

# Effectively Checking or Disproving the Finite Variant Property <sup>\*</sup>

Santiago Escobar<sup>1</sup>, José Meseguer<sup>2</sup> and Ralf Sasse<sup>2</sup>

<sup>1</sup> Universidad Politécnica de Valencia, Spain. [sescobar@dsic.upv.es](mailto:sescobar@dsic.upv.es)

<sup>2</sup> University of Illinois at Urbana-Champaign, USA.  
[{meseguer,rsasse}@cs.uiuc.edu](mailto:{meseguer,rsasse}@cs.uiuc.edu)

**Abstract.** An equational theory decomposed into a set  $B$  of equational axioms and a set  $\Delta$  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  $\{t_1, \dots, t_n\}$  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, both an algorithm ensuring the sufficient condition, and thus FV, and another disproving the necessary condition, and thus disproving FV. These algorithms can check automatically a number of examples and counterexamples 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  $\Sigma$ , rewrite rules  $\Delta$ , and equational axioms  $B$  introduced by Comon-Lundh and Delaune in [2]. Very simply, it states the existence of a finite set of pairs  $(t_i, \theta_i)$  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  $\rho$ , 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  $\Delta$  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

---

<sup>\*</sup> 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.

obtain a finitary unification algorithm modulo  $\Delta \uplus B$  if a finitary  $B$ -unification 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 [20,2]. 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: are there effective *algorithms* that can ensure that  $\mathcal{R} = (\Sigma, B, \Delta)$  has, or does not have, the FV property? Of course an algorithm for *checking* the FV property can be different from one for *disproving* it; and in general neither of these algorithms may be able to decide whether or not a given theory 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, and in Section 6 at the desired disproving algorithm. 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. Regarding an algorithm for disproving FV, since FVNS is a necessary condition for FV, it is enough to disprove FVNS. Therefore, in Section 6 we give a simple sufficient condition for the failure of FVNS that can be effectively checked.

We discuss several examples of theories that have, or fail to have, the FV property. In particular, we show that for all the examples presented in [2], which were there each proved or disproved to have the FV property by mathematical arguments given for each specific theory, our checking and disproving methods can *automatically* prove or disprove the FV property. 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 are in Appendix B.

## 2 Preliminaries

We follow the classical notation and terminology from [19] for term rewriting and from [13,14] for rewriting logic and order-sorted notions. We assume an *order-sorted signature*  $\Sigma$  with a finite poset of sorts  $(S, \leq)$  and a finite number of function symbols. We furthermore assume that: (i) each connected component in the poset ordering has a top sort, and for each  $s \in S$  we denote by  $[s]$  the top sort in the component of  $s$ ; and (ii) for each operator declaration  $f : s_1 \times \dots \times s_n \rightarrow s$  in  $\Sigma$ , there is also a declaration  $f : [s_1] \times \dots \times [s_n] \rightarrow [s]$ . We assume an  $S$ -sorted family  $\mathcal{X} = \{\mathcal{X}_s\}_{s \in S}$  of disjoint variable sets with each  $\mathcal{X}_s$  countably infinite.  $\mathcal{T}_\Sigma(\mathcal{X})_s$  is the set of terms of sort  $s$ , and  $\mathcal{T}_{\Sigma,s}$  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  $\lambda$ . 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*  $\sigma$  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  $\sigma$  is  $Ran(\sigma)$ . The identity substitution is *id*. Substitutions are homomorphically extended to  $\mathcal{T}_\Sigma(\mathcal{X})$ . The application of a substitution  $\sigma$  to a term  $t$  is denoted by  $t\sigma$ . The restriction of  $\sigma$  to a set of variables  $V$  is  $\sigma|_V$ . Composition of two substitutions is denoted by  $\sigma\sigma'$ . We call a substitution  $\sigma$  a *renaming* if there is another substitution  $\sigma^{-1}$  such that  $\sigma\sigma^{-1}|_{Dom(\sigma)} = id$ .

A  $\Sigma$ -*equation* is an unoriented pair  $t = t'$ , where  $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})_s$  for some sort  $s \in S$ . Given  $\Sigma$  and a set  $E$  of  $\Sigma$ -equations such that  $\mathcal{T}_{\Sigma,s} \neq \emptyset$  for every sort  $s$ , order-sorted equational logic induces a congruence relation  $=_E$  on terms  $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$  (see [14]). Throughout this paper we assume that  $\mathcal{T}_{\Sigma,s} \neq \emptyset$  for every sort  $s$ . An *equational theory*  $(\Sigma, E)$  is a set of  $\Sigma$ -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  $\sigma$  such that  $t\sigma =_E t'$ ; such a substitution  $\sigma$  is said to be an  $E$ -*match* from  $t$  to  $t'$ . For substitutions  $\sigma, \rho$  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  $\eta$  such that  $(\sigma\eta)|_V =_E \rho|_V$ .

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

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

We say that the relation  $\rightarrow_{R/E}$  is *terminating* if there is no infinite sequence  $t_1 \rightarrow_{R/E} t_2 \rightarrow_{R/E} \dots \rightarrow_{R/E} \dots$ . We say that the relation  $\rightarrow_{R/E}$  is *confluent* if whenever  $t \rightarrow_{R/E}^* t'$  and  $t \rightarrow_{R/E}^* t''$ , there exists a term  $t'''$  such that  $t' \rightarrow_{R/E}^* t'''$  and  $t'' \rightarrow_{R/E}^* t'''$ . An order-sorted rewrite theory  $\mathcal{R} = (\Sigma, E, R)$  is *confluent* (resp. *terminating*) if the relation  $\rightarrow_{R/E}$  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  $t \rightarrow_{R/E}^! t'$  or  $t \downarrow_{R/E}$  (when  $t'$  is not relevant).

