Effectively Checking the Finite Variant Property*

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

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

Abstract. An equational theory decomposed into a set B of equational axioms and a set Δ of rewrite rules has the *finite variant* (FV) *property* in the sense of Comon-Lundh and Delaune iff for each term t there is a finite set $\{t_1, \ldots, t_n\}$ of $\rightarrow_{\Delta,B}$-normalized instances of t so that any instance of t normalizes to an instance of some t_i modulo B. This is a very useful property for cryptographic protocol analysis, and for solving both unification and disunification problems. Yet, at present the property has to be established by hand, giving a separate mathematical proof for each given theory: no checking algorithms seem to be known. In this paper we give both a necessary and a sufficient condition for FV from which we derive an algorithm ensuring the sufficient condition, and thus FV. This algorithm can check automatically a number of examples of FV known in the literature.

1 Introduction

The *finite variant* (FV) *property* is a useful property of a rewrite theory $\mathcal{R} = (\Sigma, B, \Delta)$ with signature Σ, rewrite rules Δ, and equational axioms B introduced by Comon-Lundh and Delaune in [2]. Very simply, it states the existence of a finite set of pairs (t_i, θ_i) for a given term t such that: (i) t_i is the $\rightarrow_{\Delta,B}$-normal form of $t\theta_i$, and (ii) for any normalized substitution ρ, the $\rightarrow_{\Delta,B}$-normal form of $t\rho$ is, up to B-equivalence, a substitution instance of some t_i. Comon-Lundh and Delaune list several important applications in [2], including formal reasoning about cryptographic protocol security using constraints [3], and reducing disunification problems modulo $\Delta \uplus B$ (when rules in Δ are viewed as equations) to disunification problems modulo B.

We have studied in detail how, if a rewrite theory $\mathcal{R} = (\Sigma, B, \Delta)$ is confluent, terminating, and coherent modulo the axioms B, and has the FV property, one can define an efficient narrowing strategy, which we call *variant narrowing*, to obtain a finitary unification algorithm modulo $\Delta \uplus B$ if a finitary B-unification

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

A. Voronkov (Ed.): RTA 2008, LNCS 5117, pp. 79–93, 2008.

algorithm exists [6]. We agree with Comon-Lundh and Delaune [2] that if an efficient, dedicated $\Delta \uplus B$-unification algorithm is known, using the FV property to generate unifiers is usually much less efficient. But such an efficient, dedicated algorithm may not be known at all. Furthermore, for common equational axioms such as AC, it is well-known that narrowing modulo AC almost never terminates [2]. Typically it does not terminate even when $\mathcal{R} = (\Sigma, B, \Delta)$ has the FV property; yet, existence of a *finite*, complete set of narrowing-generated unifiers is guaranteed by a *bound* on the depth of the narrowing tree that has to be explored [6]. Therefore, we view the FV property as the basis of an attractive method for obtaining finitary unification algorithms in many cases where no dedicated algorithm is known, and narrowing itself would almost certainly be nonterminating and therefore would yield an infinitary algorithm.

For all the above reasons: for reasoning about cryptographic protocols, to solve disunification problems, and, in our view, to solve also unification problems, it would be very useful to be able to *check* in an effective way whether a given rewrite theory $\mathcal{R} = (\Sigma, B, \Delta)$ has the FV property. This is the main question that we ask and we provide an answer for in this paper: is there an effective *algorithm* that can ensure that $\mathcal{R} = (\Sigma, B, \Delta)$ has the FV property?

We approach this main goal by stages. In Section 4, we give a necessary and a sufficient condition for FV. The necessary condition, which we abbreviate to FVNS is the absence of infinite *variant-preserving narrowing sequences*. The sufficient condition is the conjunction of FVNS with a second condition which we call *variant-preservingness* (VP). So we have a chain of implications

$$(FVNS \wedge VP) \Rightarrow FV \Rightarrow FVNS$$

This chain of implications then provides a useful division of labor for arriving in Section 5 at the desired checking algorithms. Since checking FVNS and VP ensures FV, we need algorithms checking both of these properties. It turns out that, under mild conditions on B, VP is a *decidable* property, so we have an algorithm for it. Instead, for FVNS we have a situation strongly analogous to what happens with the use of the dependency pairs (DP) method [1] for termination proofs: the DP method is sound and complete for termination, yet termination is undecidable. The point, of course, is that one usually cannot compute the *exact* dependency graph, but can nevertheless compute an *estimated* dependency graph and use it in termination proofs. This analogy is not far-fetched at all, since in fact we were inspired by the DP-method (in its "modulo" version as developed by Giesl and Kapur in [7]) to develop a DP-like analysis of the theory $\mathcal{R} = (\Sigma, B, \Delta)$ from which we derive our desired algorithm for checking FVNS.

We discuss several examples of theories that have the FV property. In particular, we show that for all the examples presented in [2] that were there proved to have the FV property by mathematical arguments given for each specific theory, our checking method can *automatically* prove the FV property. In [5], we also provide a method for disproving the FV property and show that all the examples presented in [2] that were there disproved to have the FV property are automatically disproved by our method. At the end of the paper we summarize our contributions, and discuss future work and applications, including applications

to the formal analysis of cryptographic protocols modulo equational properties. All proofs can be found in [5].

