that we cannot normalize the substitution, since it would not correspond to any narrowing step and we simply discard this narrowing step because there is another more general narrowing step (i.e., $(f(a, b), \rho_2\downarrow_{E,Ax}) \sqsubseteq_{Ax} (f(a, b), \rho_1)$). Note that the ability to discard narrowing steps in confluent, terminating, and coherent systems whose computed substitution is not normalized is a key point for achieving termination for variant generation. The set of most general unifiers computed by all the narrowing steps is as follows:

$\rho_1 = \{Y_1 \mapsto f(a, b), X \mapsto Y_2\}$
$\rho_2 = \{Y_1 \mapsto f(a, b, Y_3), X \mapsto f(Y_2, Y_3)\}$
$\rho_3 = \{Y_2 \mapsto f(a, b), X \mapsto Y_1\}$
$\rho_4 = \{Y_2 \mapsto f(a, b, Y_3), X \mapsto f(Y_1, Y_3)\}$
$\rho_5 = \{Y_1 \mapsto a, Y_2 \mapsto b\}$
$\rho_6 = \{Y_1 \mapsto a, Y_2 \mapsto f(b, Y_3), X \mapsto Y_3\}$
$\rho_7 = \{Y_1 \mapsto b, Y_2 \mapsto a\}$
$\rho_8 = \{Y_1 \mapsto b, Y_2 \mapsto f(a, Y_3), X \mapsto Y_3\}$
$\rho_9 = \{Y_1 \mapsto f(a, Y_3), Y_2 \mapsto b, X \mapsto Y_3\}$
$\rho_{10} = \{Y_1 \mapsto f(a, Y_3), Y_2 \mapsto f(b, Y_4), X \mapsto f(Y_3, Y_4)\}$
$\rho_{11} = \{Y_1 \mapsto f(b, Y_3), Y_2 \mapsto a, X \mapsto Y_3\}$
$\rho_{12} = \{Y_1 \mapsto f(b, Y_3), Y_2 \mapsto f(a, Y_4), X \mapsto f(Y_3, Y_4)\}$

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

Lemma 3 (Normalization of Variant Narrowing). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of $(\Sigma, \mathcal{E})$. Let t be a Σ-term. If t is not E, Ax-irreducible, then, relative to the unique choice of $\underline{\alpha} \in [\alpha]_{\simeq_{Ax}}$ in Definition 21 , there is a unique $\rightsquigarrow_{\underline{E},Ax}$-narrowing sequence from t performing only rewriting steps.*

Proof. *Immediate, since t is not E, Ax-irreducible and the theory is confluent and sort-decreasing.* □

The following result ensures that variant narrowing is complete.

Theorem 4 (Completeness of Variant Narrowing). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of $(\Sigma, \mathcal{E})$. If $\alpha : t \rightsquigarrow^{*}_{\sigma,E,Ax} (t\sigma)\downarrow_{E,Ax}$ such that $\sigma|_{Var(t)}$ is E, Ax-normalized and α is a most general narrowing sequence, then there exists σ' such that $t \rightsquigarrow^{*}_{\sigma',\underline{E},Ax} (t\sigma')\downarrow_{E,Ax}$, and $\sigma|_{Var(t)} \approx_{Ax} \sigma'|_{Var(t)}$.*

Proof. *If $\alpha : t \rightsquigarrow^{*}_{\sigma,E,Ax} (t\sigma)\downarrow_{E,Ax}$ such that $\sigma|_{Var(t)}$ is E, Ax-normalized and α is a most general narrowing sequence, then it is sufficient to show that the computed substitution at each step in α is maximal w.r.t. $\sqsubseteq_{Ax}$.*

We prove this by contradiction. Let us consider a narrowing step $i \in \{1, \ldots, n\}$ in α, i.e. $t_i \rightsquigarrow_{\sigma_i,E,Ax} t_{i+1}$, such that σ_i is not maximal w.r.t. $\sqsubseteq_{Ax}$. That is, there is an alternative narrowing step from t_i, i.e., $t_i \rightsquigarrow_{\tau,E,Ax} w$, with a strictly more general substitution τ, i.e., there is a substitution τ' s.t. $\sigma_i|_{Var(t_i)} =_{Ax} (\tau\tau')|_{Var(t_i)}$ and τ' is not a renaming. Note that, since α is most general, there is no narrowing sequence $w \rightsquigarrow^{*}_{\phi,E,Ax} t_n$ and substitution ϕ' such that $\sigma|_{Var(t)} =_{Ax} (\sigma_1 \cdots \sigma_{i-1}\tau\phi\phi')|_{Var(t)}$. Then, we have that $t_i\sigma_i \rightarrow_{E,Ax} t_{i+1}$ and that there is a term w' such that $t_i\sigma_i \rightarrow_{E,Ax} w'$ and $w' =_{Ax} w\tau'$. By confluence, there is a term u such that $t_{i+1} \rightarrow^{*}_{E,Ax} u$ and $w' \rightarrow^{*}_{E,Ax} u$. But then, for any narrowing sequence $u \rightsquigarrow^{*}_{\mu,E,Ax} u'$ such that $\mu|_{Var(t_{i+1})} =_{Ax} (\sigma_{i+1} \cdots \sigma_n)|_{Var(t_{i+1})}$, there is a whole narrowing sequence $t \rightsquigarrow^{*}_{\sigma',E,Ax} (t\sigma')\downarrow_{E,Ax}$ such that $\sigma'|_{Var(t)} = (\sigma_1 \cdots \sigma_{i-1}\tau\mu)|_{Var(t)}$. This implies that $\sigma \sqsubset_{Ax} \sigma'$, since $(\sigma_i \cdots \sigma_n)|_{Var(t_i)} =_{Ax} (\tau\mu\tau')|_{Var(t_i)}$. Therefore, we have a contradiction because σ' is strictly more general than σ. □

Note that the previous theorem is only valid when E is confluent[2] modulo Ax, and not just *ground confluent* [46] modulo Ax, as shown by the following example.

Example 13. *Let us consider the following rewrite theory without axioms, which is terminating and ground confluent but not confluent:*

$$f(X) = 0 \quad f(X) = g(X) \quad g(0) = 0 \quad g(s(X)) = g(X)$$

If we consider the term $f(X)$ and the narrowing step taking the first equation, then we compute the most general substitution, i.e. $f(X) \rightsquigarrow_{id,E,Ax} 0$. However, if we consider $f(X)$ and the narrowing step that takes the second equation, i.e., $f(X) \rightsquigarrow_{id,E,Ax} g(X)$, we will compute an infinite number of substitutions, i.e., $\forall n \geq 0 : g(X) \rightsquigarrow^{*}_{\{X \mapsto s^n(0)\},E,Ax} 0$, and none of them is more general than the identity substitution computed with the first equation.

[2]Note that a decomposition already requires confluence instead of ground confluence.

The following interesting result holds for folding variant narrowing but not for folding full-narrowing.

Theorem 5 (Minimality of Folding Variant Narrowing). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of $(\Sigma, \mathcal{E})$. If $\alpha : t \rightsquigarrow^*_{\sigma,E,Ax} (t\sigma)\downarrow_{E,Ax}$ with $\sigma|_{Var(t)}$ being E, Ax-normalized and $\alpha' : t \rightsquigarrow^*_{\sigma',E,Ax} (t\sigma')\downarrow_{E,Ax}$ with $\sigma'|_{Var(t)}$ being E, Ax-normalized such that $\sigma|_{Var(t)} \sqsubset_{Ax} \sigma'|_{Var(t)}$, and α' is a most general narrowing sequence, then there is a narrowing sequence $\beta : t \rightsquigarrow^*_{\theta,E,Ax} (t\theta)\downarrow_{E,Ax}$ in $VN^{\circlearrowleft}_{\mathcal{R}}$ such that $\alpha' \approx_{Ax} \beta$ but there is no narrowing sequence $\beta' : t \rightsquigarrow^*_{\theta',E,Ax} (t\theta')\downarrow_{E,Ax}$ in $VN^{\circlearrowleft}_{\mathcal{R}}$ such that $\alpha \approx_{Ax} \beta'$.*

Proof. *The first statement is proved by the most generality of α' and Theorem 4, i.e., there is $\beta : t \rightsquigarrow^*_{\theta,E,Ax} (t\theta)\downarrow_{E,Ax}$ in $VN^{\circlearrowleft}_{\mathcal{R}}$ such that $\alpha' \approx_{Ax} \beta$. The second statement is proved by contradiction, i.e., we asume that there is $\beta' : t \rightsquigarrow^*_{\theta',E,Ax} (t\theta')\downarrow_{E,Ax}$ in $VN^{\circlearrowleft}_{\mathcal{R}}$ such that $\alpha \approx_{Ax} \beta'$. For simplicity, we assume that $\alpha' \in VN^{\circlearrowleft}_{\mathcal{R}}$ and use α' instead of β in the rest of the proof. Let α and α' be as follows:*

$$\alpha' : t \rightsquigarrow_{\sigma'_1,E,Ax} t'_1 \rightsquigarrow_{\sigma'_2,E,Ax} t'_2 \cdots t'_{m-1} \rightsquigarrow_{\sigma'_m,E,Ax} t'_m = (t\sigma')\downarrow_{E,Ax}$$

and

$$\alpha : t \rightsquigarrow_{\sigma_1,E,Ax} t_1 \rightsquigarrow_{\sigma_2,E,Ax} t_2 \cdots t_{n-1} \rightsquigarrow_{\sigma_n,E,Ax} t_n = (t\sigma)\downarrow_{E,Ax}$$

Let us consider the first narrowing step $i \in \{1, \ldots, n\}$ in α, i.e. $t_{i-1} \rightsquigarrow_{\sigma_i,E,Ax} t_i$, where there is a substitution τ such that $\sigma_i|_{Var(t_i)} =_{Ax} (\sigma'_i\tau)|_{Var(t_i)}$ and τ is not a renaming. Since $(\sigma_1 \cdots \sigma_{i-1})|_{Var(t)} \approx_{Ax} (\sigma'_1 \cdots \sigma'_{i-1})|_{Var(t)}$, by coherence and confluence, there are two terms w and w' such that $t\sigma_1 \cdots \sigma_{i-1} \rightarrow^*_{E,Ax} w$, $t\sigma'_1 \cdots \sigma'_{i-1} \rightarrow^*_{E,Ax} w'$, and $w \approx_{Ax} w'$. Let ρ be such that $(\sigma_1 \cdots \sigma_{i-1})|_{Var(t)} =_{Ax} (\sigma'_1 \cdots \sigma'_{i-1}\rho)|_{Var(t)}$ and $w =_{Ax} w'\rho$. We can add substitution σ'_i to have rewrite sequences $t\sigma_1 \cdots \sigma_{i-1}\sigma'_i \rightarrow^*_{E,Ax} w\sigma'_i$ and $t\sigma'_1 \cdots \sigma'_{i-1}\rho\sigma'_i \rightarrow^*_{E,Ax} w\sigma'_i$. By completeness of narrowing, there exist substitutions ϕ and ϕ' and a most general narrowing sequence $\alpha'' : t_{i-1} \rightsquigarrow^*_{\phi,E,Ax} u$ such that $\sigma'_i|_{Var(t_{i-1})} =_{Ax} (\phi\phi')|_{Var(t_{i-1})}$, and $w\sigma'_i =_{Ax} u\phi'$. But then there are two narrowing steps from term t_{i-1}, $t_{i-1} \rightsquigarrow_{\sigma_i,E,Ax} t_i$ and the first step of α'' s.t. the first step of α'' has a substitution more general than σ_i. But the $VN_{\mathcal{R}}$ strategy would have chosen the first step of α'' instead of the narrowing step $t_{i-1} \rightsquigarrow_{\sigma_i,E,Ax} t_i$ and this contradicts that there is $\beta' : t \rightsquigarrow^*_{\theta',E,Ax} (t\theta')\downarrow_{E,Ax}$ in $VN^{\circlearrowleft}_{\mathcal{R}}$ such that $\alpha \approx_{Ax} \beta'$. □

Now, we know that $VN^{\circlearrowleft}_{\mathcal{R}}$ is an efficient variant-complete and variant-minimal strategy, so we can use it to effectively compute variants.

Corollary 4. *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. The folding variant narrowing strategy $VN^{\circlearrowleft}_{\mathcal{R}}$ is variant-complete and variant-minimal, i.e., for any Σ-term t, $[\![t]\!]_{E,Ax} \approx_{Ax} [\![t]\!]^{VN^{\circlearrowleft}_{\mathcal{R}}}_{E,Ax}$.*

Finally, we return to our running example for the $VN^{\circlearrowleft}_{\mathcal{R}}$ strategy.