### 3 Narrowing and Variants

Since  $E$ -congruence classes can be infinite,  $\rightarrow_{R/E}$ -reducibility is undecidable in general. Therefore,  $R/E$ -rewriting is usually implemented [11] 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  $\sigma$ , we have  $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_s$  if and only if  $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_s$ , and all variables in  $Var(t)$  have a top sort.
2.  $E$  has a finitary and complete unification algorithm.
3. For each  $t \rightarrow t'$  in  $R$  we have  $Var(t') \subseteq Var(t)$ .

4.  $R$  is *sort-decreasing*, i.e., for each  $t \rightarrow t'$  in  $R$ , each  $s \in S$ , and each substitution  $\sigma$ ,  $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_s$  implies  $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_s$ .
5. The rewrite rules  $R$  are *confluent and terminating modulo  $E$* , i.e., the relation  $\rightarrow_{R/E}$  is confluent and terminating.

**Definition 1 (Rewriting modulo).** [4,21,18] *Let  $\mathcal{R} = (\Sigma, E, R)$  be an order-sorted rewrite theory satisfying properties (1)–(5). We define the relation  $\rightarrow_{R,E}$  on  $\mathcal{T}_\Sigma(\mathcal{X})$  by  $t \rightarrow_{R,E} t'$  iff there is a  $p \in \text{Pos}_\Sigma(t)$ ,  $l \rightarrow r$  in  $R$  and substitution  $\sigma$  such that  $t|_p \equiv_E l\sigma$  and  $t' = t[r\sigma]_p$ .*

Note that, since  $E$ -matching is decidable,  $\rightarrow_{R,E}$  is decidable. Notions such as confluence, termination, irreducible terms, normalized substitution, and normalized rewrite steps are defined in a straightforward manner for  $\rightarrow_{R,E}$ . 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 [12,7] for coherence completion algorithms.

6.  $\rightarrow_{R,E}$  is  *$E$ -coherent* [18,11], i.e.,  $\forall t_1, t_2, t_3$  we have  $t_1 \rightarrow_{R,E} t_2$  and  $t_1 \equiv_E t_3$  implies  $\exists t_4, t_5$  such that  $t_2 \rightarrow_{R,E}^* t_4$ ,  $t_3 \rightarrow_{R,E}^+ t_5$ , and  $t_4 \equiv_E t_5$ .

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., [11,15]) *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  $t \overset{p,\sigma}{\rightsquigarrow}_{R,E} t'$  (or  $\overset{\sigma}{\rightsquigarrow}$  or  $\rightsquigarrow_\sigma$  if  $p, R, E$  are understood) if there is  $p \in \text{Pos}_\Sigma(t)$ , a (possibly renamed) rule  $l \rightarrow r$  in  $R$  s.t.  $\text{Var}(l) \cap \text{Var}(t) = \emptyset$ , 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  $(\Sigma, E)$  be an order-sorted equational theory. We call  $(\Delta, B)$  a decomposition of  $E$  if  $E = B \uplus \Delta$  and  $(\Sigma, B, \vec{\Delta})$  is an order-sorted rewrite theory satisfying properties (1)–(6), where rules  $\vec{\Delta}$  are an oriented version of  $\Delta$ .*

*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.

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

This equational theory  $(\Sigma, E)$  has a decomposition into  $\Delta$  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  $(t', \theta)$  is an  $E$ -variant of  $t$  if  $t\theta =_E t'$ , where  $\text{Dom}(\theta) \subseteq \text{Var}(t)$  and  $\text{Ran}(\theta) \cap \text{Var}(t) = \emptyset$ .*

**Definition 5 (Complete set of variants).** [2] *Let  $(\Delta, B)$  be a decomposition of an order-sorted equational theory  $(\Sigma, E)$ . 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  $\sigma$ , there is a variant  $(t', \rho) \in S$  and a substitution  $\theta$  such that: (i)  $t'$  is  $\Delta, B$ -irreducible, (ii)  $(t\sigma)\downarrow_{\Delta, B} =_B t'\theta$ , and (iii)  $(\sigma\downarrow_{\Delta, B})|_{\text{Var}(t)} =_B (\rho\theta)|_{\text{Var}(t)}$ .*

**Definition 6 (Finite variant property).** [2] *Let  $(\Delta, B)$  be a decomposition of an order-sorted equational theory  $(\Sigma, E)$ . Then  $E$ , and thus  $(\Delta, B)$ , 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  $(\Delta, B)$  a finite variant decomposition if  $(\Delta, B)$  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  $(\Delta, B)$  be a decomposition of an order-sorted equational theory  $(\Sigma, E)$ .  $(\Delta, B)$  satisfies the boundedness property (BP) if for every term  $t$  there exists an integer  $n$ , denoted by  $\#_{\Delta, B}(t)$ , such that for every  $\Delta, B$ -normalized substitution  $\sigma$  the normal form of  $t\sigma$  is reachable by a  $\Delta, B$ -rewriting derivation whose length can be bounded by  $n$  (thus independently of  $\sigma$ ):*

$$\forall t, \exists n, \forall \sigma \text{ s.t. } t(\sigma\downarrow_{\Delta, B}) \xrightarrow[\Delta, B]{\leq n} (t\sigma)\downarrow_{\Delta, B}$$

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

Obviously, if for a term  $t$ , the minimal length of a rewrite sequence to the canonical form of an instance  $t\sigma$ , with  $\sigma$  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  $(\Delta, B)$  be a finite variant decomposition of an order-sorted equational theory  $(\Sigma, E)$ . 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  $t \xrightarrow{\sigma}_{\Delta, B}^{\leq n} s$  such that  $s$  is  $\rightarrow_{\Delta, B}$ -irreducible and  $\sigma$  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  $t \xrightarrow{!}_{\Delta, B} 0$  we have  $t \xrightarrow{id!}_{\Delta, B} 0$ . 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)  $s \xrightarrow{id*}_{\Delta, B} X \oplus Y$ , (ii)  $s \rightsquigarrow^*_{\{X \mapsto Z \oplus U, Y \mapsto U\}, \Delta, B} Z$ , (iii)  $s \rightsquigarrow^*_{\{X \mapsto U, Y \mapsto Z \oplus U\}, \Delta, B} Z$ , (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.