2 Preliminaries

We follow the classical notation and terminology from [13] for term rewriting and from [10,11] for rewriting logic and order-sorted notions. We 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 term algebras. For a term t we write $Var(t)$ for the set of all variables in t. The set of positions of a term t is written $Pos(t)$, and the set of non-variable positions $Pos_\Sigma(t)$. The root position of a term is Λ. The subterm of t at position p is $t|_p$ and $t[u]_p$ is the term t where $t|_p$ is replaced by u. A *substitution* σ is a sorted mapping from a finite subset of $\mathcal{X}$, written $Dom(\sigma)$, to $\mathcal{T}_\Sigma(\mathcal{X})$. The set of variables introduced by σ is $Ran(\sigma)$. The identity substitution is *id*. Substitutions are homomorphically extended to $\mathcal{T}_\Sigma(\mathcal{X})$. The application of a substitution σ to a term t is denoted by $t\sigma$. The restriction of σ to a set of variables V is $\sigma|_V$. Composition of two substitutions is denoted by $\sigma\sigma'$. We call a substitution σ a *renaming* if there is another substitution σ^{-1} such that $\sigma\sigma^{-1}|_{Dom(\sigma)} = id$.

A *Σ-equation* is an unoriented pair $t = t'$, where $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ for some sort $\mathsf{s} \in \mathsf{S}$. Given Σ and a set E of Σ-equations such that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s, order-sorted equational logic induces a congruence relation $=_E$ on terms $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ (see [11]). Throughout this paper we assume that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s. An *equational theory* (Σ, E) is a set of Σ-equations.

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

An *E-unifier* for a Σ-equation $t = t'$ is a substitution σ such that $t\sigma =_E t'\sigma$. For $Var(t) \cup Var(t') \subseteq W$, a set of substitutions $CSU_E(t = t')$ is said to be a *complete* set of unifiers of the equation $t =_E t'$ away from W if: (i) each $\sigma \in CSU_E(t = t')$ is an E-unifier of $t =_E t'$; (ii) for any E-unifier ρ of $t =_E t'$ there is a $\sigma \in CSU_E(t = t')$ such that $\sigma|_W \leq_E \rho|_W$; (iii) for all $\sigma \in CSU_E(t = t')$, $Dom(\sigma) \subseteq (Var(t) \cup Var(t'))$ and $Ran(\sigma) \cap W = \emptyset$. An E-unification algorithm is *complete* if for any equation $t = t'$ it generates a complete set of 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 *rewrite rule* is an oriented pair $l \to r$, where $l \notin \mathcal{X}$, and $l, r \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ for some sort $\mathsf{s} \in \mathsf{S}$. An *(unconditional) order-sorted rewrite theory* is a triple $\mathcal{R} = (\Sigma, E, R)$ with Σ an order-sorted signature, E a set of Σ-equations, and R a set of rewrite rules. The rewriting relation on $\mathcal{T}_\Sigma(\mathcal{X})$, written $t \to_R t'$ or

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

For substitutions σ, ρ and a set of variables V we define $\sigma|_V \to_{R/E} \rho|_V$ if there is $x \in V$ such that $x\sigma \to_{R/E} x\rho$ and for all other $y \in V$ we have $y\sigma =_E y\rho$. A substitution σ is called *R/E-normalized* (or normalized) if $x\sigma$ is R/E-irreducible for all $x \in V$. We say a rewrite step $t \xrightarrow{p}_{R/E} s$ is *normalized* if the substitution σ, s.t. $t =_E t'$ and $t'|_p = l\sigma$, is R/E-normalized.

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

3 Narrowing and Variants

Since E-congruence classes can be infinite, $\to_{R/E}$-reducibility is undecidable in general. Therefore, R/E-rewriting is usually implemented [9] by R, E-rewriting. We assume the following properties on R and E:

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

Definition 1 (Rewriting modulo). [14] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(5)*. We define the relation $\to_{R,E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ by $t \to_{R,E} t'$ iff there is a $p \in Pos_\Sigma(t)$, $l \to r$ in R and substitution σ such that $t|_p =_E l\sigma$ and $t' = t[r\sigma]_p$.*

Note that, since E-matching is decidable, $\to_{R,E}$ is decidable. Notions such as confluence, termination, irreducible terms, normalized substitution, and normalized rewrite steps are defined in a straightforward manner for $\to_{R,E}$. Note that

since R is confluent and terminating (modulo E), the relation $\rightarrow^{!}_{R,E}$ is decidable, i.e., it terminates and produces a unique term (up to E-equivalence) for each initial term t, denoted by $t{\downarrow_{R,E}}$. Of course $t \rightarrow_{R,E} t'$ implies $t \rightarrow_{R/E} t'$, but the converse need not hold. To prove completeness of $\rightarrow_{R,E}$ w.r.t. $\rightarrow_{R/E}$ we need the following additional *coherence* assumption; we refer the reader to [7] for coherence completion algorithms.