Example 14. *Consider Example 9. For $t = X \oplus Y$ we get the following $VN^{\circlearrowleft}_{\mathcal{R}}$ steps with normalized substitutions:*

(i) $(X \oplus Y, id) \rightsquigarrow_{\phi_1} (Z, \phi_1)$, *using Equation* (6) *and substitution* $\phi_1 = \{X \mapsto 0, Y \mapsto Z\}$,
(ii) $(X \oplus Y, id) \rightsquigarrow_{\phi_2} (Z, \phi_2)$, *using Equation* (6) *and substitution* $\phi_2 = \{X \mapsto Z, Y \mapsto 0\}$,
(iii) $(X \oplus Y, id) \rightsquigarrow_{\phi_3} (Z, \phi_3)$, *using Equation* (8) *and substitution* $\phi_3 = \{X \mapsto Z \oplus U, Y \mapsto U\}$,

(iv) $(X \oplus Y, id) \rightsquigarrow_{\phi_4} (Z, \phi_4)$*, using Equation* (8) *and substitution* $\phi_4 = \{X \mapsto U, Y \mapsto Z \oplus U\}$*,*
(v) $(X \oplus Y, id) \rightsquigarrow_{\phi_5} (0, \phi_5)$*, using Equation* (7) *and substitution* $\phi_5 = \{X \mapsto U, Y \mapsto U\}$*,*
(vi) $(X \oplus Y, id) \rightsquigarrow_{\phi_6} (Z_1 \oplus Z_2, \phi_6)$*, using Equation* (8) *and* $\phi_6 = \{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\}$*.*

Note that $VN^{\circlearrowleft}_{\mathcal{R}}$ *terminates (as* $Full^{\circlearrowleft}_{\mathcal{R}}$ *does) after generating all these narrowing steps.*

In the following, we study under which conditions the folding variant narrowing strategy is optimally variant-terminating, providing the best narrowing strategy for computing variants in the modulo case but also in the free theory, improving beyond basic narrowing.

6. The Finite Variant Property

An interesting case is when we know a priori that any Σ-term has a finite number of most general variants.

Definition 23 (Finite variant property). [11] *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$*. Then* $(\Sigma, \mathcal{E})$*, and thus* $\mathcal{R}$*, has the* finite variant property (FV) *iff for each* Σ*-term* t*, the set* $[\![t]\!]_{E,Ax}$ *is finite. We call* $\mathcal{R}$ *a* finite variant decomposition *of* $(\Sigma, \mathcal{E})$ *iff* $\mathcal{R}$ *has the finite variant property.*

The following corollary is immediate for finite variant decompositions.

Corollary 5. *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$ *and* $\mathcal{S}_{\mathcal{R}}$ *be an* E, Ax*-variant-complete narrowing strategy.* $\mathcal{S}^{\circlearrowleft}_{\mathcal{R}}$ *is variant-terminating iff* $\mathcal{R}$ *is a finite variant decomposition of* $(\Sigma, \mathcal{E})$*.*

Proof. *Given a* Σ*-term* t*, for each* $(t', \sigma) \in [\![t]\!]_{E,Ax}$*, by Corollary 2, there are* t''*,* σ'*, and* ρ *such that* $(t \rightsquigarrow^*_{\sigma', E, Ax} t'') \in \mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t)$*,* t'' *is* $\rightarrow_{E,Ax}$*-irreducible,* $\sigma'|_{Var(t)}$ *is* $\rightarrow_{E,Ax}$*-normalized,* ρ *is a renaming,* $t' =_{Ax} t''\rho$*, and* $\sigma|_{Var(t)} =_{Ax} (\sigma'\rho)|_{Var(t)}$*. Since* $[\![t]\!]_{E,Ax}$ *is finite and it contains the most general variants w.r.t.* $\sqsubseteq_{E,Ax}$*, for each possible variant* $(u, \phi) \in [\![t]\!]^{\star}_{E,Ax}$*, there is a node* (u', ϕ') *in the narrowing tree such that* $(u, \phi) \sqsubseteq_{E,Ax} (u', \phi')$ *and, thus, the narrowing tree generated by* $\mathcal{S}^{\circlearrowleft}_{\mathcal{R}}(t)$ *has a bounded depth.* □

The folding variant narrowing $VN^{\circlearrowleft}_{\mathcal{R}}$ is variant-minimal and the following corollary holds for finite variant decompositions.

Corollary 6. *If* $\mathcal{R} = (\Sigma, Ax, E)$ *is a finite variant decomposition of* $(\Sigma, \mathcal{E})$*, then* $VN^{\circlearrowleft}_{\mathcal{R}}$ *is optimally variant-terminating.*

Proof. *By Corollary 4,* $VN^{\circlearrowleft}_{\mathcal{R}}$ *is variant-minimal and, thus, the narrowing tree generated by* $VN^{\circlearrowleft}_{\mathcal{R}}$ *contains all and only all the variants of the set* $[\![t]\!]_{E,Ax}$ *for a given* Σ*-term* t*. Therefore, the narrowing tree is always the shortest tree possible for generating the set of most general variants* $[\![t]\!]_{E,Ax}$ *and we conclude that* $VN^{\circlearrowleft}_{\mathcal{R}}$ *is optimally variant-terminating.* □

6.1. Computing Variants for Theories with the Finite Variant Property

Comon and Delaune characterize the finite variant property in terms of the following boundedness property, which is *equivalent* to FV.

Lemma 4. [11] *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. $\mathcal{R}$ has the finite variant property if and only if for every term t, there is a finite set $\Theta(t)$ of substitutions such that*

$$\forall\sigma, \exists\theta \in \Theta(t), \exists\tau : (\sigma{\downarrow_{E,Ax}})|_{Var(t)} =_{Ax} (\theta\tau)|_{Var(t)} \wedge (t\sigma){\downarrow_{E,Ax}} =_{Ax} ((t\theta){\downarrow_{E,Ax}})\tau$$

Definition 24 (Boundedness property). [11] *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. $\mathcal{R}$ has the* boundedness property *(BP) iff for every term t there exists an integer n, denoted by $\#_{E,Ax}(t)$, such that for every E, Ax-normalized substitution σ the normal form of $t\sigma$ is reachable by an E, Ax-rewriting sequence whose length can be bounded by n (thus independently of σ), i.e.,*

$$\forall t, \exists n, \forall\sigma, t(\sigma{\downarrow_{E,Ax}}) \xrightarrow{\leq n}_{E,Ax} (t\sigma){\downarrow_{E,Ax}}.$$

Lemma 4 and Definition 24 allow the following result.

Theorem 6. [11] *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. Then, $\mathcal{R}$ satisfies the boundedness property if and only if $\mathcal{R}$ is a finite variant decomposition of $(\Sigma, \mathcal{E})$.*

Obviously, if for a term t, the minimal length of a rewrite sequence to the canonical form of an instance $t\sigma$, with σ normalized, cannot be bounded, the theory does not have the finite variant property. It is easy to see that for the addition equations

$$0 + Y = Y \qquad\qquad s(X) + Y = s(X + Y)$$

the term $t = X + Y$, and the family of substitutions $\sigma_n = \{X \mapsto s^n(0)\}$, $n \in \mathbb{N}$, this is the case, and therefore, since $FV \Leftrightarrow BP$, the addition theory lacks the finite variant property.

Example 15. *Consider again Example 7 consisting of the rewrite theory $\mathcal{R} = (\Sigma, \emptyset, E)$ where E is the set of confluent and terminating 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 theory has the finite variant property as it does have the boundedness property, since for any term t and a normalized substitution θ, a bound for t is given by the number of f symbols in the term.*

Proposition 2 (Computing the Finite Variants). [20] *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a finite variant decomposition of an order-sorted equational theory $(\Sigma, \mathcal{E})$. Let t be a Σ-term and $\#_{E,Ax}(t) = n$. Then, $(s, \sigma) \in [\![t]\!]_{E,Ax}$ if and only if there is a narrowing sequence $t \rightsquigarrow^{\leq n}_{\sigma,E,Ax} s$ such that s is $\to_{E,Ax}$-irreducible and σ is $\to_{E,Ax}$-normalized.*

Example 16. *Consider again Example 3. For this theory, narrowing clearly does not terminate because $Z_1 \oplus Z_2 \rightsquigarrow_{\{Z_1 \mapsto X_1 \oplus Z'_1,\ Z_2 \mapsto X_1 \oplus Z'_2\}, E, Ax} Z'_1 \oplus Z'_2$ and this can be repeated infinitely often. This equational theory has the boundedness property, as it is shown to have FV in Example 26 below. A bound for this theory is the number of $\oplus$ symbols in the term, so that the narrowing tree can be restricted to depth 1 for the term $t = Z_1 \oplus Z_2$. Let us explain in detail why the bound is the number of $\oplus$ symbols. Given the narrowing sequence*

$$Z_1 \oplus Z_2 \rightsquigarrow_{\{Z_1 \mapsto X_1 \oplus Z'_1, Z_2 \mapsto X_1 \oplus Z'_2\}, E, Ax} Z'_1 \oplus Z'_2 \rightsquigarrow_{\{Z'_1 \mapsto X'_1 \oplus Z''_1, Z'_2 \mapsto X'_1 \oplus Z''_2\}, E, Ax} Z''_1 \oplus Z''_2 \tag{11}$$

we have the variant $(Z_1'' \oplus Z_2'', \rho)$ *with* $\rho = \{Z_1 \mapsto X_1 \oplus X_1' \oplus Z_1'', Z_2 \mapsto X_1 \oplus X_1' \oplus Z_2'', Z_1' \mapsto X_1' \oplus Z_1'', Z_2' \mapsto X_1' \oplus Z_2''\}$. *Also, the normalization sequence corresponding to* $t\rho$ *that mimics the narrowing sequence* (11) *is*

$$X_1 \oplus X_1' \oplus Z_1'' \oplus X_1 \oplus X_1' \oplus Z_2'' \to_{E,Ax} X_1' \oplus Z_1'' \oplus X_1' \oplus Z_2'' \to_{E,Ax} Z_1'' \oplus Z_2'' \tag{12}$$

However, we can also reduce $t\rho$ *to the same normal form of* (12) *using only one application of* (8) *and the following normalized substitution* $\rho = \{X \mapsto X_1 \oplus X_1', Y \mapsto Z_1'' \oplus Z_2''\}$*:*

$$X_1 \oplus X_1' \oplus Z_1'' \oplus X_1 \oplus X_1' \oplus Z_2'' \to_{E,Ax} Z_1'' \oplus Z_2'' \tag{13}$$

The trick is that rule (8) *allows combining all pairs of canceling terms and thus gets rid of all of them at once. That is why the theory has the finite variant property.*

At this point, we have three different ways of computing variants that we would like to discuss with some examples:

1. Computing the narrowing tree associated to a term t up to the bound $\#_{E,Ax}(t)$ and extracting the variants from the narrowing tree.
2. Computing the narrowing tree using $Full_{\mathcal{R}}^{\circlearrowleft}$ and extracting the variants from the narrowing tree.
3. Computing the narrowing tree using $VN_{\mathcal{R}}^{\circlearrowleft}$ and extracting the variants from the narrowing tree.

$VN_{\mathcal{R}}^{\circlearrowleft}$ is the best approach, since the other two approaches are cruder and can be massively inefficient. This can be illustrated as follows.

Example 17. *Consider again Example 3 and the term* $u = X \oplus Y \oplus X \oplus Y$*, whose most general variant is* $(0, id)$*. As explained in Example 11, this term can be normalized in one rewriting step. However, the approaches* (1)–(3) *work very differently.*

1. *Since we showed that the narrowing bound is the number of* $\oplus$ *symbols, we have* $\#_{E,Ax}(u) = 3$*. The full narrowing tree up to bound* 3 *is huge and we do not include it here (see Examples 5, 9, and 11).*
2. $Full_{\mathcal{R}}^{\circlearrowleft}$ *will behave a little better by producing only narrowing sequences of length* 1*, since it will compute the rewriting step to the term* 0 *among the* 150 *narrowing steps, but all these extra narrowing steps are unnecessary. Again, we are not including here the* $Full_{\mathcal{R}}^{\circlearrowleft}$ *narrowing tree (see Examples 5, 9, and 11).*
3. $VN_{\mathcal{R}}^{\circlearrowleft}$ *performs just one rewriting step to the normal form, being optimal in both length and number of sequences (see Example 11).*

In the following section, we study conditions for checking whether a theory has the finite variant property or not.

6.2. Necessary and Sufficient Conditions for FV

Deciding whether an equational theory has the finite variant property is a nontrivial task, since we have to decide whether we can stop generating normalized substitution instances by narrowing for each term. We present here an algorithm for checking whether a decomposition of an equational theory has the finite variant property (FV) which is based on two notions: (i) a new

notion, called *variant-preservingness* (VP), that ensures that an intuitive bottom-up generation of variants is complete; and (ii) the property that there are no infinite sequences when we restrict ourselves to such intuitive bottom-up generation of variants (FVNS). In what follows, we show that $(VP \wedge FVNS) \Rightarrow FV$. Note that the folding variant narrowing $VN_{\mathcal{R}}^{\circlearrowleft}$ will be used for effectively computing the variants but a different narrowing strategy will be used for a bottom-up generation of variants in the procedure of detecting whether a theory has the finite variant property (FV).