Note that it is more efficient to use the variant narrowing strategy defined in [6] than full narrowing for computing the finite variants of a term.

## 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<sup>3</sup> generation of variants. The following notion is useful.

**Definition 8 (Variant-pattern).** *Let  $\mathcal{R} = (\Sigma, E, R)$  be an order-sorted rewrite theory satisfying properties (1)–(6). We call a term  $f(t_1, \dots, t_n)$  a variant-pattern if all subterms  $t_1, \dots, t_n$  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  $X_1, \dots, X_k$  of the appropriate top sorts and there is a substitution  $\theta \in CSU_E(t = f(X_1, \dots, X_k))$  such that  $\theta$  is normalized, where  $t' = f(X_1, \dots, X_k)\theta$ . 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.

<sup>3</sup> 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  $c(f(X), X)$ .



*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  $t_0 \xrightarrow{p_1}_{R,E} t_1 \cdots \xrightarrow{p_n}_{R,E} t_n$  is called variant-preserving if  $t_{i-1}|_{p_i}$  has a variant-pattern for  $i \in \{1, \dots, n\}$  and there is no sequence  $t_0 \xrightarrow{m}_{R,E} t'_m$  such that  $m < n$  and  $t_n =_E t'_m$ . A narrowing sequence  $t_0 \xrightarrow{p_1, \sigma_1}_{R,E} t_1 \cdots \xrightarrow{p_n, \sigma_n}_{R,E} t_n$ ,  $\sigma = \sigma_1 \cdots \sigma_n$ , is called variant-preserving if  $\sigma$  is  $\rightarrow_{R,E}$ -normalized and  $t_0\sigma \xrightarrow{p_1}_{R,E} t_1\sigma \cdots \xrightarrow{p_n}_{R,E} t_n$  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  $t \xrightarrow{\sigma} \xrightarrow{\leq n}_{R,E} s$  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 Appendix B) is a straightforward extension of the standard notion of descendant for rules. Given  $t =_E s$  and  $p \in Pos(t)$ , we write  $p \setminus\!\!\setminus_s$  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  $p \setminus\!\!\setminus_{t_3} = \emptyset$  implies that for all  $p' \leq p$  such that  $p' \setminus\!\!\setminus_{t_3} = \emptyset$ , there exist  $t'_3, t_4, t_5$  such that  $t_1 \xrightarrow{p'}_{R,E} t'_3$ ,  $t_2 \xrightarrow{*}_{R,E} t_4$ ,  $t'_3 \xrightarrow{*}_{R,E} t_5$ , 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  $\sigma$  s.t.  $t\sigma|_p$  is  $\rightarrow_{R,E}$ -reducible and then, let  $p = p_1 \cdot \dots \cdot p_k$ , for  $i \in \{1, \dots, k-1\}$ ,  $t\sigma|_{p_i}$  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.  $\text{Var}(l) \cap \text{Var}(l') = \emptyset$ ) and for all  $X \in \text{Var}(l)$ , the term  $t = l\theta$ , where  $\theta = \{X \mapsto l'\}$  such that  $\theta$  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  $t$ .*

Example 17 in Appendix A proves the variant-preservingness property for the exclusive or theory. 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*<sup>4</sup> 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  $D = \{\text{root}(l) \mid l \rightarrow r \in R\} \uplus \{\text{root}(v) \mid u = v \in E \text{ or } v = u \in E, \text{root}(u) \in D\}$ .*

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  $\text{Ins}_E(R)$  be a set containing only rules of the form  $l\sigma \rightarrow r\sigma$  (where  $\sigma$  is a substitution and  $l \rightarrow r \in R$ ).  $\text{Ins}_E(R)$  is called an instantiation of  $R$  for the equations  $E$  iff  $\text{Ins}_E(R)$  is the smallest set such that: (a)  $R \subseteq \text{Ins}_E(R)$ , (b) for all  $l \rightarrow r \in R$ , all  $v$  such that  $u = v \in E$  or  $v = u \in E$ , and all  $\sigma \in \text{CSU}_E(v = l)$ , there exists a rule  $l' \rightarrow r' \in \text{Ins}_E(R)$  and a variable renaming  $\nu$  such that  $l\sigma =_E l'\nu$  and  $r\sigma =_E r'\nu$ .*

<sup>4</sup> Note that regularity does not imply collapse-free, e.g. equation 1 of Example 1 is regular but also collapsing.

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  $l \rightarrow C[g(t_1, \dots, t_m)]$  is a rule of  $Ins_E(\mathcal{R})$  with  $C$  a context and  $g$  a defined symbol in  $Ins_E(\mathcal{R})$ , then  $\langle l, g(t_1, \dots, t_m) \rangle$  is called a dependency pair of  $\mathcal{R}$ .*

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

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

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

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

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

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

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<sup>5</sup>.

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

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  $\sigma$  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

<sup>5</sup> 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.

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. Indeed, the dependency graphs of Figures 2 and 4 shown in Appendix A consider the estimated dependency graph.