6. $\rightarrow_{R,E}$ is *E-coherent* [9], i.e., $\forall t_1, t_2, t_3$ we have $t_1 \rightarrow_{R,E} t_2$ and $t_1 =_E t_3$ implies $\exists t_4, t_5$ such that $t_2 \rightarrow^{*}_{R,E} t_4$, $t_3 \rightarrow^{+}_{R,E} t_5$, and $t_4 =_E t_5$.

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

Definition 2 (Narrowing modulo). *(see, e.g.,* [9,12]*) Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. Let $CSU_E(u = u')$ provide a finitary, and complete set of unifiers for any pair of terms u, u'. The R, E-narrowing relation on $\mathcal{T}_\Sigma(\mathcal{X})$ is defined as $t \overset{p,\sigma}{\leadsto}_{R,E} t'$ (or $\overset{\sigma}{\leadsto}$ or $\leadsto_\sigma$ if p, R, E are understood) if there is $p \in Pos_\Sigma(t)$, a (possibly renamed) rule $l \rightarrow r$ in R s.t. $Var(l) \cap Var(t) = \emptyset$, and $\sigma \in CSU_E(t|_p = l)$ such that $t' = (t[r]_p)\sigma$.*

In the following, we introduce the notion of variant and finite variant property.

Definition 3 (Decomposition). [6] *Let (Σ, E) be an order-sorted equational theory. We call (Δ, B) a* decomposition *of E if $E = B \uplus \Delta$ and $(\Sigma, B, \overrightarrow{\Delta})$ is an order-sorted rewrite theory satisfying properties* (1)–(6)*, where rules $\overrightarrow{\Delta}$ are an oriented version of Δ.*

Example 1 (Exclusive Or). The following equational theory, denoted $\mathcal{R}_\oplus$, is a presentation of the exclusive or operator together with the cancellation equations for public key encryption/decryption.

$$X \oplus 0 = X \ (1) \quad pk(K, sk(K, M)) = M \ (4) \quad X \oplus (Y \oplus Z) = (X \oplus Y) \oplus Z \ (6)$$
$$X \oplus X = 0 \ (2) \quad sk(K, pk(K, M)) = M \ (5) \qquad X \oplus Y = Y \oplus X \qquad (7)$$
$$X \oplus X \oplus Y = Y \ (3)$$

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

We recall the notions of *variant*, *finite variants*, and the *finite variant property* proposed by Comon and Delaune in [2].

Definition 4 (Variants). [2] *Given a term t and an order-sorted equational theory E, we say that (t', θ) is an E-*variant *of t if $t\theta =_E t'$, where $Dom(\theta) \subseteq Var(t)$ and $Ran(\theta) \cap Var(t) = \emptyset$.*

Definition 5 (Complete set of variants). [2] *Let (Δ, B) be a decomposition of an order-sorted equational theory (Σ, E). A* complete set of E-variants *(up to renaming) of a term t, denoted $V_{\Delta,B}(t)$, is a set S of E-variants of t such that, for each substitution σ, there is a variant $(t', \rho) \in S$ and a substitution θ such that: (i) t' is Δ, B-irreducible, (ii) $(t\sigma)\downarrow_{\Delta,B} =_B t'\theta$, and (iii) $(\sigma\downarrow_{\Delta,B})|_{Var(t)} =_B (\rho\theta)|_{Var(t)}$.*

Definition 6 (Finite variant property). [2] *Let (Δ, B) be a decomposition of an order-sorted equational theory (Σ, E). Then E, and thus (Δ, B), has the* finite variant (FV) property *if for each term t, there exists a finite and complete set of E-variants, denoted $FV_{\Delta,B}(t)$. We will call (Δ, B) a* finite variant decomposition *if (Δ, B) has the finite variant property.*

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

Definition 7 (Boundedness property). [2] *Let (Δ, B) be a decomposition of an order-sorted equational theory (Σ, E). (Δ, B) satisfies the* boundedness property *(BP) if for every term t there exists an integer n, denoted by $\#_{\Delta,B}(t)$, such that for every Δ, B-normalized substitution σ the normal form of $t\sigma$ is reachable by a Δ, B-rewriting derivation whose length can be bounded by n (thus independently of σ), i.e., $\forall t, \exists n, \forall \sigma$ s.t. $t(\sigma\downarrow_{\Delta,B}) \xrightarrow{\leq n}_{\Delta,B} (t\sigma)\downarrow_{\Delta,B}$.*

Theorem 1. [2] *Let (Δ, B) be a decomposition of an order-sorted equational theory (Σ, E). Then, (Δ, B) satisfies the boundedness property if and only if (Δ, B) is a finite variant decomposition of (Σ, E).*

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

We can effectively compute a complete set of variants in the following form.