Variant-preservingness (VP) ensures that we can perform an intuitive bottom-up generation of variants. The following notion is useful for the definition of VP.

Definition 25 (Variant-pattern). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of $(\Sigma, \mathcal{E})$. We call a term $f(t_1, \ldots, t_n)$ a* variant-pattern *if all subterms $t_1, \ldots, t_n$ are $\rightarrow_{E,Ax}$-irreducible. We say that a term t* has *a variant-pattern if there is a variant-pattern t' s.t. $t' =_{Ax} t$.*

It is worth pointing out that whether a term has a variant-pattern is decidable, assuming a finitary and complete Ax-matching procedure: given a term t, t has a variant-pattern t' iff there is a symbol $f \in \Sigma$ with arity k and variables $X_1, \ldots, X_k$ of the appropriate top sorts and there is a substitution θ such that $t =_{Ax} f(X_1, \ldots, X_k)\theta$ and θ is E, Ax-normalized, where $t' = f(X_1, \ldots, X_k)\theta$. We can simplify this procedure when term t is rooted by an AC symbol to say that we only have to consider the same AC symbol at the root of t, instead of every symbol. And we can simplify this procedure even more when term t is rooted by a free function symbol (i.e., such a symbol does not satisfy any axiom of Ax) to say that t has a variant-pattern if it is already a variant-pattern, i.e., every argument of the root symbol must be E, Ax-irreducible.

Variant-preservingness induces a bottom-up variant generation; note that a bottom-up variant generation is not the same as innermost narrowing.

Definition 26 (Variant-preserving). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of $(\Sigma, \mathcal{E})$. We say that $\mathcal{R}$ is* variant-preserving *(VP) if for any variant-pattern t, either t is $\rightarrow_{E,Ax}$-irreducible or there is a $\rightarrow_{E,Ax}$ step at the top position with a $\rightarrow_{E,Ax}$-normalized substitution.*

Note that a theory can have the finite variant property even if it is not variant-preserving.

Example 18. *Consider the decomposition of Example 12. This theory does not have the variant-preserving property, e.g., given the term $t = f(X, Y)$ and any normalized substitution $\theta \in \{X \mapsto f(a^n), Y \mapsto f(b^n, Z)\}$ for $n \geq 2$, there is no normalized reduction for $t\theta$. However, the theory does have the boundedness property, and therefore FV, since for any term rooted by f (which is the only non-constant symbol), its normal form can be obtained in at most one step.*

The following example motivates why narrowing sequences have to be restricted for a bottom-up variant generation.

Example 19. *Consider the decomposition $f(f(X)) = X$ without axioms. This theory is well-known to be non-terminating for narrowing, e.g.,*

$$c(f(X), X) \rightsquigarrow_{\{X \mapsto f(X')\}, E, Ax} c(X', f(X')) \rightsquigarrow_{\{X' \mapsto f(X'')\}, E, Ax} c(f(X''), X'') \cdots$$

Although the theory is non-terminating for narrowing, it is FV. When we consider all possible instances of the term $c(f(X), X)$ for normalized substitutions, we obtain the term $c(f(X), X)$ itself and the sequence $c(f(X), X) \rightsquigarrow_{\{X \mapsto f(X')\}, E, Ax} c(X', f(X'))$. The theory does have the boundedness property, and therefore FV, since for any term t and a normalized substitution θ, a bound for t is the number of f symbols in the term.

Therefore, for a bottom-up generation of variants in a finite decomposition, not all the narrowing sequences are relevant, as shown in the previous example, and thus we must identify the relevant ones associated to the notion of variant pattern.

Definition 27 (Shortest Rewrite Sequence). *Given a decomposition* (Σ, Ax, E)*, a rewrite sequence* $t_0 \to_{p_1,E,Ax} t_1 \cdots \to_{p_n,E,Ax} t_n$ *is called* shortest *if there is no sequence* $t_0 \to^m_{E,Ax} t'_m$ *such that* $m < n$ *and* $t_n =_{Ax} t'_m$*.*

Definition 28 (Variant-preserving sequences). *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of* $(\Sigma, \mathcal{E})$*. A rewrite sequence* $\alpha : t_0 \to_{p_1,E,Ax} t_1 \cdots \to_{p_n,E,Ax} t_n$ *is called* variant-preserving *if, for* $i \in \{1, \ldots, n\}$*,* $t_{i-1}|_{p_i}$ *has a variant-pattern and* α *is a shortest rewrite sequence. A narrowing sequence* $t_0 \rightsquigarrow_{p_1,\sigma_1,E,Ax} t_1 \cdots \rightsquigarrow_{p_n,\sigma_n,E,Ax} t_n$*,* $\sigma = \sigma_1 \cdots \sigma_n$*, is called* variant-preserving *if* σ *is* E, Ax*-normalized and* $t_0\sigma \to_{p_1,E,Ax} t_1\sigma \cdots \to_{p_n,E,Ax} t_n$ *is variant-preserving.*

The set of variant-preserving sequences is not computable in general. However, we provide sufficient conditions in Section 7. Note that we are not going to use variant-preserving narrowing sequences for computing variants but only for deciding whether a theory has the finite variant property.

Example 20. *The infinite narrowing sequence of Example 19 is not variant-preserving, since for any finite prefix of length greater than* 1 *the computed substitution is non-normalized. The only variant-preserving sequences for the term* $c(f(X), X)$ *are the term itself and the one-step sequence with substitution* $\{X \mapsto f(X')\}$*.*

Example 21. *For Example 3, the narrowing sequence*

$$Z_1 \oplus Z_2 \rightsquigarrow_{\{Z_1 \mapsto X_1 \oplus Z'_1, Z_2 \mapsto X_1 \oplus Z'_2\}, E, Ax} Z'_1 \oplus Z'_2 \rightsquigarrow_{\{Z'_1 \mapsto X'_1 \oplus Z''_1, Z'_2 \mapsto X'_1 \oplus Z''_2\}, E, Ax} Z''_1 \oplus Z''_2$$

is not a variant-preserving sequence, since the alternative rewrite sequence $X_1 \oplus X'_1 \oplus Z''_1 \oplus X_1 \oplus X'_1 \oplus Z''_2 \to_{E,Ax} Z''_1 \oplus Z''_2$ *is shorter.*

The following result provides sufficient conditions for the finite variant property.

Theorem 7 (Sufficient conditions for FV). *Let* $\mathcal{R} = (\Sigma, E, R)$ *be a decomposition of* $(\Sigma, \mathcal{E})$*. If (i)* $\mathcal{R}$ *is variant-preserving (VP), and (ii) there is no infinite variant-preserving narrowing sequence (FVNS), then* $\mathcal{R}$ *satisfies the finite variant property.*

Proof. *Since we assume that the* Ax *unification algorithm is finitary, and therefore the narrowing tree is finitely branching, by König's Lemma the tree of variant-preserving narrowing sequences is finite. Given a term* t*, we denote by* $\#(t)$ *the length of the longest variant-preserving narrowing sequence from* t*. We prove that, for any substitution* σ*,* $t(\sigma\downarrow_{E,Ax}) \to^{\leq n}_{E,Ax} (t\sigma)\downarrow_{E,Ax}$ *by induction on* $n = \#(t)$*.*

- $(n = 0)$ *Then* t *is irreducible and, for any substitution* σ*,* $t(\sigma\downarrow_{E,Ax})$ *is also irreducible.*
- $(n > 0)$ *Let* $t = f(t_1, \ldots, t_k)$ *and* σ *be a substitution. Let us assume that* $t\sigma$ *is eventually reduced at the top in every variant-preserving rewrite sequence. Otherwise, we can prove by structural induction and the boundedness property that the bound for* t *is the sum of the bounds for the arguments* $t_1, \ldots, t_k$*. We have* $\#(t_i) < \#(t)$*. By induction hypothesis, for any substitution* σ*,* $t_i(\sigma\downarrow_{E,Ax})$ *is bounded by* $\#(t_i)$ *for* $i \in \{1, \ldots, k\}$*. Let us pick any variant*

(t'_i, ρ_i) *for each* t_i, $i \in \{1, \ldots, k\}$ *such that* $\sigma \sqsubseteq_{Ax} (\rho_1 \cdots \rho_k)$. *Let* $t' = f(t'_1, \ldots, t'_k)$. *By variant-preservingness, there is a rule* $l \to r \in E$ *and a normalized substitution* θ *such that* $t' =_{Ax} l\theta$. *Since* $\#(r) < \#(t)$, *we can apply the induction hypothesis and, for any substitution* σ', $r(\sigma'{\downarrow_{E,Ax}})$ *is bounded by* $\#(r)$. *Since* θ *is normalized,* $r\theta$ *is also bounded by* $\#(r)$. *Note that* $\#(t_1) + \cdots + \#(t_k) + \#(t_r) < \#(t)$. *Thus, for any substitution* σ, $t\sigma$ *is bounded by* $\#(t)$. □

Note that variant-preservingness is not a *necessary* condition for FV, as shown in Example 18. However, there are many theories where lack of variant preservingness causes loss of FV, as illustrated below.

Example 22. *Consider again Example 3, which as we show in Example 26 below is an FV decomposition, but let us assume now that some variables in rules* (7) *and* (8) *of that example are restricted to a subsort* Element, *so that they cannot match any term rooted by* $\oplus$. *That is, we have two sorts* Xor *and* Element *such that* $\_\oplus\_ : \mathsf{Xor}\ \mathsf{Xor} \to \mathsf{Xor}$ *and all other symbols* a, b, 0, $pk(\_,\_)$, *and* $sk(\_,\_)$ *are defined on sort* Element *and not on sort* Xor. *The new equations are as follows:*

$$X{:}\mathsf{Xor} \oplus 0 \;=\; X{:}\mathsf{Xor} \qquad\qquad X{:}\mathsf{Element} \oplus X{:}\mathsf{Element} \;=\; 0 \tag{14}$$

$$X{:}\mathsf{Element} \oplus X{:}\mathsf{Element} \oplus Y{:}\mathsf{Xor} \;=\; Y{:}\mathsf{Xor} \tag{15}$$

Let us consider the term $t = a \oplus (b \oplus (a \oplus b))$. *Rule* (14) *cannot be applied at any position, and only rule* (15) *can be applied at the top. However, there is no possible application with a normalized substitution and thus term* t *cannot be reduced to its normal form in one step, i.e.,* $a \oplus (b \oplus (a \oplus b)) \to_{E,Ax} b \oplus b \to_{E,Ax} 0$. *Indeed, note that given a term* $s = X{:}\mathsf{Xor} \oplus Y{:}\mathsf{Xor}$ *and any normalized substitution* σ, *the number of reduction steps for* $s\sigma$ *to reach its normal form clearly depends on the number of* $\oplus$ *symbols introduced by* σ, *and therefore this modified example fails to satisfy FV.*

Although VP is not a necessary condition, the absence of infinite variant-preserving narrowing sequences is a *necessary* condition for FV.

Theorem 8 (Necessary condition for FV). *Let* $\mathcal{R} = (\Sigma, E, R)$ *be a decomposition of* $(\Sigma, \mathcal{E})$. *If there is an infinite variant-preserving narrowing sequence, then* $\mathcal{R}$ *does not have the finite variant property.*

Proof. *Let us consider an infinite variant-preserving narrowing sequence. We can take any finite prefix* $t \rightsquigarrow^*_{\sigma,E,Ax} s$ *and build a variant-preserving rewrite sequence* $t\sigma \to^*_{E,Ax} (t\sigma){\downarrow_{E,Ax}}$. *Note that* $\sigma|_{Var(t)}$ *is* E, Ax*-normalized by definition. Thus, we obtain an infinite number of rewrite sequences with increasing length. Since the theory is terminating for rewriting and the computed substitutions are normalized, the rewrite sequences are increasing in length because the computed substitutions are increasing in depth. Since these rewrite sequences are the shortest ones, this contradicts the boundedness property.* □

7. Checking the Finite Variant Property

In the following we show that the property of being variant-preserving is clearly checkable, but the absence of infinite variant-preserving narrowing sequences is not computable in general. In Section 7.2, we approximate the absence of infinite variant-preserving narrowing sequences by a checkable condition using the dependency pairs technique of [24] for the modulo case.

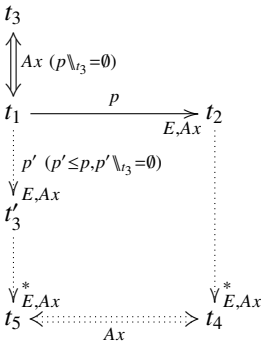


Figure 2: Upper-Ax-coherence

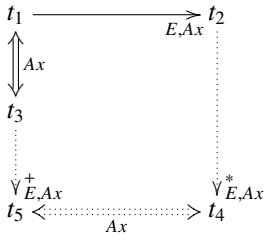


Figure 3: Ax-coherence

7.1. Checking Variant-Preservingness

The following class of equational theories is relevant. The notion of *Ax-descendants* is a straightforward extension of the standard notion of descendant for rules.