*Example 11.* Creating the dependency graph for Example 10 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. As you can see in Figure 2 in Appendix A, 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:

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

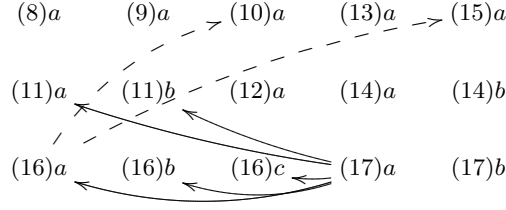
With the new dummy dependency pairs included we get the dependency graph of Figure 4 shown in Appendix A.

**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  $\sigma$  such that  $\sigma$  is  $\rightarrow_{R,E}$ -normalized and the following rewrite sequence obtainable from the chain  $s_1\sigma \rightarrow_{R,E} C_1[t_1]\sigma \xrightarrow{*}_{R,E} C_1[s_2]\sigma \rightarrow_{R,E} C_1[C_2[t_2]]\sigma \xrightarrow{*}_{R,E} \cdots \xrightarrow{*}_{R,E} C_1[C_2[\cdots C_{n-1}[s_n]]]\sigma \rightarrow_{R,E} C_1[C_2[\cdots C_{n-1}[C_n[t_n]]]]\sigma$  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.



**Fig. 1.** Variant-preserving dependency graph

**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. In Appendix A, we show why we can drop some of the cycles and edges in the original dependency graph of Figure 4 shown in Appendix A.

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  $l \rightarrow r \in R$  giving rise to dependency pairs  $dp_1, dp_2, \dots, dp_n$ , its rank is  $rank_{R,E}(l \rightarrow r) = (rank_{R,E}(dp_1) - 1) + (rank_{R,E}(dp_2) - 1) + \dots + (rank_{R,E}(dp_n) - 1) + 1$ . For a defined symbol  $f$ , its rank is  $rank_{R,E}(f) = \max\{rank_{R,E}(l \rightarrow r) \mid l \rightarrow r \in R, \text{root}(l) = f\}$ . For a term  $t$ , its rank is  $rank_{R,E}(t) = \sum_{f \in \mathcal{D}} (rank_{R,E}(f) * \#_f(t))$  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  $\infty$  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 Appendix A, 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  $\text{rank}_{R,E}(f)$  is finite, then  $\mathcal{R}$  has the finite variant property.*

## 6 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 4. There are works devoted to disproving the termination of rewriting [9,16] or disproving the termination of logic programs [17] but, to the best of our knowledge, there are no works on non-termination of narrowing. However, we can give a simple sufficient condition.

**Theorem 7 (Non-termination of narrowing).** *Let  $\mathcal{R} = (\Sigma, E, R)$  be an order-sorted rewrite theory satisfying properties (1)–(6) above. Let  $E$  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 (properly renamed versions of)  $s$  and  $t$  unify, called a self-cycle, then there is an infinite variant-preserving narrowing sequence starting from term  $s$ .*

*Example 15 (ACUNh).* [2] Let us present the ACU example with nilpotence and homomorphism as discussed by Comon and Delaune.<sup>6</sup> This is  $\mathcal{R}_{ACUNh}$ , with  $+$  AC, which has the variant-preserving property:

$$X + 0 \rightarrow X \quad (18) \qquad h(0) \rightarrow 0 \quad (21)$$

$$X + X \rightarrow 0 \quad (19) \qquad h(X + Y) \rightarrow h(X) + h(Y) \quad (22)$$

$$X + X + Y \rightarrow Y \quad (20)$$

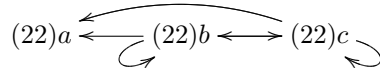
We get the following dependency pairs. For the first four rules we only get the dummy dependency pair, which we do not show here, while for the last rule we get three dependency pairs:

$$(22)a : \langle h(x + y), h(x) + h(y) \rangle \quad (22)b : \langle h(x + y), h(x) \rangle \\ (22)c : \langle h(x + y), h(y) \rangle$$

---

<sup>6</sup> There is another, alternative term rewriting system representing this theory, which suffers from the same problems, so we skip it.

It is easy to see that there are self-cycles in (22)*b* and (22)*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, where the dummy dependency pairs have been omitted:



By Theorem 4, this theory does not have the finite variant property, as also proved in a different way in [2].

## 7 Conclusions

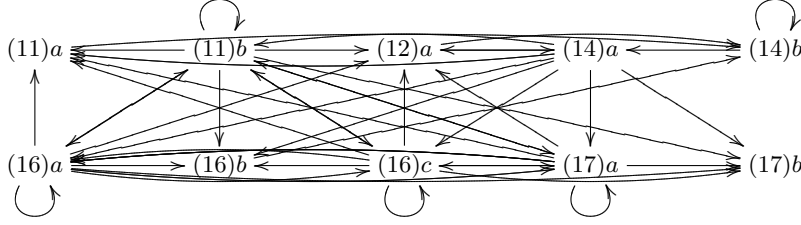
We have recalled Comon-Lundh and Delaune’s finite variant property (FV) and summarized some of its applications. Our main two contributions have been: (i) giving new necessary conditions and new sufficient conditions for FV; and (ii) deriving from these conditions algorithms for checking or disproving 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; and a more accurate analysis of narrowing sequences associated to cycles in the dependency graph will help the disproving 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 [5], a tool for the analysis of cryptographic protocols modulo algebraic properties.