Proposition 1 (Computing the Finite Variants). [6] *Let (Δ, B) be a finite variant decomposition of an order-sorted equational theory (Σ, E). Let $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and $\#_{\Delta,B}(t) = n$. Then, $(s, \sigma) \in FV_{\Delta,B}(t)$ if and only if there is a narrowing derivation $t \overset{\sigma}{\leadsto}{}^{\leq n}_{\Delta,B} s$ such that s is $\rightarrow_{\Delta,B}$-irreducible and σ is $\rightarrow_{\Delta,B}$-normalized.*

Example 2. The equational theory from Example 1 has the boundedness property. Thus, we use Proposition 1 to get the E-variants of $t{=}M \oplus sk(K, pk(K, M))$. As $t \rightarrow^!_{\Delta,B} 0$ we have $t \overset{id}{\leadsto}{}^!_{\Delta,B} 0$. Therefore, $(0, id) \in FV_{\Delta,B}(t)$ and it is the only element of the complete set of E-variants as no more general narrowing sequences are possible. For $s = X \oplus sk(K, pk(K, Y))$ we get (i) $s \overset{id}{\leadsto}{}^*_{\Delta,B} X \oplus Y$, (ii) $s \leadsto^*_{\{X \mapsto Z \oplus U, Y \mapsto U\},\Delta,B} Z$, (iii) $s \leadsto^*_{\{X \mapsto U, Y \mapsto Z \oplus U\},\Delta,B} Z$,

(iv) $s \rightsquigarrow^*_{\{X \mapsto U \oplus Z_1, Y \mapsto U \oplus Z_2\}, \Delta, B} Z_1 \oplus Z_2$, and (v) $s \rightsquigarrow^*_{\{X \mapsto U, Y \mapsto U\}, \Delta, B} 0$, so $(X \oplus Y, id)$, $(Z, \{X \mapsto Z \oplus U, Y \mapsto U\})$, $(Z, \{X \mapsto U, Y \mapsto Z \oplus U\})$, $(Z_1 \oplus Z_2, \{X \mapsto U \oplus Z_1,\ Y \mapsto U \oplus Z_2\})$, and $(0, \{X \mapsto U, Y \mapsto U\})$, are the E-variants. As no more general narrowing sequences are possible, these make up a complete set of E-variants. Note that (iv) is an instance of (i) and it is not necessary for a minimal and complete set of variants.

Example 3. Consider again Example 1. For this theory, narrowing clearly does not terminate because $Z_1 \oplus Z_2 \rightsquigarrow_{\{Z_1 \mapsto X_1 \oplus Z'_1,\ Z_2 \mapsto X_1 \oplus Z'_2\}, \Delta, B} Z'_1 \oplus Z'_2$ and this can be repeated infinitely often. However, if we always assume that we are interested only in a normalized substitution, which is the case, for any narrowing sequence obtained in the previous form, there is a one-step rewriting sequence that provides the same result. That is, given the narrowing sequence

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

and its corresponding rewrite sequence

$$X_1 \oplus X'_1 \oplus Z''_1 \oplus X_1 \oplus X'_1 \oplus Z''_2 \rightarrow_{\Delta, B} X'_1 \oplus Z''_1 \oplus X'_1 \oplus Z''_2 \rightarrow_{\Delta, B} Z''_1 \oplus Z''_2$$

we can also reduce it to the same normal form using only one application of (3) and the following normalized substitution $\rho = \{X \mapsto X_1 \oplus X'_1, Y \mapsto Z''_1 \oplus Z''_2\}$. The trick is that rule (3) allows combining all pairs of canceling terms and thus gets rid of all of them at once.

4 Sufficient and Necessary Conditions for FV

Deciding whether an equational theory has the finite variant property is a non-trivial task, since we have to decide whether we can stop generating normalized substitution instances by narrowing for each term. Intuitively, since the theory is convergent, we only have to focus on normalized substitutions and, since it has the boundedness property, we can compute the variants in a bottom-up manner. Moreover, any rewrite sequence with a normalized substitution will be captured by a narrowing sequence leading to the same variant (i.e., irreducible term). Our algorithm for checking that an equational theory has the finite variant property 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) 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 $(VP \wedge FVNS) \Rightarrow FV \Rightarrow FVNS$.

Variant–preservingness (VP) ensures that we can perform an intuitive bottom-up[1] generation of variants. The following notion is useful.

[1] Note that this is not the same as innermost narrowing nor innermost narrowing up to some bound. Consider Example 5 where innermost narrowing does not terminate for term $c(f(X), X)$, since it looks for an innermost narrowing redex each time. A bottom-up generation of invariants does terminate (see Proposition 1) providing terms $c(f(X), X)$ and $c(X', f(X'))$. Even in the case of innermost narrowing with a bound, it will miss the term $c(f(X), X)$.

Definition 8 (Variant–pattern). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. We call a term $f(t_1, \ldots, t_n)$ a* variant–pattern *if all subterms $t_1, \ldots, t_n$ are $\rightarrow_{R,E}$-irreducible. We will say a term t* has *a variant–pattern if there is a variant–pattern t' s.t. $t' =_E t$.*

It is worth pointing out that whether a term has a variant–pattern is decidable, assuming a finitary and complete E-unification 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 $\theta \in CSU_E(t = f(X_1, \ldots, X_k))$ such that θ is normalized, where $t' = f(X_1, \ldots, X_k)\theta$. In the case of a term t rooted by a free symbol, t has a variant–pattern if it is already a variant–pattern, i.e., every argument of the root symbol must be irreducible. And, in the case of a term t rooted by an AC symbol, we only have to consider in the previous algorithm the same AC symbol at the root of t, instead of every symbol.