Definition 29 (Descendants). [46] *Let $A : t \xrightarrow{p}_{l\to r} s$ and $q \in Pos(t)$. The set $q\backslash\backslash A$ of descendants of q in s w.r.t. A is defined as follows:*

$$q\backslash\backslash A = \begin{cases} \{q\} & \text{if } q < p \text{ or } q \parallel p \text{ (i.e., } q \not\leq p \text{ and } p \not\leq q), \\ \{p.p_3.p_2 \mid r|_{p_3} = l|_{p_1}\} & \text{if } q = p.p_1.p_2 \text{ with } p_1 \in Pos_{\mathcal{X}}(l), \text{i.e., } p_1 \text{ is a variable position} \\ \emptyset & \text{otherwise.} \end{cases}$$

If $Q \subseteq Pos(t)$ then $Q\backslash\backslash A$ denotes the set $\bigcup_{q\in Q} q\backslash\backslash A$. The notion of descendant extends to rewrite sequences in the obvious way. If Q is a set of pairwise disjoint positions in t and $A : t \to^* s$, then the positions in $Q\backslash\backslash A$ are pairwise disjoint. The notion of descendant is extended to an equational theory Ax as follows.

Definition 30 (Ax-descendants). *Let Ax be a set of regular and sort-preserving Σ-equations. Let $\overleftrightarrow{Ax} = \{u \to v \mid u = v \text{ or } v = u \in Ax\}$. Given two terms $t =_{Ax} s$, i.e., $A : t \to^*_{\overleftrightarrow{Ax}} s$, and a set Q of pairwise disjoint positions in t, the Ax-*descendants *of Q in s are $Q\backslash\backslash_s = Q\backslash\backslash A$.*

Now we can introduce the relevant notion of upper-Ax-coherence, depicted in Figure 2. Note that dotted arrows imply they are involved in an existential quantifier.

Definition 31 (Upper-Ax-coherence). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of $(\Sigma, \mathcal{E})$. We say $\mathcal{R}$ is* upper-Ax-coherent *iff for all t_1, t_2, t_3, $t_1 \xrightarrow{p}_{E,Ax} t_2$, $t_1 =_{Ax} t_3$, $p > \wedge$, and $p\backslash\backslash_{t_3} = \emptyset$ imply that for all $p' \leq p$ such that $p'\backslash\backslash_{t_3} = \emptyset$, there exist t'_3, t_4, t_5 such that $t_1 \xrightarrow{p'}_{E,Ax} t'_3$, $t_2 \to^*_{E,Ax} t_4$, $t'_3 \to^*_{E,Ax} t_5$, and $t_4 =_{Ax} t_5$.*

Assuming Ax-coherence (defined by Condition (4) in Section 2.1 and depicted in Figures 1 and 3, both identical but using R,Ax or E,Ax labels), checking upper-Ax-coherence consists in considering each term t in each equation $t = t' \in Ax$ (or its reverse), finding a position $p \in Pos(t)$ s.t. $p > \wedge$ and a substitution σ s.t. $t\sigma|_p$ is $\to_{E,Ax}$-reducible and then, if $p = p_1.\cdots.p_k$, then, for $i \in \{1, \ldots, k-1\}$, $t\sigma|_{p_i}$ must be $\to_{E,Ax}$-reducible. In general, upper-Ax-coherence is much more demanding than Ax-coherence, as shown below.

Example 23. *Let us consider the equational theory* $E = \{g(f(X)) \to d,\ a \to c\}$ *and* $Ax = \{g(f(f(a))) = g(b)\}$. *For the term* $t = g(f(f(a)))$, *subterm* a *is reducible,* $t =_{Ax} g(b)$, *but subterms* $f(f(a))$ *and* $f(a)$ *are not reducible and thus the theory is not upper-Ax-coherent. However, the theory is trivially Ax-coherent because of the use of symbol* g *at the top of both sides of the equation in Ax.*

Note that upper-AC-coherence and AC-coherence coincide, since the axioms of associativity and commutativity can never satisfy $t_1 =_{AC} t_3$, $p > \wedge$, and $p\backslash\backslash_{t_3} = \emptyset$. We can now provide an algorithm for checking variant-preservingness.

Theorem 9 (Checking Variant-preservingness). *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of* $(\Sigma, \mathcal{E})$ *that is upper-Ax-coherent.* $\mathcal{R}$ *has the variant-preserving property iff for all* $l \to r, l' \to r' \in E$ *(possibly renamed s.t.* $Var(l) \cap Var(l') = \emptyset$*) and for each* $X \in Var(l)$, *the term* $t = l\theta$, *where* $\theta = \{X \mapsto l'\}$ *is an order-sorted substitution, satisfies that either: (i)* t *does not have a variant-pattern, or (ii) otherwise there is a normalized reduction on* t.

Proof. *The only if part is immediate by definition. For the if part, we consider a term* $t = f(t_1, \ldots, t_k)$ *such that* $t_1, \ldots, t_k$ *are* $\to_{E,Ax}$*-irreducible terms. If* t *is* $\to_{E,Ax}$*-irreducible, we are done. Otherwise, there is a rule* $l \to r \in E$ *and a substitution* θ *such that* $t = l\theta$. *If* θ *is* $\to_{E,Ax}$*-normalized, we are done. Otherwise, we prove below that there is a rule* $l' \to r' \in E$ *and a substitution* θ' *such that* $t = l'\theta'$ *and* θ' *is* $\to_{E,Ax}$*-normalized.*

Let $l \to r \in E$ *and* θ *be such that* θ *has the maximum number of redexes possible for* t. *Let* n *be such a maximum number. We prove the fact by induction on* n.

($n = 0$) *This means that* θ *is* $\to_{E,Ax}$*-normalized and we are done.*

($n > 0$) *Let* $X \mapsto u$ *be one of the non-normalized bindings in* θ. *Let* p *be one of the topmost positions in* u *with an actual redex, i.e., there is a rule* $\hat{l} \to \hat{r} \in E$ *and a substitution* σ *such that* $u|_p =_{Ax} \hat{l}\sigma$. *We can take the maximum prefix* $\hat{u}$ *of* u *with no redexes and build a substitution* $\hat{\theta} = \{X \mapsto \hat{u}[\hat{l}]_p\}$. *Let us assume that* $\hat{u}[\hat{l}]_p$ *is properly renamed so that* $Var(\hat{u}[\hat{l}]_p) \cap Var(l) = \emptyset$. *There is a substitution* ρ *such that* $\theta =_{Ax} \hat{\theta}\rho$. *Since the terms* $t_1, \ldots, t_k$ *are irreducible,* $\hat{l}$ *is not a subterm of any of them and there is a context* $C[\ ]$ *of* t *and another context* $\hat{C}[\ ]$ *of* $l\hat{\theta}$ *such that* $C[\ ] =_{Ax} \hat{C}[\ ]$ *and* $\hat{l}$ *must overlap with* $\hat{C}[\ ]$. *Then,* $p = \wedge$, *because of coherence, i.e., if* $u|_p$ *is a redex, then* u *must also be a redex. Just note that a coherence completion algorithm adds rules of the form* $C[l\sigma] \to C[r\sigma]$ *for any rule* $l \to r$ *where* $C[\ ]$ *and* σ *are determined by the equational theory Ax. Now, by the condition given in the Theorem, there is a normalized substitution on* $l\hat{\theta}$, *i.e., there is a rule* $l' \to r'$ *and a substitution* τ *such that* $l\hat{\theta} =_{Ax} l'\tau$ *and* τ *is* $\to_{E,Ax}$*-normalized. Finally, when we consider the term* $l'\tau\rho$, *we can apply the induction hypothesis because* ρ *contains less redexes than* θ *and obtain that there is a rule* $l'' \to r''$ *and a substitution* τ' *such that* $t =_{Ax} l'\tau\rho =_{Ax} l''\tau'$ *and* τ' *is* $\to_{E,Ax}$*-normalized.* □

The upper-Ax-coherence condition is necessary, as shown below.

Example 24. *The theory of Example 23 satisfies the conditions of Theorem 9 except upper Ax-coherence. That is, when the left-hand sides* $g(f(X))$ *and* a *are used to build the term* $g(f(a))$, *this term does not have a variant-pattern, as required by Theorem 9. Similarly, when the properly renamed left-hand sides* $g(f(X))$ *and* $g(f(X'))$ *are used to build the term* $g(f(g(f(X'))))$, *this*

term does not have a variant-pattern either. However, according to Definition 26, we have to test also the variant-pattern $g(b)$. Although this term is reducible, it is not $\rightarrow_{E,Ax}$-reducible with a normalized substitution. Thus the equational theory is not variant-preserving.

Let us first show another example of a theory that is not variant-preserving.

Example 25. *Let us consider again Example 12. Let us check this rewrite theory with the condition from Theorem 9. Using the rule given with the renamed version $f(a, b, X') \rightarrow f(a, b)$ we get $l\theta = f(a, b, a, b, X')$, which has a variant-pattern, namely $f(f(a, a, X'), f(b, b))$ where the extra appearances of f inside are to show which are the irreducible subterms. Also, there is no reduction with a normalized substitution, since the only reduction possible is by using the given rule, with X renamed to V and the substitution $\sigma = \{V \mapsto f(a, b, X')\}$ which is not normalized. So this theory is not variant-preserving.*

Let us prove that the exclusive or theory has the the variant-preservingness property.

Example 26. *Let $\mathcal{R} = (\Sigma, E, R)$ be the exclusive or theory from Example 3, with only* (6)–(8) *used as rules. Using Theorem 9 we find that this theory is variant-preserving. All the combinations of rules not involving* (8) *as the first rule do not have a variant-pattern, let us just show one of the combinations of rule* (8) *with itself where $l = X \oplus X \oplus Y$ and $l' = X' \oplus X' \oplus Y'$. We get two terms, one for each of the substitutions $\theta_1 = \{X \mapsto l'\}$ and $\theta_2 = \{Y \mapsto l'\}$. We get $l\theta_1 = X' \oplus X' \oplus Y' \oplus X' \oplus X' \oplus Y' \oplus Y$, which does not have a variant-pattern. On the other hand, $l\theta_2 = X \oplus X \oplus X' \oplus X' \oplus Y'$ does have a variant-pattern, but has also a normalized reduction with another renaming of rule* (8)*, namely $V \oplus V \oplus W \rightarrow W$, and substitution $\sigma = \{V \mapsto X \oplus X', W \mapsto Y'\}$. Note that the theory has the finite variant property (FV), since it is VP and the right hand sides of all the equations are constants or variables, which trivially satisfies the FVNS property.*

7.2. Checking Finiteness of Variant-Preserving Narrowing Sequences

In this section, we approximate the absence of infinite variant-preserving narrowing sequences by a checkable condition using the dependency pairs technique of [24] for the modulo case. Note that we do not really extend the dependency pairs technique to narrowing, since we do not allow extra variables in right-hand sides of rules; see [1] for an extension of the dependency pairs technique to narrowing, and [40] for termination of narrowing using the dependency pair technique. Termination of narrowing is a much harder problem than that of termination of rewriting [2] and we do not prove that narrowing or folding variant narrowing terminate; indeed recall that we are only interested in termination of the variant generation process rather than termination of narrowing strategies in general. In this section, we reuse the dependency pair technique and approximate the property of the absence of infinite variant-preserving narrowing sequences by avoiding any possible cycle in function calls. For avoiding cycles we use the dependency graph and adapt the notion of dependency pair chain to the variant case.

First, we need to extend the notion of a defined symbol. An equation $u = v$ is called *collapsing* if $v \in \mathcal{X}$ or $u \in \mathcal{X}$. We say a theory is *collapse-free*[3] if all its equations are non-collapsing.

[3]Note that regularity does not imply collapse-free, e.g., equation (6) of Example 3 is regular but also collapsing. Note also that if Ax contains collapsing axioms such as the identity axiom (6), it may be possible to use the variant based technique in [14] (see also the discussion in Section 9) to transform a decomposition (Σ, Ax, R) into a semantically equivalent one $(\Sigma, Ax_0, R \cup \overrightarrow{A}_{clps})$ where Ax_0 is collapse-free and $\overrightarrow{A}_{clps}$ are rewrite rules for the collapse axioms.

Definition 32 (Defined Symbols for Rewriting Modulo Equations). [24] *Let* (Σ, Ax, R) *be an order-sorted rewrite theory with* Ax *collapse-free. Then the set of defined symbols* D *is the smallest set such that* $D = \{root(l) \mid l \to r \in R\} \cup \{root(v) \mid u = v \in Ax \text{ or } v = u \in Ax, root(u) \in D\}$.