## References

1. T. Arts and J. Giesl. Termination of term rewriting using dependency pairs. *Theor. Comput. Sci.*, 236(1-2):133–178, 2000.
2. H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In J. Giesl, editor, *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2005.
3. H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *LICS*, pages 271–280. IEEE Computer Society, 2003.
4. N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science, Vol. B*, pages 243–320. North-Holland, 1990.
5. S. Escobar, C. Meadows, and J. Meseguer. A rewriting-based inference system for the nrl protocol analyzer and its meta-logical properties. *Theor. Comput. Sci.*, 367(1-2):162–202, 2006.
6. S. Escobar, J. Meseguer, and R. Sasse. Variant narrowing and equational unification. In *Accepted at: 7th International Workshop on Rewriting Logic and its Applications*, 2008.



7. J. Giesl and D. Kapur. Dependency pairs for equational rewriting. In A. Middeldorp, editor, *RTA*, volume 2051 of *Lecture Notes in Computer Science*, pages 93–108. Springer, 2001.
8. J. Giesl, P. Schneider-Kamp, and R. Thiemann. Automatic termination proofs in the dependency pair framework. In U. Furbach and N. Shankar, editors, *IJCAR*, volume 4130 of *Lecture Notes in Computer Science*, pages 281–286. Springer, 2006.
9. J. Giesl, R. Thiemann, and P. Schneider-Kamp. Proving and disproving termination in the dependency pair framework. In F. Baader, P. Baumgartner, R. Nieuwenhuis, and A. Voronkov, editors, *Deduction and Applications, 23.-28. October 2005*, volume 05431 of *Dagstuhl Seminar Proceedings*. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2006.
10. J.-M. Hullot. A catalogue of canonical term rewriting systems. Technical Report CSL-113, SRI International, 1980.
11. J.-P. Jouannaud, C. Kirchner, and H. Kirchner. Incremental construction of unification algorithms in equational theories. In J. Díaz, editor, *ICALP*, volume 154 of *Lecture Notes in Computer Science*, pages 361–373. Springer, 1983.
12. J.-P. Jouannaud and H. Kirchner. Completion of a set of rules modulo a set of equations. *SIAM J. Comput.*, 15(4):1155–1194, 1986.
13. J. Meseguer. Conditioned rewriting logic as a united model of concurrency. *Theor. Comput. Sci.*, 96(1):73–155, 1992.
14. J. Meseguer. Membership algebra as a logical framework for equational specification. In F. Parisi-Presicce, editor, *WADT*, volume 1376 of *Lecture Notes in Computer Science*, pages 18–61. Springer, 1997.
15. J. Meseguer and P. Thati. Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols. *Higher-Order and Symbolic Computation*, 20(1–2):123–160, 2007.
16. É. Payet. Detecting non-termination of term rewriting systems using an unfolding operator. In G. Puebla, editor, *Logic-Based Program Synthesis and Transformation, 16th International Symposium, LOPSTR 2006, Venice, Italy, July 12-14, 2006, Revised Selected Papers*, volume 4407 of *Lecture Notes in Computer Science*, pages 194–209. Springer, 2007.
17. É. Payet and F. Mesnard. Non-termination inference of logic programs. *ACM Trans. Program. Lang. Syst.*, 28(2):256–289, 2006.
18. G. E. Peterson and M. E. Stickel. Complete sets of reductions for some equational theories. *J. ACM*, 28(2):233–264, 1981.
19. TeReSe, editor. *Term Rewriting Systems*. Cambridge University Press, Cambridge, 2003.
20. E. Viola. E-unifiability via narrowing. In A. Restivo, S. R. D. Rocca, and L. Roversi, editors, *ICTCS*, volume 2202 of *Lecture Notes in Computer Science*, pages 426–438. Springer, 2001.
21. P. Viry. Equational rules for rewriting logic. *Theor. Comput. Sci.*, 285(2):487–517, 2002.



**Fig. 2.** Dependency graph of Abelian group

## A Further Examples

*Example 16.* The following equational theory borrowed from [2], denoted  $\mathcal{R}_{DYT}$ , is the classical Dolev-Yao model with explicit destructors such as decryption and projections. Note that the use of explicit destructors in this example is different to the cancellation of public and private encryption/decryption of Example 1.

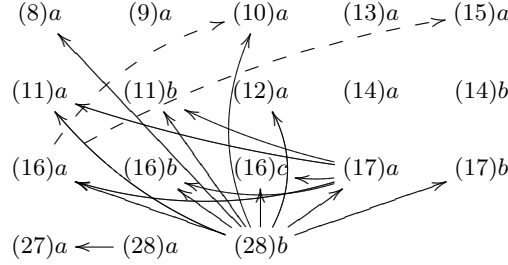
$$\begin{aligned} fst(X; Y) &= X & (23) & & d(e(X, Y), Y^{-1}) &= X & (25) \\ snd(X; Y) &= Y & (24) & & (X^{-1})^{-1} &= X & (26) \end{aligned}$$

This equational theory does not have any equational axiom, i.e., it has a decomposition  $(\Sigma, \emptyset, R)$ . The theory trivially satisfies the finite variant property. Moreover, since  $E = \emptyset$ , it satisfies the variant-preserving property and the associated dependency graph has no cycle. Moreover, the rank function for every defined symbol is 1.

*Example 17.* Let  $\mathcal{R} = (\Sigma, E, R)$  be the exclusive or theory from Example 1, with only (1)–(3) used as rules. Now with Theorem 5 we find this theory to be variant-preserving. All the combinations of rules not involving (3) as the first rule do not have a variant-pattern, let us just show one of the combinations of rule (3) with itself where  $l = X \oplus X \oplus Y$  and  $l' = X' \oplus X' \oplus Y'$ . We will 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 it also has a normalized reduction with another renaming of rule (3), namely  $V \oplus V \oplus W \rightarrow W$ , and substitution  $\sigma = \{V \mapsto X \oplus X', W \mapsto Y'\}$ .