Definition 9 (Variant–preserving). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. We say that the theory $\mathcal{R}$ is* variant–preserving *(VP) if for any variant–pattern t, either t is $\rightarrow_{R,E}$-irreducible or there is a normalized $\rightarrow_{R,E}$ step at the top position.*

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

Example 4. Consider the following equational theory $f(a, b, X) = c$, where symbol f is AC and X is a variable. The narrowing relation $\rightsquigarrow_{R,E}$ terminates for any term but the 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.

We characterize variant–preservingness in Section 5.1. A theory that already has the variant–preserving property, if there is no infinite E-narrowing sequence, clearly has the finite variant property. However, if infinite E-narrowing sequences exist, a theory may still have the finite variant property.

Example 5. Consider the equational theory $f(f(X)) = X$, which is well-known to be non-terminating for narrowing, i.e.,

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

When we consider all possible instances of term $c(f(X), X)$ for normalized substitutions, we obtain term $c(f(X), X)$ itself and the sequence $c(f(X), X) \rightsquigarrow_{\{X \mapsto f(X')\}, R, E} c(X', f(X'))$. The theory does have the boundedness property, and therefore FV, since for any term and a normalized substitution, a bound is the number of f symbols in the term.

Not all the narrowing sequences are relevant for the finite variant property, as shown in the previous example, and thus we must identify the relevant ones.

Definition 10 (Variant–preserving sequences). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. A rewrite sequence $t_0 \overset{p_1}{\rightarrow}_{R,E} t_1 \cdots \overset{p_n}{\rightarrow}_{R,E} t_n$ is called* variant–preserving *if $t_{i-1}|_{p_i}$ has a variant–pattern for $i \in \{1, \ldots, n\}$ and there is no sequence $t_0 \rightarrow^m_{R,E} t'_m$ such that $m < n$ and $t_n =_E t'_m$. A narrowing sequence $t_0 \overset{p_1,\sigma_1}{\rightsquigarrow}_{R,E} t_1 \cdots \overset{p_n,\sigma_n}{\rightsquigarrow}_{R,E} t_n$, $\sigma = \sigma_1 \cdots \sigma_n$, is called* variant–preserving *if σ is $\rightarrow_{R,E}$-normalized and $t_0\sigma \overset{p_1}{\rightarrow}_{R,E} t_1\sigma \cdots \overset{p_n}{\rightarrow}_{R,E} t_n$ is variant–preserving.*

The set of variant–preserving sequences is not computable in general. However, we provide sufficient conditions in Section 5.

Example 6. The infinite narrowing sequence of Example 5 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 term $c(f(X), X)$ are the term itself and the one-step sequence with substitution $\{X \mapsto f(X')\}$.

Example 7. For Example 3, the narrowing sequence

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

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

We prove that using variant–preserving sequences is sound and complete.

Theorem 2 (Computing with variant–preserving sequences). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *that also has the finite variant property. Let $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and $\#_{R,E}(t) = n$. Then, $(s, \sigma) \in FV_{R,E}(t)$ if and only if there is a variant–preserving narrowing derivation $t \overset{\sigma}{\rightsquigarrow}^{\leq n}_{R,E} s$ such that s is $\rightarrow_{R,E}$-irreducible.*

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

Theorem 3 (Sufficient conditions for FV). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. 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.*

Note that variant-preservingness is not a *necessary* condition for FV, as shown in Example 4. However, the absence of infinite variant–preserving narrowing sequences is a *necessary* condition for FV.

Theorem 4 (Necessary condition for FV). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. If there is an infinite variant–preserving narrowing sequence, then $\mathcal{R}$ does not satisfy the finite variant property.*

5 Checking the Finite Variant Property

In the following, we show that the variant-preserving property is clearly checkable, in Section 5.1, but the absence of infinite variant-preserving narrowing sequences is not computable in general, and we approximate such property, in Section 5.2, by a checkable one using the dependency pairs technique of [7] for the modulo case.

5.1 Checking Variant–Preservingness

The following class of equational theories is relevant. The notion of E-descendants (given in [5]) is a straightforward extension of the standard notion of descendant for rules. Given $t =_E s$ and $p \in Pos(t)$, we write $p\backslash\backslash_s$ for the E-descendants of p in s.

Definition 11 (Upper-E-coherence). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(5)*. We say $\mathcal{R}$ is* upper-E-coherent *if for all t_1, t_2, t_3 we have $t_1 \xrightarrow{p}_{R,E} t_2$, $t_1 =_E t_3$, $p > \Lambda$, and $p\backslash\backslash_{t_3} = \emptyset$ implies that for all $p' \leq p$ such that $p'\backslash\backslash_{t_3} = \emptyset$, there exist t'_3, t_4, t_5 such that $t_1 \xrightarrow{p'}_{R,E} t'_3$, $t_2 \rightarrow^*_{R,E} t_4$, $t'_3 \rightarrow^*_{R,E} t_5$, and $t_4 =_E t_5$.*

Assuming E-coherence, checking upper-E-coherence consists of taking term t for each equation $t = t' \in E$ (or reverse), finding a position $p \in Pos(t)$ s.t. $p > \Lambda$ and a substitution σ s.t. $t\sigma|_p$ is $\rightarrow_{R,E}$-reducible and then, let $p = p_1 . \cdots . p_k$, for $i \in \{1, \ldots, k-1\}$, $t\sigma|_{p_i}$ must be $\rightarrow_{R,E}$-reducible. In general, upper-E-coherence implies E-coherence but not vice versa, as shown below.