In order to correctly approximate the dependency relation between defined symbols in the theory, we need to extend the equational theory in the following way.

Definition 33 (Adding Instantiations). [24] *Given an order-sorted rewrite theory* $\mathcal{R} = (\Sigma, Ax, R)$ *with* Ax *collapse-free, let* $Ins_{Ax}(R)$ *be a set containing only rules of the form* $l\sigma \to r\sigma$ *(where* σ *is a substitution and* $l \to r \in R$*). *$Ins_{Ax}(R)$* is called an instantiation of* R *for the equations* Ax *iff* $Ins_{Ax}(R)$ *is the smallest set such that: (a)* $R \subseteq Ins_{Ax}(R)$*, (b) for all* $l \to r \in R$*, all* v *such that* $u = v \in Ax$ *or* $v = u \in Ax$*, and all* $\sigma \in CSU_{Ax}(v = l)$*, there exists a rule* $l' \to r' \in Ins_{Ax}(R)$ *and a variable renaming* ρ *such that* $l\sigma =_{Ax} l'\rho$ *and* $r\sigma =_{Ax} r'\rho$.

Note that when $Ax = \emptyset$ or Ax contains only AC or C axioms, $Ins_{Ax}(R) = R$. Dependency pairs are obtained as follows. Since we are dealing with the modulo case, it will be notationally more convenient to use terms directly in dependency pairs, without the usual capital letters for the top symbols.

Definition 34 (Dependency Pair). [24] *Let* $\mathcal{R} = (\Sigma, Ax, R)$ *be an order-sorted rewrite theory with* Ax *collapse-free. Let* $Ins_{Ax}(R)$ *be the instantiations of* R *for the equations* Ax*. If* $l \to C[g(t_1, \ldots, t_m)]$ *is a rule of* $Ins_{Ax}(R)$ *with* C *a context and* g *a defined symbol in* $Ins_{Ax}(R)$*, then* $\langle l, g(t_1, \ldots, t_m)\rangle$ *is called a* dependency pair *of* $\mathcal{R}$.

Example 27 (Abelian Group). *The following presentation of the Abelian group theory, called* $\mathcal{R}_* = (\Sigma, Ax, E)$*, has been shown to satisfy the finite variant property in [11]. The operators* Σ *are* $\_*\_$*,* $(\_)^{-1}$*, and* 1*. The set of equations* Ax *consists of associativity and commutativity for* $\_*\_$*. The rules* E *are:*

$$
\begin{array}{rcll}
x * 1 & \to & x & (16)\\
1^{-1} & \to & 1 & (17)\\
x * x^{-1} & \to & 1 & (18)\\
x^{-1} * y^{-1} & \to & (x * y)^{-1} & (19)\\
(x * y)^{-1} * y & \to & x^{-1} & (20)
\end{array}
\qquad
\begin{array}{rcll}
x^{-1^{-1}} & \to & x & (21)\\
(x^{-1} * y)^{-1} & \to & x * y^{-1} & (22)\\
x * (x^{-1} * y) & \to & y & (23)\\
x^{-1} * (y^{-1} * z) & \to & (x * y)^{-1} * z & (24)\\
(x * y)^{-1} * (y * z) & \to & x^{-1} * z & (25)
\end{array}
$$

The AC-dependency pairs for this rewrite theory are as follows.

$$
\begin{array}{llll}
(19)a: & \langle x^{-1} * y^{-1} \,,\, (x * y)^{-1}\rangle & (19)b: & \langle x^{-1} * y^{-1} \,,\, x * y\rangle\\
(22)a: & \langle (x^{-1} * y)^{-1} \,,\, x * y^{-1}\rangle & (22)b: & \langle (x^{-1} * y)^{-1} \,,\, y^{-1}\rangle\\
(24)a: & \langle x^{-1} * y^{-1} * z \,,\, (x * y)^{-1} * z\rangle & (24)b: & \langle x^{-1} * y^{-1} * z \,,\, (x * y)^{-1}\rangle\\
(24)c: & \langle x^{-1} * y^{-1} * z \,,\, x * y\rangle & (20)a: & \langle (x * y)^{-1} * y \,,\, x^{-1}\rangle\\
(25)a: & \langle (x * y)^{-1} * y * z \,,\, x^{-1} * z\rangle & (25)b: & \langle (x * y)^{-1} * y * z \,,\, x^{-1}\rangle
\end{array}
$$

We have used the AProVE tool [25] to generate the dependency pairs. AProVE first applies the coherence algorithm of [24] to this example, which is unnecessary here and thus we drop the dependency pairs created that way.

The relevant notions from the dependency pairs technique are chains of dependency pairs and the dependency graph.

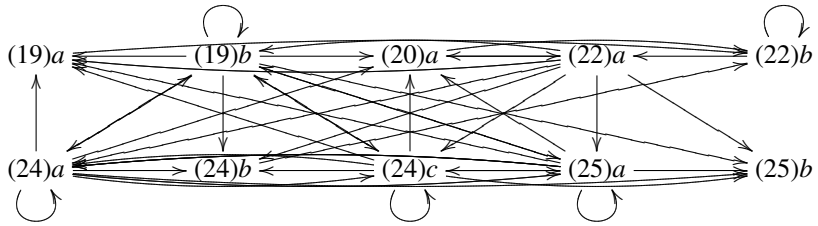


Figure 4: Dependency graph of Abelian group

Definition 35 (Chain). [8] *Let $\mathcal{R} = (\Sigma, Ax, R)$ be an order-sorted rewrite theory with Ax collapse-free. A sequence of dependency pairs $\langle s_1, t_1\rangle\langle s_2, t_2\rangle \cdots \langle s_n, t_n\rangle$ of $\mathcal{R}$ is an* $\mathcal{R}$-chain *if there is a substitution σ such that $t_j\sigma \to^*_{R,Ax} s_{j+1}\sigma$ holds for every two consecutive pairs $\langle s_j, t_j\rangle$ and $\langle s_{j+1}, t_{j+1}\rangle$ in the sequence.*

Definition 36 (Dependency Graph). [8] *Let $\mathcal{R} = (\Sigma, Ax, R)$ be an order-sorted rewrite theory with Ax collapse-free. The dependency graph of $\mathcal{R}$ is the directed graph whose nodes (vertices) are the dependency pairs of R and there is an arc (directed edge) from $\langle s, t\rangle$ to $\langle u, v\rangle$ if $\langle s, t\rangle\langle u, v\rangle$ is a chain.*

Chains are not computable in general and an approximation must be performed. The notions of *connectable terms* and the *estimated dependency graph* as defined in [8] provide a useful approximation of the dependency graph. The estimated dependency graph can be computed using the Cap and Ren procedures [8]: For any term $t \in \mathcal{T}_\Sigma(\mathcal{X})$, let Cap($t$) replace each proper subterm rooted by a defined symbol by a fresh variable and let Ren(t) independently rename all occurrences of variables in t by fresh variables. Note that such an estimated dependency graph has been used in all examples in this section.

Example 28. *The dependency graph for Example 27 is shown in Figure 4. It was created with AProVE [25]. We see that there are self-loops on* (19)*b,* (22)*b,* (24)*a,* (24)*c and* (25)*a.* (19)*a has a loop with* (22)*a,* (22)*a has a loop with* (24)*b, and so on. It is a very highly connected graph.*

The most important notion for the absence of infinite narrowing sequences is that of a cycle in the dependency graph.

Definition 37 (Cycle). [8] *A nonempty set $\mathcal{P}$ of dependency pairs is called a* cycle *if, for any two dependency pairs $\langle s, t\rangle, \langle u, v\rangle \in \mathcal{P}$, there is a nonempty path from $\langle s, t\rangle$ to $\langle u, v\rangle$ and from $\langle u, v\rangle$ to $\langle s, t\rangle$ in the dependency graph that traverses dependency pairs from $\mathcal{P}$ only.*

As already demonstrated in the previous section, not all the rewriting (narrowing) sequences are relevant for the finite variant property, so that we can restrict the dependency graph only to variant-preserving rewriting (narrowing) sequences.

Definition 38 (Variant-preserving chain). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a variant-preserving decomposition of an equational theory $(\Sigma, \mathcal{E})$. A chain of dependency pairs $\langle s_1, t_1\rangle\langle s_2, t_2\rangle \cdots \langle s_n, t_n\rangle$ of $\mathcal{R}$ is a* variant-preserving chain *if there is a substitution σ such that σ is $\to_{E,Ax}$-normalized and the following rewrite sequence $s_1\sigma \to_{E,Ax} C_1[t_1]\sigma \to^*_{E,Ax} C_1[s_2]\sigma \to_{E,Ax} C_1[C_2[t_2]]\sigma \to^*_{E,Ax} \cdots \to^*_{E,Ax} C_1[C_2[\cdots C_{n-1}[s_n]]]\sigma \to_{E,Ax} C_1[C_2[\cdots C_{n-1}[C_n[t_n]]]]\sigma$ obtainable from the chain $\langle s_1, t_1\rangle\langle s_2, t_2\rangle \cdots \langle s_n, t_n\rangle$ is variant-preserving.*

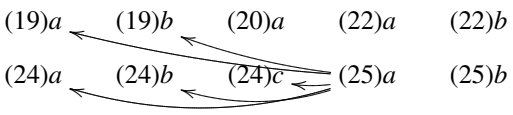


Figure 5: Variant-preserving dependency graph

The notions of a cycle, dependency graph, and estimated dependency graph are easily extended to the variant-preserving case. The following result approximates the absence of infinite narrowing sequences. We simply approximate such property by avoiding any cycle. We do not use any of the dependency pair processors of the dependency pair framework (see [8, 26]) and we do not require any term ordering. Obviously, there may be more specific techniques based on termination of narrowing for deciding the termination of variant-preserving narrowing sequences but this is left for future work.

Proposition 3 (Checking Finiteness of the VP Narrowing sequences). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a variant-preserving decomposition of an equational theory $(\Sigma, \mathcal{E})$. Let Ax contain only linear, non-collapsing equations. If the estimated dependency graph does not contain any variant-preserving cycle, then there are no infinite variant-preserving narrowing sequences.*

Proof. *We prove this result by contradiction. Assume that the estimated dependency graph does not contain any variant-preserving cycle but there is an infinite variant-preserving narrowing sequence $\alpha : t_0 \rightsquigarrow_{p_1,\sigma_1,E,Ax} t_1 \cdots \rightsquigarrow_{p_n,\sigma_n,E,Ax} t_n \cdots$. From α we can obtain an infinite number of finite variant-preserving rewrite sequences of the form $t_0\theta_i \rightarrow_{p_1,E,Ax} t_1\theta_i \cdots \rightarrow_{p_i,E,Ax} t_i\theta_i$ with $\theta_i = \sigma_1 \cdots \sigma_i$. For each variant-preserving rewrite sequence $t_0\theta_i \rightarrow_{p_1,E,Ax} t_1\theta_i \cdots \rightarrow_{p_i,E,Ax} t_i\theta_i$, there is a variant-preserving chain corresponding to such rewrite sequence. Since the number of dependency pairs is finite, there is a natural number k such that for the variant-preserving rewrite sequence $t_0\theta_k \rightarrow_{p_1,E,Ax} t_1\theta_k \cdots \rightarrow_{p_k,E,Ax} t_k\theta_k$, the variant-preserving chain associated to it is a cycle. Thus, the conclusion follows, because we assume that there is no variant-preserving cycle.* □

Note that the conditions that the axioms are non-collapsing and linear are necessary for completeness of the dependency graph, we refer the reader to [24] for explanations.