*Example 18.* Consider Example 13 for the variant-preserving dependency pair graph of the Abelian group. For the dependency pair (11)b and its self-loop we need a substitution  $\sigma$  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 (16)a, i.e.,  $\langle s_1, t_1 \rangle = \langle X^{-1} * Y^{-1} * Z, (X * Y)^{-1} * Z \rangle$ , and (17)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  $((X * Y)^{-1} * Z)\sigma =_{AC} ((X' * Y')^{-1} * Y' * Z')\sigma$



**Fig. 3.** Variant-preserving dependency graph for Diffie-Hellman

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, it is not a variant-preserving sequence as there is a shorter rewriting sequence using rule (15)a,  $X'^{-1} * Y'^{-1} * Y' * Z' \rightarrow X'^{-1} * Z'$ , so there is no variant-preserving chain here.

Similarly for the chain from (16)a to (17)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  $*(., Z')$  and so the same shorter rewriting sequence exists.

In the other direction, from (17)a to (16)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  $(X * Y')^{-1} * Y' * Y^{-1} * Z \rightarrow X^{-1} * Y^{-1} * Z \rightarrow (X * Y)^{-1} * Z$ . The alternative rewriting sequence applying the rules in reverse order is  $(X * Y')^{-1} * Y' * Y^{-1} * Z \rightarrow (X * Y' * Y)^{-1} * Y' * Z \rightarrow (X * Y)^{-1} * Z$  which is not shorter, so this is a variant-preserving sequence and thus we have a variant-preserving chain.

For the dependency pairs (16)a, i.e.,  $\langle s_1, t_1 \rangle = \langle X^{-1} * Y^{-1} * Z, (X * Y)^{-1} * Z \rangle$  to (15)a, i.e.,  $\langle s_2, t_2 \rangle = \langle X' * X'^{-1} * Y', Y' \rangle$  with for example substitution  $\sigma' = \{X' \mapsto X * Y, Z \mapsto X * Y * Y'\}$  we have  $s_1\sigma =_{AC} X^{-1} * Y^{-1} * X * Y * Y'$  which has a variant-pattern and the rewrite sequence  $s_1\sigma \rightarrow (X * Y)^{-1} * X * Y * Y' \rightarrow Y'$ . The alternate rewrite sequence is  $s_1\sigma \rightarrow Y^{-1} * Y * Y' \rightarrow Y'$  which is not shorter, so we have a variant-preserving chain.

The arrow for this chain is dotted though as the concatenation of (17)a to (16)a and (16)a to (15)a is not a variant-preserving chain. This becomes obvious when looking at instantiations of the left-hand side of (17)a so that all three rules can be applied in the given order. We get for example the term  $t = (X * Y)^{-1} * Y * Y'^{-1} * X * Y' * Z''$  for which there is a shorter rewrite sequence using rule (15) twice:  $t =_{AC} (X * Y)^{-1} * X * Y * Y'^{-1} * Y' * Z'' \rightarrow Y'^{-1} * Y' * Z'' \rightarrow Z''$ . As this sequence is shorter we do not have a variant-preserving chain here.

*Example 19 (Diffie-Hellman).* We get a rewrite theory representing the Diffie-Hellman theory, called  $\mathcal{R}_{DH}$ , by extending the theory  $\mathcal{R}_*$  from Example 10 by

adding a new binary symbol  $exp$  and the following two rules:

$$exp(x, 1) \rightarrow x \tag{27}$$

$$exp(exp(x, y), z) \rightarrow exp(x, y * z) \tag{28}$$

We can compute the dependency pairs and the associated graph based on the results we already have from Example 13. 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 20 respectively Example 21. The following additional dependency pairs are required, where the first one is a dummy:

$$\begin{aligned} (27)a : & \quad \langle exp(x, 1) \ , \ x \rangle \\ (28)a : & \quad \langle exp(exp(x, y), z) \ , \ exp(x, y * z) \rangle \\ (28)b : & \quad \langle exp(exp(x, y), z) \ , \ y * z \rangle \end{aligned}$$

As you can see in Figure 3, for rule (28) we have two independent possible ways to go. One from the dependency pair (28)a to (27)a, which means we need to potentially take an extra step after applying rule (28). There are a lot of possibilities to go from (28)b, but the longest possible path has length 3. Let us show that there is actually a chain for the path from (28)b via (17)a to (11)a. After substituting as needed for this in the left-hand side of (28) we get  $exp(exp(X, (U * V)^{-1}), V * W^{-1}) \rightarrow exp(X, (U * V)^{-1} * V * W^{-1})$ , let us call this term  $t$ . Then from there we have  $t \rightarrow exp(X, U^{-1} * W^{-1}) \rightarrow exp(X, (U * W)^{-1})$  and alternatively  $t \rightarrow exp(X, (U * V * W)^{-1} * V) \rightarrow exp(X, (U * W)^{-1})$  which is not shorter. So this is really a variant-preserving chain and the rank of (28)b is 3. Overall that means that for rule (28) we have rank 4, and thus  $rank_{R,E}(exp) = 4$ . Therefore our bound for variant narrowing will be as follows: For a term  $t$  we have  $(\#_{exp}(t) * 4) + (\#_*(t) * 2) + \#_{-1}(t)$  as the rank.

*Example 20.* Let us check variant-preservingness for  $\mathcal{R}_*$  by use of Theorem 5. For rule (8) and any other rule there is no variant-pattern for  $l\theta$  where  $\theta$  substitutes another left-hand side into  $X$ . The reason is that the constant 1 needs to stay isolated as otherwise a rewrite is possible, and so the left-hand side that was inserted stays together and is reducible.