Example 8. Let us consider the rewrite theory $R = \{g(f(X)) \rightarrow d,\ a \rightarrow c\}$ and $E = \{g(f(f(a))) = g(b)\}$. For the term $t = g(f(f(a)))$, subterm a is reducible, $t =_E g(b)$, but subterms $f(f(a))$ and $f(a)$ are not reducible and thus the theory is not upper-E-coherent. However, the theory is trivially E-coherent because of the use of symbol g at the top of both sides of the equation.

Now, we can provide an algorithm for checking variant–preservingness.

Theorem 5 (Checking Variant–preservingness). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *that is upper-E-coherent. $\mathcal{R}$ has the variant–preserving property iff for all $l \rightarrow r, l' \rightarrow r' \in R$ (possibly renamed s.t. $Var(l) \cap Var(l') = \emptyset$) and for all $X \in Var(l)$, the term $t = l\theta$, where $\theta = \{X \mapsto l'\}$ such that θ 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.*

In [5], the variant-preservingness property for the exclusive or theory is proved. The upper-E-coherence condition is necessary, as shown below.

Example 9. The theory of Example 8 satisfies the conditions of Theorem 5 but it is not variant–preserving. That is, $g(f(a))$ does not have a variant–pattern. However, $g(b)$ is a variant–pattern, it is reducible, but it is not $\rightarrow_{R,E}$-reducible with a normalized substitution.

5.2 Checking Finiteness of Variant–Preserving Narrowing Sequences

First, we need to extend the notion of 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*[2] if all its equations are non-collapsing.

Definition 12 (Defined Symbols for Rewriting Modulo Equations). [7] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory with E collapse-free. Then the set of defined symbols D is the smallest set such that $D = \{root(l) \mid l \to r \in R\} \uplus \{root(v) \mid u = v \in E \text{ or } v = u \in E, root(u) \in D\}$.*

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 13 (Adding Instantiations). [7] *Given an order-sorted rewrite theory $\mathcal{R} = (\Sigma, E, R)$, let $Ins_E(R)$ be a set containing only rules of the form $l\sigma \to r\sigma$ (where σ is a substitution and $l \to r \in R$). $Ins_E(R)$ is called an instantiation of R for the equations E iff $Ins_E(R)$ is the smallest set such that: (a) $R \subseteq Ins_E(R)$, (b) for all $l \to r \in R$, all v such that $u = v \in E$ or $v = u \in E$, and all $\sigma \in CSU_E(v = l)$, there exists a rule $l' \to r' \in Ins_E(R)$ and a variable renaming ν such that $l\sigma =_E l'\nu$ and $r\sigma =_E r'\nu$.*

Note that when $E = \emptyset$ or E contains only AC or C axioms, $Ins_E(R) = R$. 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 14 (Dependency Pair). [1] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory. If $l \to C[g(t_1, \ldots, t_m)]$ is a rule of $Ins_E(\mathcal{R})$ with C a context and g a defined symbol in $Ins_E(\mathcal{R})$, then $\langle l, g(t_1, \ldots, t_m)\rangle$ is called a* dependency pair *of $\mathcal{R}$.*

Example 10 (Abelian Group). This presentation of Abelian group theory, called $\mathcal{R}_* = (\Sigma, E, R)$, has been shown to satisfy the finite variant property in [2]. The operators Σ are $\_*\_$, $(\_)^{-1}$, and 1. The set of equations E consists of associativity and commutativity for $*$. The rules R are:

$$x * 1 \to x \quad (8) \qquad x^{-1^{-1}} \to x \quad (13)$$

$$1^{-1} \to 1 \quad (9) \qquad (x^{-1} * y)^{-1} \to x * y^{-1} \quad (14)$$

$$x * x^{-1} \to 1 \quad (10) \qquad x * (x^{-1} * y) \to y \quad (15)$$

$$x^{-1} * y^{-1} \to (x * y)^{-1} \quad (11) \qquad x^{-1} * (y^{-1} * z) \to (x * y)^{-1} * z \quad (16)$$

$$(x * y)^{-1} * y \to x^{-1} \quad (12) \qquad (x * y)^{-1} * (y * z) \to x^{-1} * z \quad (17)$$

[2] Note that regularity does not imply collapse-free, e.g. equation 1 of Example 1 is regular but also collapsing.