Example 29 (Abelian group variant-preserving dependency pair graph). *We can show the variant-preserving dependency graph of Example 27 in Figure 5. One can see in the picture that all the cycles have disappeared, because they involved non-normalized substitutions, or terms without a variant-pattern, or could be shortened. Detailed reasons are provided next.*

For the dependency pair (19)*b and its self-loop we need a substitution σ for which $(X * Y)\sigma =_{AC} (X'^{-1} * Y'^{-1})\sigma$. But then, e.g., $\sigma = \{X \mapsto X'^{-1}, Y \mapsto Y'^{-1}\}$ and the left-hand side of the dependency pair becomes $(X'^{-1})^{-1} * (Y'^{-1})^{-1}$, which does not have a variant-pattern, as $(X'^{-1})^{-1}$ is reducible, so the self-loop is not a variant-preserving sequence and thus not a variant-preserving chain.*

For the dependency pairs (24)*a, i.e., $\langle s_1, t_1\rangle = \langle X^{-1} * Y^{-1} * Z, (X * Y)^{-1} * Z\rangle$, and* (25)*a, i.e., $\langle s_2, t_2\rangle = \langle (X' * Y')^{-1} * Y' * Z', X'^{-1} * Z'\rangle$ let us consider both directions. For one direction we have $((X * Y)^{-1} * Z)\sigma =_{AC} ((X' * Y')^{-1} * Y' * Z')\sigma$ so for example $\sigma = \{Z \mapsto Y' * Z', X \mapsto X', Y \mapsto Y'\}$. Then $s_1\sigma =_{AC} X'^{-1} * Y'^{-1} * Y' * Z'$ which has a variant-pattern and for which the rewriting sequence is $X'^{-1} * Y'^{-1} * Y' * Z' \rightarrow (X' * Y')^{-1} * Y' * Z' \rightarrow X'^{-1} * Z'$. Nevertheless,*

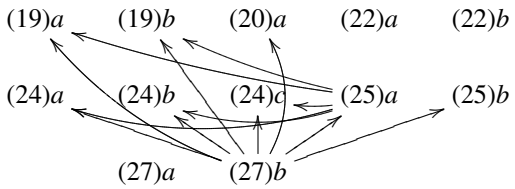


Figure 6: Variant-preserving dependency graph for Diffie-Hellman

it is not a variant-preserving sequence as there is a shorter rewriting sequence using rule (23)*,* $X'^{-1} * Y'^{-1} * Y' * Z' \to X'^{-1} * Z'$*, so there is no variant-preserving chain here.*

Similarly for the chain from (24)*a to* (25)*b as the only difference is in* t_2*, so that* $t_2\sigma = X'^{-1}$ *but that will be padded with the context of* $\_*\_([], Z')$ *(where* [] *is the hole) and so the same shorter rewriting sequence exists.*

In the other direction, from (25)*a to* (24)*a, we have* $(X'^{-1} * Z')\sigma =_{AC} (X^{-1} * Y^{-1} * Z)\sigma$ *so then for example* $\sigma = \{Z' \mapsto Y^{-1}Z, X' \mapsto X\}$ *and* $s_2\sigma =_{AC} (X * Y')^{-1} * Y' * Y^{-1} * Z$ *which has a variant-pattern and the rewriting sequence* $(X * Y')^{-1} * Y' * Y^{-1} * Z \to X^{-1} * Y^{-1} * Z \to (X * Y)^{-1} * Z$*. The alternative rewriting sequence applying the rules in reverse order is* $(X * Y')^{-1} * Y' * Y^{-1} * Z \to (X * Y' * Y)^{-1} * Y' * Z \to (X * Y)^{-1} * Z$ *which is not shorter, so this is a variant-preserving sequence and thus we have a variant-preserving chain.*

Let us first introduce a representation of the Diffie-Hellman theory and then show the VP property for the theories of Abelian groups and Diffie-Hellman exponentiation, and also the finite variant property for the Diffie-Hellman theory.

Example 30 (Diffie-Hellman). *We get a rewrite theory representing the Diffie-Hellman theory, called* $\mathcal{R}_{\mathcal{DH}}$*, by extending the theory* $\mathcal{R}_*$ *from Example 27 by adding a new binary symbol* exp *and the following two rules:*

$$exp(x, 1) \to x \tag{26}$$

$$exp(exp(x, y), z) \to exp(x, y * z) \tag{27}$$

We can compute the dependency pairs and the associated graph using the results we already have from Example 29. Also note, that the rewrite theories $\mathcal{R}_*$ *and* $\mathcal{R}_{\mathcal{DH}}$ *both have the variant-preserving property, which we will check in Example 31, respectively Example 32. The following additional dependency pairs are required:*

$$\begin{array}{lcl} (27)a & : & \langle exp(exp(x, y), z) \quad , \quad exp(x, y * z)\rangle \\ (27)b & : & \langle exp(exp(x, y), z) \quad , \quad y * z\rangle \end{array}$$

As shown in Figure 6, for rule (27) *there are a lot of possibilities to go from* (27)*b, but the longest possible path has length* 2*. Let us show that there is actually a chain for the path from* (27)*b via* (25)*a to* (19)*a. After substituting as needed for this in the left-hand side of* (27) *we get* $exp(exp(X, (U * V)^{-1}), V * W^{-1}) \to exp(X, (U * V)^{-1} * V * W^{-1})$*, let us call this term t. Then from there we have* $t \to exp(X, U^{-1} * W^{-1}) \to exp(X, (U * W)^{-1})$ *and alternatively* $t \to exp(X, (U * V * W)^{-1} * V) \to exp(X, (U * W)^{-1})$ *which is not shorter. So this is really a variant-preserving chain and the longest chain from* (27)*b is length* 2*.*

We show VP for our Abelian group representation next.

Example 31. *Let us check variant-preservingness for $\mathcal{R}_*$ by using Theorem 9. For rule* (16) *and any other rule there is no variant-pattern for $l\theta$ where θ substitutes another left-hand side into X. The reason is that the constant* 1 *needs to stay isolated, since otherwise a rewrite is possible, and so the left-hand side that was inserted stays together and is reducible. As rule* (17) *does not have any variable, the property holds trivially.*

For all following rules let us note that instantiating a variable that is a subterm of an inverse operator $^{-1}$ with a left-hand side of another rule, immediately results in a term that has no variant-pattern as that left-hand side stays together underneath. Thus the rules (18)–(22) *do not need to be considered as all variables appear at least once underneath an inverse operator.*

In this vein for rule (23) *we only need to consider the terms created when instantiating Y. Only combination with* (18),(20), (23), *and* (25) *results in a term that has a variant-pattern. Let us show for example* (23) *with* (25) *(renamed to primed variables). The resulting term is $X * X^{-1} * (X' * Y')^{-1} * Y' * Z'$ which can be reduced by rule* (24) *(renamed to doubly primed variables) with substitution $\{X'' \mapsto X, Y'' \mapsto X' * Y', Z'' \mapsto X * Y' * Z'\}$ which is normalized.*

For rule (24) *the only useful (i.e., with a chance of having a variant-pattern) instantiations are for Z, but also as there are already two appearances of a term headed by the inverse only left-hand sides with no inverse have a chance at having a variant-pattern. That only leaves rule* (16) *which results in term $X^{-1} * Y^{-1} * X' * 1$ which also does not have a variant-pattern.*

Finally, for rule (25) *we only need to instantiate the variable Z. There are variant-patterns for the combinations with* (18), (20), (23), *and* (25), *let us just show the last of these combinations,* (25) *with itself. The resulting term is $(X*Y)^{-1}*Y*(X'*Y')^{-1}*Y'*Z'$, which has a variant-pattern but also can rewrite with rule* (24) *(renamed with two primes) with the normalized substitution $\{X'' \mapsto X * Y, Y'' \mapsto X' * Y', Z'' \mapsto Y * Y' * Z'\}$.*

Therefore, $\mathcal{R}_*$ has the variant-preserving property.

Based on VP for Abelian groups we can check VP for Diffie-Hellman. It also turns out that Diffie-Hellman has the finite-variant property.

Example 32. *Variant-preservingness of the Diffie-Hellman theory $\mathcal{R}_{\mathcal{DH}}$ can be shown using Theorem 9 based upon the variant-preservingness of $\mathcal{R}_*$ shown in Example 31. Let us just observe that $\mathcal{R}_{\mathcal{DH}}$ is obtained by just adding a new symbol exp and rules for it. Putting this into any variable of any of the prior rules results in a term that has no variant-pattern. The other way around, any left-hand side put into any of the variables of the left-hand sides of one of the two new rules results in a term that has no variant-pattern. So $\mathcal{R}_{\mathcal{DH}}$ has the variant-preserving property, too.*

The proof of our final result for this section is trivial: since if there are no cycles in the estimated dependency graph, then we know for sure that there is no infinite variant-preserving rewrite sequence.

Theorem 10 (Approximation for the finite variant property). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a variant-preserving decomposition of an equational theory $(\Sigma, \mathcal{E})$ such that Ax contains only linear, non-collapsing equations. If the estimated dependency graph does not contain any variant-preserving cycle, then $\mathcal{R}$ has the finite variant property.*

Proof. *By Proposition 3 and Theorem 8.* □

7.3. Disproving the Finite Variant Property

If there are infinite variant-preserving narrowing sequences, we are done, because the finite variant property does not hold by Theorem 8. We can give a simple sufficient condition, a consequence of Theorem 8.

Theorem 11 (Non-termination of narrowing). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a variant-preserving decomposition of an equational theory $(\Sigma, \mathcal{E})$. Let Ax contain only linear, non-collapsing equations. If the estimated dependency graph does contain a variant-preserving chain $\langle s,t\rangle\langle s,t\rangle$ such that $s \sqsubseteq_{Ax} t$, called a* self-cycle*, and the* Cap *and* Ren *procedures were not necessary for obtaining term t, then there is an infinite variant-preserving narrowing sequence starting from term s.*

Proof. *The estimated dependency graph contains the chain $\langle s,t\rangle\langle s,t\rangle$ for the dependency pair $\langle s,t\rangle$. The dependency pair $\langle s,t\rangle$ comes from a rule $s \to C[t]_p$. Let σ be such that $s =_{Ax} t\sigma$. Since the* Cap *and* Ren *procedures have not been applied to term t, we have the infinite narrowing sequence $s \rightsquigarrow_{\lambda,id,E,Ax} C[t]_p \rightsquigarrow_{p,\sigma,E,Ax} C[C'[t']_p]_p \rightsquigarrow_{p.p,\sigma',E,Ax} C[C'[C''[t'']_p]_p]_p \cdots$ where C' and C'' are properly renamed versions of C, t' and t'' are properly renamed versions of t, and σ' is a properly renamed version of σ.* □

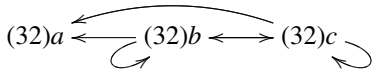
Example 33 (ACUNh). [11] *Let us present the ACU example with nilpotence and homomorphism as discussed by Comon and Delaune.*[4] *This is $\mathcal{R}_{ACUNh}$, with + AC, which has the variant-preserving property:*

$$\begin{array}{rcll} X+0 & \to & X & (28) \\ X+X & \to & 0 & (29) \\ X+X+Y & \to & Y & (30) \end{array} \qquad \begin{array}{rcll} h(0) & \to & 0 & (31) \\ h(X+Y) & \to & h(X)+h(Y) & (32) \end{array}$$

For the last rule we get three dependency pairs:

$$(32)a \;:\; \langle h(x+y) \;,\; h(x)+h(y)\rangle \qquad \begin{array}{rcl} (32)b & : & \langle h(x+y) \;,\; h(x)\rangle \\ (32)c & : & \langle h(x+y) \;,\; h(y)\rangle \end{array}$$

It is easy to see that there are self-cycles in (32)b and (32)c using the substitution $x \mapsto x_1 + z_1$, which also allows going back and forth between them. This gives rise to the following graph:



By Theorem 8, this theory does not have the finite variant property, as also proved in a different way in [11].

8. Variant-based Equational Unification

The intimate connection between variants and $\mathcal{E}$-unification is then as follows.

Definition 39. *For $\mathcal{R} = (\Sigma, Ax, E)$ with poset of sorts $(\mathsf{S}, \leq)$ being a decomposition of an equational theory $(\Sigma, \mathcal{E})$, we extend (Σ, Ax, E) and $(\mathsf{S}, \leq)$ to $(\widehat{\Sigma}, Ax, \widehat{E})$ and $(\widehat{\mathsf{S}}, \leq)$ as follows:*

1. *we add a new sort* Truth *to $\widehat{\mathsf{S}}$, not related to any sort in Σ,*

[4] There is another, alternative term rewriting system representing this theory, which suffers from the same problems.

2. *we add a constant operator* $\mathtt{tt}$ *of sort* Truth *to* $\widehat{\Sigma}$,
3. *for each top sort of a connected component* $[\mathtt{s}]$*, we add an operator* $\mathtt{eq} : [\mathtt{s}] \times [\mathtt{s}] \to \mathsf{Truth}$ *to* $\widehat{\Sigma}$*, and*
4. *for each top sort* $[\mathtt{s}]$*, we add a variable* $X{:}[\mathtt{s}]$ *and an extra rule* $\mathtt{eq}(X{:}[\mathtt{s}], X{:}[\mathtt{s}]) \to \mathtt{tt}$ *to* $\widehat{E}$.

Then, given any two Σ-terms t, t', if θ is an $\mathcal{E}$-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 $(\mathtt{tt}, \theta)$ must be a variant of the term $\mathtt{eq}(t, t')$. Furthermore, if the term $\mathtt{eq}(t, t')$ 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*.