As rule (9) does not have any variable, the property holds trivially.

For all following rules let us note that instantiating a variable that is underneath 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 (10)–(14) do not need to be considered as all variables appear at least once underneath an inverse operator.

In this vein for rule (15) we only need to consider the terms created when instantiating  $Y$ . Only combination with (10),(12), (15), and (17) results in a term that has a variant-pattern. Let us show for example (15) with (17) (renamed to variables with a prime). The resulting term is  $X * X^{-1} * (X' * Y')^{-1} * Y' * Z'$  which can be reduced by rule (16) (renamed to variables with two primes) with substitution  $\{X'' \mapsto X, Y'' \mapsto X' * Y', Z'' \mapsto X * Y' * Z'\}$  which is normalized.

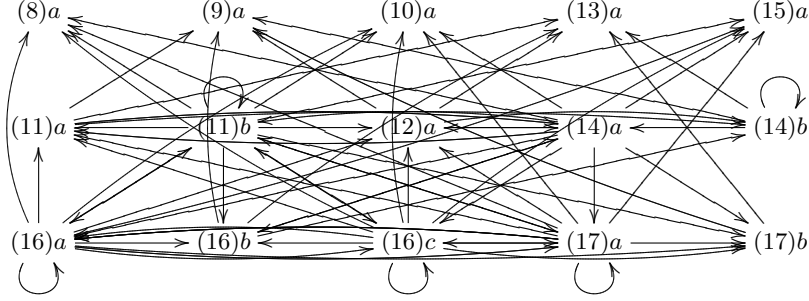


Fig. 4. Dependency graph of Abelian group with dummy dependency pairs

For rule (16) the only useful (read: have a chance at having a variant-pattern) instantiations are for  $Z$ , but also as there are already 2 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 (8) which results in term  $X^{-1} * Y^{-1} * X' * 1$  which also does not have a variant-pattern.

Finally, for rule (17) we only need to instantiate the variable  $Z$ . There are variant-patterns for the combinations with (10), (12), (15), and (17), let us just show the last of these combinations, (17) 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 (16) (renamed with two primes) with the normalized substitution  $\{X'' \mapsto X * Y, Y'' \mapsto X' * Y', Z'' \mapsto Y * Y' * Z'\}$ .

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

*Example 21.* Variant-preservingness of the Diffie-Hellman theory  $\mathcal{R}_{\mathcal{DH}}$  can be shown using Theorem 5 based upon the variant-preservingness of  $\mathcal{R}_*$  shown in Example 20. Let us just observe that  $\mathcal{R}_{\mathcal{DH}}$  is only adding a free symbol 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 2 new rules results in a term that has no variant-pattern. So  $\mathcal{R}_{\mathcal{DH}}$  has the variant-preserving property, too.

## B Proofs

**Theorem 2 (Computing with variant-preserving sequences).** *Let  $\mathcal{R} = (\Sigma, E, R)$  be an order-sorted rewrite theory satisfying properties (1)–(6) and that 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  $t \xrightarrow{\sigma}_{R,E}^{\leq n} s$  such that  $s$  is  $\rightarrow_{R,E}$ -irreducible.*

*Proof.* Let  $t$  be a given term. The *if* part is implied by Proposition 1. For the *only if* part, let us consider a variant  $(s, \sigma)$ , i.e.,  $t\sigma \rightarrow_{R,E}^{\leq n} s$  and  $s$  is irreducible.

Note that  $\sigma$  is  $\rightarrow_{R,E}$ -normalized and so, by completeness, there is at least one narrowing sequence  $t \xrightarrow{\sigma'}_{R,E}^{\leq n} s'$  and substitution  $\rho$  such that  $t\sigma =_E t\sigma'\rho$  and  $s =_E s'\rho$ . Since  $FV_{\Delta,B}(t)$  is complete,  $\sigma$  is a most general substitution and, therefore,  $\sigma' =_E \sigma$ . Finally, such most general narrowing sequence or a shorter one computing the same substitution  $\sigma$  is variant-preserving.  $\square$

**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.*

*Proof.* Given a term  $t$ , we denote by  $\#(t)$  the length of the longest variant-preserving narrowing sequence from  $t$ . Such longest sequence exists by the FVNS property. Given a term  $t$  and  $\#(t) = n$ , we prove that, for any substitution  $\sigma$ ,  $t(\sigma \downarrow_{R,E}) \rightarrow_{R,E}^{\leq n} (t\sigma) \downarrow_{R,E}$  by induction on  $n$ .

- ( $n = 0$ ) Then  $t$  is irreducible and, for any substitution  $\sigma$ ,  $t(\sigma \downarrow_{R,E})$  is also irreducible.
- ( $n > 0$ ) Let  $t = f(t_1, \dots, t_k)$  and  $\sigma$  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  $t_1, \dots, t_k$ . We have  $\#(t_i) < \#(t)$ . By induction hypothesis, for any substitution  $\sigma$ ,  $t_i(\sigma \downarrow_{R,E})$  is bounded by  $\#(t_i)$  for  $i \in \{1, \dots, k\}$ . Let us pick any variant  $(t'_i, \rho_i)$  for each  $t_i$ ,  $i \in \{1, \dots, k\}$  such that  $(\rho_1 \cdots \rho_k) \leq_E \sigma$ . Let  $t' = f(t'_1, \dots, t'_k)$ . By variant-preservingness, there is a rule  $l \rightarrow r \in R$  and a normalized substitution  $\theta$  such that  $t' =_E l\theta$ . Since  $\#(r) < \#(t)$ , we can apply the induction hypothesis and, for any substitution  $\sigma'$ ,  $r(\sigma' \downarrow_{R,E})$  is bounded by  $\#(r)$ . Since  $\theta$  is normalized,  $r\theta$  is also bounded by  $\#(r)$ . Note that  $\#(t_1) + \dots + \#(t_k) + \#(r) < \#(t)$ . Thus, for any substitution  $\sigma$ ,  $t\sigma$  is bounded by  $\#(t)$ .  $\square$