The AC-dependency pairs for this rewrite theory are as follows. The other rules not mentioned here do not give rise to an AC-dependency pair[3].

$$\begin{array}{llll}
(11)a: & \langle x^{-1} * y^{-1} \, , \, (x * y)^{-1} \rangle & (11)b: & \langle x^{-1} * y^{-1} \, , \, x * y \rangle \\
(14)a: & \langle (x^{-1} * y)^{-1} \, , \, x * y^{-1} \rangle & (14)b: & \langle (x^{-1} * y)^{-1} \, , \, y^{-1} \rangle \\
(16)a: & \langle x^{-1} * y^{-1} * z \, , \, (x * y)^{-1} * z \rangle & (16)b: & \langle x^{-1} * y^{-1} * z \, , \, (x * y)^{-1} \rangle \\
(16)c: & \langle x^{-1} * y^{-1} * z \, , \, x * y \rangle & (12)a: & \langle (x * y)^{-1} * y \, , \, x^{-1} \rangle \\
(17)a: & \langle (x * y)^{-1} * y * z \, , \, x^{-1} * z \rangle & (17)b: & \langle (x * y)^{-1} * y * z \, , \, x^{-1} \rangle
\end{array}$$

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

Definition 15 (Chain). [1] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory. 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 $t_j \sigma \rightarrow^*_{R,E} s_{j+1} \sigma$ 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 16 (Dependency Graph). [1] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory. 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.*

As in the dependency pair technique [1], the variant–preserving chains are not computable in general and an approximation must be performed. The notion of *connectable terms* as defined in [1] can be easily extended to the variant–preserving case, and the *estimated dependency graph* [1] can be computed using the CAP and REN procedures [1]. We omit this in the paper for lack of space but such an estimated dependency graph has been used in all examples.

Example 11. In [5], the dependency graph for Example 10 is shown. It was created with AProVE. We see that there are self-loops on (11)b, (14)b, (16)a, (16)c and (17)a. (11)a has a loop with (14)a, (14)a has a loop with (16)b, and so on. It is a very highly connected graph.

In order to correctly approximate the bound for the finite variant property, we include rules without defined symbols in their right-hand sides as extra dependency pairs, that we call *dummy*.

Definition 17 (Dummy dependency pairs). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory. If for a rule $l \rightarrow r \in R$ the right-hand side r does not contain a defined symbol then $\langle l, r \rangle$ is a* dummy *dependency pair of $\mathcal{R}$.*

Example 12 (Abelian group variant–preserving dependency pairs). Building upon the AC-dependency pairs computed in Example 10 we need to add these dummy dependency pairs, to the set of dependency pairs from the prior example:

$$\begin{array}{lll}
(8)a : \langle x * 1 \, , \, x \rangle & (9)a : \langle 1^{-1} \, , \, 1 \rangle & (10)a : \langle x * x^{-1} \, , \, 1 \rangle \\
(13)a : \langle x^{-1^{-1}} \, , \, x \rangle & (15)a : \langle x * x^{-1} * y \, , \, y \rangle &
\end{array}$$

[3] We have used the AProVE tool [8] to generate the dependency pairs. AProVE first applies the coherence algorithm of [7] to this example which is unnecessary here and thus we drop the dependency pairs created that way.

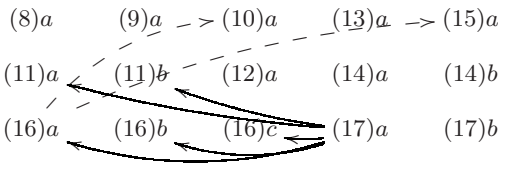

Fig. 1. Variant–preserving dependency graph

Definition 18 (Cycle). [1] *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.

Definition 19 (Variant–preserving chain). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory. 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 $\rightarrow_{R,E}$-normalized and the following rewrite sequence obtainable from the chain $s_1\sigma \rightarrow_{R,E} C_1[t_1]\sigma \rightarrow^*_{R,E} C_1[s_2]\sigma \rightarrow_{R,E} C_1[C_2[t_2]]\sigma \rightarrow^*_{R,E} \cdots \rightarrow^*_{R,E} C_1[C_2[\cdots C_{n-1}[s_n]]]\sigma \rightarrow_{R,E} C_1[C_2[\cdots C_{n-1}[C_n[t_n]]]]\sigma$ is variant–preserving.*

The notions of a cycle, the dependency graph and the estimated dependency graph are easily extended to the variant–preserving case. The following straightforward result approximates the absence of infinite narrowing sequences.

Proposition 2 (Checking Finiteness of the VP Narrowing sequences). *Let $\mathcal{R} = (\Sigma, E, R)$ be a variant–preserving, order-sorted rewrite theory. Let E 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.*

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 [7] for explanations.

Example 13 (Abelian group variant–preserving dependency pair graph). We can show the variant–preserving dependency graph of Example 12 in Figure 1. As you can see in the picture, all the cycles have disappeared, because they involved non-normalized substitutions, or terms without a variant–pattern, or could be shortened.

Finally, we are able to provide an approximation result for the absence of infinite variant–preserving narrowing sequences. Also, we are able to compute a bound for each defined symbol thanks to a notion of *rank*.

Definition 20 (Rank). *The* rank *of a dependency pair p, denoted $rank_{R,E}(p)$, is the length of the longest variant–preserving chain starting from p. For a rule $l \to r \in R$ giving rise to dependency pairs $dp_1, dp_2, \ldots, dp_n$, its rank is $rank_{R,E}(l \to r) = (rank_{R,E}(dp_1)-1)+(rank_{R,E}(dp_2)-1)+\ldots+(rank_{R,E}(dp_n)-1)+1$. For a defined symbol f, its rank is $rank_{R,E}(f) = max\{rank_{R,E}(l \to r) \mid l \to r \in R, root(l)=f\}$. For a term t, its rank is $rank_{R,E}(t)=\Sigma_{f\in\mathcal{D}}(rank_{R,E}(f)*\#_f(t))$ where $\mathcal{D}$ is the set of defined symbols in $\mathcal{R}$ and $\#_f(t)$ is the number of appearances of f in t.*

Any cycle in the variant–preserving dependency graph of course gives the rank ∞ to all dependency pairs involved in the cycle. For any symbol f it is obvious that $rank_{R,E}(f) \geq 1$ iff f is a defined symbol.