Corollary 7. *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *with poset of sorts* $(\mathsf{S}, \leq)$ *be a finite variant decomposition of an equational theory* $(\Sigma, \mathcal{E})$*. The equational theory* $(\widehat{\Sigma}, Ax, \widehat{E})$ *with poset of sorts* $(\widehat{\mathsf{S}}, \leq)$ *of Definition 39 is a finite decomposition.*

Proof. *Given a term* $\mathtt{eq}(t, t')$*, for any variant* $(u, \sigma) \in [\![\mathtt{eq}(t, t')]\!]_{E,Ax}$*, either* $u = \mathtt{tt}$ *or* $u = \mathtt{eq}(v, v')$ *such that* $(v, \phi) \in [\![t]\!]_{E,Ax}$ *and* $(v', \phi') \in [\![t']\!]_{E,Ax}$ *for some substitutions* ϕ *and* ϕ'*. Since* $[\![t]\!]_{E,Ax}$ *and* $[\![t']\!]_{E,Ax}$ *are finite, we conclude that* $[\![\mathtt{eq}(t, t')]\!]_{E,Ax}$ *is finite.* □

Let us make explicit the relation between variants and $\mathcal{E}$-unification. Given a decomposition (Σ, Ax, E) of an equational theory, two Σ-terms t_1 and t_2 such that $W_\cap = Var(t_1) \cap Var(t_2)$ and $W_\cup = Var(t_1) \cup Var(t_2)$, and two sets V_1 and V_2 of variants of t_1 and t_2, respectively, we define $V_1 \cap V_2 = \{(u_1\sigma, \theta_1\sigma \cup \theta_2\sigma \cup \sigma) \mid (u_1, \theta_1) \in V_1 \wedge (u_2, \theta_2) \in V_2 \wedge \exists \sigma : \sigma \in CSU_{Ax}^{W_\cup}(u_1 = u_2) \wedge (\theta_1\sigma)|_{W_\cap} =_{Ax} (\theta_2\sigma)|_{W_\cap}\}$.

Proposition 4 (Variant-based Unification). *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$*. Let* t_1, t_2 *be two* Σ*-terms. Then,* ρ *is an* $\mathcal{E}$*-unifier of* t_1 *and* t_2 *iff* $\exists (t', \rho) \in [\![t_1]\!]^\star_{E,Ax} \cap [\![t_2]\!]^\star_{E,Ax}$.

Proof. ($\Rightarrow$) *If* ρ *is an* $\mathcal{E}$*-unifier of* t_1 *and* t_2*, then* $(t_1\rho)\downarrow_{E,Ax} =_{Ax} (t_2\rho)\downarrow_{E,Ax}$*. Let* $t'_1 = (t_1\rho)\downarrow_{E,Ax}$ *and* $t'_2 = (t_2\rho)\downarrow_{E,Ax}$*. We also have that* $(t'_1, \rho) \in [\![t_1]\!]^\star_{E,Ax}$*,* $(t'_2, \rho) \in [\![t_1]\!]^\star_{E,Ax}$*,* $(t'_1, \rho) \in [\![t_2]\!]^\star_{E,Ax}$*, and* $(t'_2, \rho) \in [\![t_2]\!]^\star_{E,Ax}$.

($\Leftarrow$) *If* $\exists (t', \rho) \in [\![t_1]\!]^\star_{E,Ax} \cap [\![t_2]\!]^\star_{E,Ax}$*, then* $t' =_{Ax} (t_1\rho)\downarrow_{E,Ax} =_{Ax} (t_2\rho)\downarrow_{E,Ax}$ *and clearly* ρ *is an* $\mathcal{E}$*-unifier of* t_1 *and* t_2. □

Proposition 5 (Minimal and Complete $\mathcal{E}$-unification). *Let* $\mathcal{R} = (\Sigma, Ax, E)$ *with poset of sorts* $(\mathsf{S}, \leq)$ *be a decomposition of an equational theory* $(\Sigma, \mathcal{E})$*. Let* t, t' *be two* Σ*-terms. Then,* $U = \{\theta \mid (\mathtt{tt}, \theta) \in [\![\mathtt{eq}(t, t')]\!]^\star_{\widehat{E},Ax}\}$ *is a minimal and complete set of* $\mathcal{E}$*-unifiers for* $t = t'$*, where* $\mathtt{eq}$ *and* $\mathtt{tt}$ *are new symbols as defined in Definition 39 and* $\widehat{E} = E \cup \{\mathtt{eq}(X{:}[\mathtt{s}], X{:}[\mathtt{s}]) \to \mathtt{tt} \mid \mathtt{s} \in \mathsf{S}\}$.

Proof. *We have to prove that for each* $\mathcal{E}$*-unifier* ρ *of* t *and* t'*, there is an* $\mathcal{E}$*-unifier* σ *in* U *such that* $\rho \sqsubseteq_{\mathcal{E}} \sigma$*. First, it is clear by definition of* $\mathtt{eq}$ *and* $\mathtt{tt}$ *that* $\widehat{E}$ *satisfies properties* (1)–(4) *(see Section 2.1). Let* $U^* = \{\theta \mid (\mathtt{tt}, \theta) \in [\![\mathtt{eq}(t, t')]\!]^\star_{\widehat{E},Ax}\}$*. If* ρ *is an* $\mathcal{E}$*-unifier of* t *and* t'*, then* $\rho \in U^*$*, since for* $\bar{t} = (t\rho)\downarrow_{E,Ax}$ *and* $\bar{t}' = (t'\rho)\downarrow_{E,Ax}$*, we have that* $\bar{t} =_{Ax} \bar{t}'$ *and* $\mathtt{eq}(\bar{t}, \bar{t}') \to_{\widehat{E},Ax} \mathtt{tt}$*. If* $\rho \in U^*$*, then* ρ *is an* $\mathcal{E}$*-unifier of* t *and* t'*, since* $\mathtt{eq}(t\rho, t'\rho) \to^*_{\widehat{E},Ax} \mathtt{tt}$ *and, by properties* (1)–(4)*, we have that there are* $\bar{t}, \bar{t}'$ *s.t.* $\bar{t} = (t\rho)\downarrow_{E,Ax}$*,* $\bar{t}' = (t'\rho)\downarrow_{E,Ax}$*, and the following rewrite step exists* $\mathtt{eq}(\bar{t}, \bar{t}') \to_{\widehat{E},Ax} \mathtt{tt}$.

Now, completeness means that for each $\mathcal{E}$-unifier ρ of t and t', there is an $\mathcal{E}$-unifier σ in U such that $\rho|_{t,t'} \sqsubseteq_{\mathcal{E}} \sigma|_{t,t'}$; and minimality means that for each $\mathcal{E}$-unifier σ in U there is no σ' in U such that $\sigma|_{t,t'} \sqsubseteq_{Ax} \sigma'|_{t,t'}$. Finally, by completeness and minimality of $[\![\mathtt{eq}(t,t')]\!]_{\widehat{E},Ax}$ w.r.t. $[\![\mathtt{eq}(t,t')]\!]^{\star}_{\widehat{E},Ax}$, we conclude completeness and minimality of U w.r.t U^*. □

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

Corollary 8 (Finitary $\mathcal{E}$-unification). *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a finite variant decomposition of an equational theory $(\Sigma, \mathcal{E})$. Then, for any two given terms t, t', $U = \{\theta \mid (\mathtt{tt}, \theta) \in [\![\mathtt{eq}(t,t')]\!]_{\widehat{E},Ax}\}$ is a* finite, minimal, and complete *set of $\mathcal{E}$-unifiers for $t = t'$, where $\widehat{E}$, $\mathtt{eq}$, and $\mathtt{tt}$ are defined in Definition 39.*

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 $\mathcal{R} = (\Sigma, \mathcal{E})$ 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 Example 33); the key reason for this 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 can consider how to compute a complete set of variants of a term using the variant minimality of $VN^{\circlearrowleft}_{\mathcal{R}}$. The minimality property of Definition 14 motivates the following corollary.

Corollary 9. *Let $\mathcal{R} = (\Sigma, Ax, E)$ be a decomposition of an equational theory $(\Sigma, \mathcal{E})$. For any two terms t, t' with the same top sort, the set $S = \{\theta \mid (\mathtt{tt}, \theta) \in [\![\mathtt{eq}(t,t')]\!]^{VN^{\circlearrowleft}_{\mathcal{R}}}_{\widehat{E},Ax}\}$ is a complete set of $\mathcal{E}$-unifiers for $t = t'$, where $\widehat{E}$, $\mathtt{eq}$, and $\mathtt{tt}$ are defined in Definition 39. If, in addition, $\mathcal{R}$ is a finite decomposition, then the set S is a finite set of $\mathcal{E}$-unifiers for $t = t'$.*

9. Applications

A first obvious application is in the area of unification algorithms. The key distinction is one between *dedicated* algorithms for a given theory T, for which a special-purpose algorithm exists, and *generic* algorithms such as folding variant narrowing, which can be applied to a wide range of theories not having a dedicated algorithm. The tradeoff is one of flexibility versus performance: a dedicated unification algorithm for a given theory T uses intimate knowledge of the theory's details and is typically much more efficient; but a special-purpose algorithm has to be developed for each such T, and combinations, though possible, are computationally expensive. By contrast, variant-based unification, being a generic method, is much more flexible and, as already mentioned and illustrated by several of our examples, if T and T' enjoy FV, $T \cup T'$ often does so as well, so that obtaining unification algorithms for combined theories is typically easy and does not require an explicit combination infrastructure. Of course, both methods should be used *together:* dedicated algorithms should be used whenever possible; variant-based unification can then be used to *extend the range of theories* that can be treated as follows: as soon as the theory Ax has a dedicated unification algorithm under minimal assumptions on Ax, we can *automatically* derive a unification algorithm for any theory $T = E \cup Ax$ such that E is confluent,

terminating, sort-decreasing and coherent modulo Ax, and such an algorithm is guaranteed to be finitary if T enjoys FV.

This is exactly the approach that has been followed for analyzing cryptographic protocols modulo algebraic properties in the Maude-NPA tool [17, 45]. Such protocols can be modeled as rewrite theories $\mathcal{P} = (\Sigma, E, R)$, where the algebraic properties of the cryptographic functions are specified by equations E, and the protocol's transition rules are specified by the rewrite rules R. If E can be decomposed as $G \cup Ax$, where G is confluent, terminating, sort-decreasing and coherent modulo Ax and Ax has a finitary unification algorithm, we can perform symbolic reachability analysis on $\mathcal{P}$ by narrowing its symbolic states with the transition rules R *modulo* E, where E-unification can be carried out by folding variant narrowing with G modulo Ax and therefore does not need a dedicated E-unification algorithm. In this way, the Maude-NPA has been able to analyze a substantial collection of cryptographic protocols modulo their algebraic properties, see [17]. What makes the application of folding variant narrowing to cryptographic protocol verification interesting is its flexibility for accepting different equational theories specified by the user and its order-sorted nature, which is essential for realistic protocol specification. The following paragraph from the conclusions of a survey of algebraic properties used in cryptographic protocols [12] summarizes the actual situation in protocol verification:

> In this survey, we have identified many algebraic properties that are particularly relevant for the analysis of cryptographic protocols. ... Many recent results consider some algebraic properties. However, the existing results presented in this survey have two main weaknesses. Firstly, they are mostly theoretical: very few practical implementations enable to automatically verify protocols with algebraic properties. Secondly, in most of the cases, each paper develops an ad hoc decision procedure for a particular property.

Besides being the first practical narrowing strategy we are aware of for narrowing modulo axioms, the usefulness of folding variant narrowing goes way beyond the case of providing finitary unification algorithms for FV theories, such as those used in the Maude-NPA tool to analyze cryptographic protocols, and even beyond the case of providing a complete unification algorithm for equational theories modulo axioms. As demonstrated by its recent applications to termination algorithms modulo axioms in [14], and to algorithms for checking confluence and coherence of rewrite theories modulo axioms, such as those used in the most recent Maude CRC and ChC tools [16], computing the $E \cup Ax$-*variants* of a term may be just as important as computing $E \cup Ax$-unifiers. In particular, even for theories such as the theory of associativity, which lacks a finitary unification algorithm and *a fortiori* cannot be FV, the variants of a term (particularly in an order-sorted setting, and for terms typically used in left-hand sides of rules) can be finite quite often in practice and can provide a method to prove termination, and to check the local confluence and the coherence of rewrite rules, modulo associativity.