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

*Proof.* By contradiction. Let us consider that  $\mathcal{R}$  satisfies the finite variant property and take an infinite variant-preserving narrowing sequence. We can take any finite prefix  $t \xrightarrow{\sigma^*}_{R,E} s$  and build a variant-preserving rewrite sequence  $t\sigma \xrightarrow{\sigma^*}_{R,E} (t\sigma) \downarrow_{R,E}$ . Thus, we obtain an infinite number of rewrite sequences with increasing length. Since the theory is terminating for rewriting, the rewrite sequences are increasing in length because of the computed substitutions. Finally, this contradicts the boundedness property.  $\square$

We recall here the notion of *descendants* of a position in a rewrite sequence.

**Definition 21 (Descendants).** [19] Let  $A : t \xrightarrow{p} l \rightarrow r$   $s$  and  $q \in \text{Pos}(t)$ . The set  $q \parallel A$  of descendants of  $q$  in  $s$  is defined as follows:

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

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

**Definition 22 ( $E$ -descendants).** Let  $E$  be a set of regular and sort-preserving  $\Sigma$ -equations. Let  $\overleftrightarrow{E} = \{u \rightarrow v \mid u = v \text{ or } v = u \in E\}$ . Given two terms  $t =_E s$ , i.e.,  $A : t \xrightarrow{*} s$ , and a set  $Q$  of pairwise disjoint positions in  $t$ , the  $E$ -descendants of  $Q$  in  $s$  are  $Q \parallel_s = Q \parallel A$ .

**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.  $\text{Var}(l) \cap \text{Var}(l') = \emptyset$ ) and for all  $X \in \text{Var}(l)$ , the term  $t = l\theta$ , where  $\theta = \{X \mapsto l'\}$  such that  $\theta$  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, let  $t = f(t_1, \dots, t_k)$  with  $t_1, \dots, t_k \rightarrow_{R,E}$ -irreducible terms. If  $t$  is irreducible, then we are done. Otherwise  $t$  is reducible and there is a rule  $l \rightarrow r$  and a substitution  $\theta$  s.t.  $t =_E l\theta$ . Let  $n$  be the number of redexes in  $\theta$ . We prove, by induction on  $n$ , that there exists a rule  $l' \rightarrow r' \in R$  and a substitution  $\theta'$  s.t.  $t =_E l'\theta'$  and  $\theta'$  is  $\rightarrow_{R,E}$ -normalized.

( $n = 0$ ) Then,  $\theta$  is  $\rightarrow_{R,E}$ -normalized and we are done.

( $n > 0$ ) Let  $X \mapsto u$  be a binding in  $\theta$  s.t.  $u$  is reducible. We prove below that  $u$  is reducible at the top and, thus, let us just assume it. Let  $l' \rightarrow r' \in R$  and  $\theta'$  be such that  $u =_E l'\theta'$ . Let us assume  $\text{Var}(l') \cap \text{Var}(l) = \emptyset$ . Let  $\sigma = \{X \mapsto l'\}$ . There is a substitution  $\rho$  s.t.  $t =_E l\sigma\rho$ , i.e.,  $\theta|_{\text{Var}(t)} =_E (\sigma\rho)|_{\text{Var}(t)}$ . Then, by the condition given in the Theorem, there is a normalized substitution on  $l\sigma$ , i.e., there is a rule  $l'' \rightarrow r''$  and a substitution  $\theta''$  such that  $l\sigma =_E l''\theta''$  and  $\theta''$  is  $\rightarrow_{R,E}$ -normalized. Now, when we consider the term  $l''\theta''\rho$ , we can apply the induction hypothesis because  $\rho$  contains less redexes than  $\theta$  and we obtain that there is a rule  $l''' \rightarrow r'''$  and a substitution  $\theta'''$  such that  $t =_E l''\theta''\rho =_E l'''\theta'''$  and  $\theta'''$  is  $\rightarrow_{R,E}$ -normalized.

Finally, given  $t = f(t_1, \dots, t_k)$  with  $t_1, \dots, t_k \rightarrow_{R,E}$ -irreducible terms, rule  $l \rightarrow r$  and substitution  $\theta$  s.t.  $t =_E l\theta$ , and such that  $X \mapsto u$  is a binding in  $\theta$  s.t.  $u$  is reducible, we just have to prove that  $u$  is reducible at the top. Let us prove it by contradiction. Let  $p_1, \dots, p_m$  be the topmost reducible positions

in  $u$  s.t.  $p_i \neq \Lambda$  for  $i \in \{1, \dots, m\}$ . Let us pick one  $i \in \{1, \dots, m\}$ . Let  $p_X$  be any position of variable  $X$  in  $l$ . Since  $t_1, \dots, t_k$  are irreducible, position  $p_X.p_i \in Pos(l\theta)$  does not have any  $E$ -descendant in  $t$ , i.e.,  $p_X.p_i \parallel_t = \emptyset$ . Otherwise, it will be a clear proper subterm of one of  $t_1, \dots, t_k$ . But,  $p_X.p_i \parallel_t = \emptyset$  implies by upper- $E$ -coherence that  $(l\theta)|_{p_X} = u$  must be reducible, which contradicts the assumption.  $\square$