Note that the dependency graph is not necessarily transitive for purposes of rank calculation.

Example 14 (Abelian group variant–preserving dependency pair graph rank). Consider again Example 13. The rank for the dependency pairs (17)a and (16)a is 2, the rank of all other dependency pairs is 1. Note that (17)a has rank 2 as according to Example 13 there is no variant–preserving chain of length 3 as in this case the graph is not transitive. Thus the rank of rule (17) is 2, which means that the rank of $*$ is 2 and the rank of $^{-1}$ is 1. Thus the rank for any term t is $(\#_*(t) \times 2) + \#_{^{-1}}(t)$.

In [5], we show VP for Abelian group and Diffie-Hellman, and the finite variant property for Diffie-Hellman. The proof of our final result for this section is trivial by Theorem 4, since if the rank of all symbols in the signature is finite, there are no cycles in the estimated dependency graph and we know for sure that there is no infinite variant-preserving rewrite sequence.

Theorem 6 (Approximation for the finite variant property). *Let $\mathcal{R} = (\Sigma, E, R)$ be a variant–preserving, order-sorted rewrite theory. Let E contain only linear, non-collapsing equations. If for all defined symbols f we have that $rank_{R,E}(f)$ is finite, then $\mathcal{R}$ has the finite variant property.*

6 Conclusions

We have recalled Comon-Lundh and Delaune's finite variant property (FV) and summarized some of its applications. Our main two contributions have been: (i) giving new necessary conditions and new sufficient conditions for FV; and (ii) deriving from these conditions an algorithm for checking FV. To the best of our knowledge, no such algorithms were known before. The algorithms can certainly be improved. For example, more accurate ways of computing the effective dependency graph will help the checking of FV. Regarding implementations, we plan to implement these algorithms for frequently used equational axioms B such as $\emptyset$, C, AC, and their combinations, so that they can be used in conjunction with the already-implemented variant narrowing algorithm described in [6]

to derive finitary unification algorithms. This will provide a key component of the Maude-NPA [4], a tool for the analysis of cryptographic protocols modulo algebraic properties.

References

1. Arts, T., Giesl, J.: Termination of term rewriting using dependency pairs. Theor. Comput. Sci. 236(1-2), 133–178 (2000)
2. Comon-Lundh, H., Delaune, S.: The finite variant property: How to get rid of some algebraic properties. In: Giesl, J. (ed.) RTA 2005. LNCS, vol. 3467, pp. 294–307. Springer, Heidelberg (2005)
3. Comon-Lundh, H., Shmatikov, V.: Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In: LICS, pp. 271–280. IEEE Computer Society, Los Alamitos (2003)
4. Escobar, S., Meadows, C., Meseguer, J.: A rewriting-based inference system for the NRL protocol analyzer and its meta-logical properties. Theor. Comput. Sci. 367(1-2), 162–202 (2006)
5. Escobar, S., Meseguer, J., Sasse, R.: Effectively checking or disproving the finite variant property. Technical Report UIUCDCS-R-2008-2960, Department of Computer Science - University of Illinois at Urbana-Champaign (April 2008)
6. Escobar, S., Meseguer, J., Sasse, R.: Variant narrowing and equational unification. In: 7th Int'l Workshop on Rewriting Logic and its Applications (to appear, 2008)
7. Giesl, J., Kapur, D.: Dependency pairs for equational rewriting. In: Middeldorp, A. (ed.) RTA 2001. LNCS, vol. 2051, pp. 93–108. Springer, Heidelberg (2001)
8. Giesl, J., Schneider-Kamp, P., Thiemann, R.: Automatic termination proofs in the dependency pair framework. In: Furbach, U., Shankar, N. (eds.) IJCAR 2006. LNCS (LNAI), vol. 4130, pp. 281–286. Springer, Heidelberg (2006)
9. Jouannaud, J.-P., Kirchner, C., Kirchner, H.: Incremental construction of unification algorithms in equational theories. In: Díaz, J. (ed.) ICALP 1983. LNCS, vol. 154, pp. 361–373. Springer, Heidelberg (1983)
10. Meseguer, J.: Conditioned rewriting logic as a united model of concurrency. Theor. Comput. Sci. 96(1), 73–155 (1992)
11. Meseguer, J.: Membership algebra as a logical framework for equational specification. In: Parisi-Presicce, F. (ed.) WADT 1997. LNCS, vol. 1376, pp. 18–61. Springer, Heidelberg (1998)
12. Meseguer, J., Thati, P.: Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols. Higher-Order and Symbolic Computation 20(1–2), 123–160 (2007)
13. TeReSe (ed.): Term Rewriting Systems. Cambridge University Press, Cambridge (2003)
14. Viry, P.: Equational rules for rewriting logic. Theor. Comput. Sci. 285(2), 487–517 (2002)