The key idea of why variant narrowing is important for termination, confluence, and coherence proofs, as demonstrated in [14] and in [16], is the following. Suppose that $R \cup Ax$ is a collection of rewrite rules modulo axioms Ax for which we want to prove, say, termination, or confluence, or coherence with some equations E (see [16] for an explanation of the coherence case). We may not have any tools checking such properties that can work modulo the given set of axioms Ax. For example, we are not aware of any termination tools that can handle termination modulo the commonly occurring theory ACU of associativity, commutativity and identity. What can we do? We can *decompose* Ax as a disjoint union $E \cup Ax'$, where E is confluent, terminating, sort-decreasing and coherent modulo Ax', and where we have methods to prove, e.g., termination

or confluence modulo Ax'. For example, ACU decomposes in this way as $U \cup AC$ and enjoys FV. As shown in [14], we can transform $R \cup Ax$ into a semantically equivalent[5] theory $\widehat{R} \cup E \cup Ax'$, where now the set of rules is $\widehat{R} \cup E$, modulo the much simpler axioms Ax, where $\widehat{R}$ specializes each rule in R to the family of variants of their left-hand sides. If $E \cup Ax'$ has the finite variant property, we are sure that $\widehat{R}$ will be a finite set; but in practice $\widehat{R}$ can often be finite without the FV assumption. For example, Ax can be the theory A of associativity, for which unification is not even finitary. We can view A as a rule and decompose it as $A \cup \emptyset$. In an order-sorted setting, it turns out that many theories $\widehat{R} \cup A$ of practical interest can be decomposed as $(\widehat{R} \cup A) \cup \emptyset$ with $\widehat{R}$ finite, even though we know a priori that this is not possible in general, since A is not FV and does not even have a finitary unification algorithm. For example, we can often prove confluence modulo associativity of an equational specification in this way, while the usual approach to generate critical pairs may not be feasible because of the potentially infinite number of such pairs modulo A.

10. Conclusions and Future Work

We have presented a self-contained and extended exposition of the key concepts, results, and algorithms for variant narrowing and variant-based unification; and we have illustrated the main ideas with a rich collection of examples. What these new techniques achieve is to bring narrowing modulo axioms from a theoretical possibility with hopeless practical prospects into a practically useful technique with many potential applications, some of which have already been exploited in actual tools such as the Maude-NPA or the CRC and ChC tools.

As usual much remains to be done. The main issues are: (i) better variant generation strategies and (ii) better algorithms for ensuring that a theory has the finite variant property. For example, the current implementation of folding variant narrowing and variant-based unification available in Maude [13] and used by the Maude-NPA only supports a subclass of FV theories, and could be substantially optimized in many ways. Here lazy narrowing strategies may be useful but no notion of needed or demanded evaluation step has been defined for the modulo case. Another promising direction is to further advance the proof techniques for checking FV and implement tools for such checking. There is recent work on extending techniques for termination of rewriting to termination of narrowing which could be adapted to prove FV. Modularity results for modular combination of theories enjoying the finite variant property are also interesting, similarly to modularity results for termination of basic narrowing [3].

Furthermore, a promising direction is the study of symbolic, narrowing-based, reachability analysis techniques for rewrite theories $\mathcal{R} = (\Sigma, E \cup Ax, R)$, where E is confluent, terminating, sort-decreasing and coherent modulo Ax and a finitary Ax-unification exists, but $E \cup Ax$ need not be FV. And an even more ambitious future task is to extend these techniques to new techniques for the development of finitary unification algorithms for theories that have such algorithms but do not enjoy FV.

Acknowledgements. S. Escobar has been partially supported by the EU (FEDER) and the Spanish MEC/MICINN under grant TIN 2010-21062-C02-02, and by Generalitat Valenciana PROMETEO2011/052. R. Sasse and J. Meseguer have been partially supported by NSF Grants CNS 07-16638, CNS 08-31064, CNS 09-04749, and CCF 09-05584.

[5] This semantic equivalence is very strong: that the original theory will be, e.g., terminating, confluent, and so on modulo Ax iff the transformed theory is so modulo Ax'.

References

[1] M. Alpuente, S. Escobar, J. Iborra, Termination of narrowing using dependency pairs, in: M.G. de la Banda, E. Pontelli (Eds.), Logic Programming, 24th International Conference, ICLP 2008, Udine, Italy, December 9-13 2008, Proceedings, volume 5366 of *Lecture Notes in Computer Science*, Springer, 2008, pp. 317–331.

[2] M. Alpuente, S. Escobar, J. Iborra, Termination of narrowing revisited, Theoretical Computer Science 410 (2009) 4608–4625.

[3] M. Alpuente, S. Escobar, J. Iborra, Modular termination of basic narrowing and equational unification, Logic Journal of the IGPL (2010). doi: 10.1093/jigpal/jzq009.

[4] M. Alpuente, M. Falaschi, G. Vidal, Partial Evaluation of Functional Logic Programs, ACM Transactions on Programming Languages and Systems 20 (1998) 768–844.

[5] S. Anantharaman, P. Narendran, M. Rusinowitch, Unification modulo CUI plus distributivity axioms, J. Autom. Reasoning 33 (2004) 1–28.

[6] S. Antoy, Evaluation strategies for functional logic programming, Journal of Symbolic Computation 40 (2005) 875–903.

[7] S. Antoy, R. Echahed, M. Hanus, A needed narrowing strategy, Journal of the ACM 47(4) (2000) 776–822.

[8] T. Arts, J. Giesl, Termination of term rewriting using dependency pairs, Theoretical Computer Science 236 (2000) 133–178.

[9] M. Clavel, F. Durán, S. Eker, S. Escobar, P. Lincoln, N. Martí-Oliet, J. Meseguer, C.L. Talcott, Unification and narrowing in Maude 2.4, in: R. Treinen (Ed.), Rewriting Techniques and Applications, 20th International Conference, RTA 2009, Brasília, Brazil, June 29 - July 1, 2009, Proceedings, volume 5595 of *Lecture Notes in Computer Science*, Springer, 2009, pp. 380–390.

[10] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, C.L. Talcott, All About Maude - A High-Performance Logical Framework, volume 4350 of *Lecture Notes in Computer Science*, Springer, 2007.

[11] H. Comon-Lundh, S. Delaune, The finite variant property: How to get rid of some algebraic properties, in: [23], pp. 294–307.

[12] V. Cortier, S. Delaune, P. Lafourcade, A survey of algebraic properties used in cryptographic protocols, Journal of Computer Security 14 (2006) 1–43.

[13] F. Durán, S. Eker, S. Escobar, J. Meseguer, C.L. Talcott, Variants, unification, narrowing, and symbolic reachability in maude 2.6, in: M. Schmidt-Schauss (Ed.), Proceedings of the 22nd International Conference on Rewriting Techniques and Applications, RTA 2011, May 30 - June 1, Novi Sad, Serbia, LIPIcs, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2011. To appear.

[14] F. Durán, S. Lucas, J. Meseguer, Termination modulo combinations of equational theories, in: S. Ghilardi, R. Sebastiani (Eds.), FroCos, volume 5749 of *Lecture Notes in Computer Science*, Springer, 2009, pp. 246–262.

[15] F. Durán, J. Meseguer, A Maude coherence checker tool for conditional order-sorted rewrite theories, in: [41], pp. 86–103.

[16] F. Durán, J. Meseguer, On the Church-Rosser and coherence properties of conditional order-sorted rewrite theories, Journal of Logic and Algebraic Programming (2012).

[17] S. Escobar, C. Meadows, J. Meseguer, Maude-NPA: Cryptographic protocol analysis modulo equational properties, in: A. Aldini, G. Barthe, R. Gorrieri (Eds.), FOSAD, volume 5705 of *Lecture Notes in Computer Science*, Springer, 2007, pp. 1–50.

[18] S. Escobar, J. Meseguer, Symbolic model checking of infinite-state systems using narrowing, in: F. Baader (Ed.), RTA, volume 4533 of *Lecture Notes in Computer Science*, Springer, 2007, pp. 153–168.

[19] S. Escobar, J. Meseguer, R. Sasse, Effectively checking the finite variant property, in: A. Voronkov (Ed.), RTA, volume 5117 of *Lecture Notes in Computer Science*, Springer, 2008, pp. 79–93.

[20] S. Escobar, J. Meseguer, R. Sasse, Variant narrowing and equational unification, Electronic Notes Theoretical Computer Science 238 (2009) 103–119.

[21] S. Escobar, J. Meseguer, P. Thati, Natural narrowing for general term rewriting systems, in: [23], pp. 279–293.

[22] S. Escobar, R. Sasse, J. Meseguer, Folding variant narrowing and optimal variant termination, in: [41], pp. 52–68.

[23] J. Giesl (Ed.), Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings, volume 3467 of *Lecture Notes in Computer Science*, Springer, 2005.

[24] J. Giesl, D. Kapur, Dependency pairs for equational rewriting, in: A. Middeldorp (Ed.), RTA, volume 2051 of *Lecture Notes in Computer Science*, Springer, 2001, pp. 93–108.

[25] J. Giesl, P. Schneider-Kamp, R. Thiemann, Automatic termination proofs in the dependency pair framework, in: U. Furbach, N. Shankar (Eds.), IJCAR, volume 4130 of *Lecture Notes in Computer Science*, Springer, 2006, pp. 281–286.

[26] J. Giesl, R. Thiemann, P. Schneider-Kamp, S. Falke, Mechanizing and improving dependency pairs, Journal of Automated Reasoning 37 (2006) 155–203.

[27] J.A. Goguen, J. Meseguer, Equality, types, modules, and (why not ?) generics for logic programming, Journal of Logic Programming 1 (1984) 179–210.
[28] M. Hanus, The Integration of Functions into Logic Programming: From Theory to Practice, Journal of Logic Programming 19&20 (1994) 583–628.
[29] M. Hanus, Lazy narrowing with simplification, Journal of Computer Languages 23 (1997) 61–85.
[30] M. Hanus, Multi-paradigm declarative languages, in: V. Dahl, I. Niemelä (Eds.), ICLP, volume 4670 of *Lecture Notes in Computer Science*, Springer, 2007, pp. 45–75.
[31] S. Hölldobler, Foundations of Equational Logic Programming, volume 353 of *Lecture Notes in Computer Science*, Springer, 1989.
[32] J.M. Hullot, Canonical forms and unification, in: W. Bibel, R.A. Kowalski (Eds.), CADE, volume 87 of *Lecture Notes in Computer Science*, Springer, 1980, pp. 318–334.
[33] J.P. Jouannaud, C. Kirchner, H. Kirchner, Incremental construction of unification algorithms in equational theories, in: J. Díaz (Ed.), ICALP, volume 154 of *Lecture Notes in Computer Science*, Springer, 1983, pp. 361–373.
[34] J.P. Jouannaud, H. Kirchner, Completion of a set of rules modulo a set of equations, SIAM J. Comput. 15 (1986) 1155–1194.
[35] J. Meseguer, Conditional rewriting logic as a unified model of concurrency, Theoretical Computer Science 96 (1992) 73–155.
[36] J. Meseguer, Membership algebra as a logical framework for equational specification, in: F. Parisi-Presicce (Ed.), WADT, volume 1376 of *Lecture Notes in Computer Science*, Springer, 1997, pp. 18–61.
[37] J. Meseguer, P. Thati, Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols, Higher-Order and Symbolic Computation 20 (2007) 123–160.
[38] A. Middeldorp, E. Hamoen, Completeness results for basic narrowing, Journal of Applicable Algebra in Engineering, Communication, and Computing 5 (1994) 213–253.
[39] J.C.G. Moreno, M.T. Hortalá-González, F.J. López-Fraguas, M. Rodríguez-Artalejo, An approach to declarative programming based on a rewriting logic, Journal of Logic Programming 40 (1999) 47–87.
[40] N. Nishida, G. Vidal, Termination of narrowing via termination of rewriting, Appl. Algebra Eng. Commun. Comput. 21 (2010) 177–225.
[41] P.C. Ölveczky (Ed.), Rewriting Logic and Its Applications - 8th International Workshop, WRLA 2010, Held as a Satellite Event of ETAPS 2010, Paphos, Cyprus, March 20-21, 2010, Revised Selected Papers, volume 6381 of *Lecture Notes in Computer Science*, Springer, 2010.
[42] G.E. Peterson, M.E. Stickel, Complete sets of reductions for some equational theories, J. ACM 28 (1981) 233–264.
[43] M. Rodríguez-Artalejo, Functional and constraint logic programming, in: H. Comon, C. Marché, R. Treinen (Eds.), CCL, volume 2002 of *Lecture Notes in Computer Science*, Springer, 1999, pp. 202–270.
[44] P.Y.A. Ryan, S.A. Schneider, An attack on a recursive authentication protocol. A cautionary tale, Inf. Process. Lett. 65 (1998) 7–10.
[45] R. Sasse, S. Escobar, C. Meadows, J. Meseguer, Protocol analysis modulo a combination of theories: A case study in Maude-NPA, in: 6th International Workshop on Security and Trust Management (STM'10), Lecture Notes in Computer Science, Springer, 2010. To appear.
[46] TeReSe (Ed.), Term Rewriting Systems, Cambridge University Press, Cambridge, 2003.
[47] L. Vigneron, Automated deduction techniques for studying rough algebras, Fundamenta Informaticae 33 (1998) 85–103.
[48] E. Viola, E-unifiability via narrowing, in: A. Restivo, S.R.D. Rocca, L. Roversi (Eds.), ICTCS, volume 2202 of *Lecture Notes in Computer Science*, Springer, 2001, pp. 426–438.
[49] P. Viry, Equational rules for rewriting logic, Theoretical Computer Science 285 (2002) 487–517.