The finite variant property: How to get rid of some algebraic properties. *

Hubert Comon-Lundh[2] and Stéphanie Delaune[1,2]

[1] France Télécom R&D
[2] Laboratoire Spécification & Vérification
ENS de Cachan & CNRS UMR 8643
61, avenue du Président Wilson,
94235 CACHAN Cedex, FRANCE
email: comon,delaune@lsv.ens-cachan.fr

Abstract. We consider the following problem: Given a term t, a rewrite system $\mathcal{R}$, a finite set of equations E' such that $\mathcal{R}$ is E'-convergent, compute finitely many instances of t: $t_1, \ldots, t_n$ such that, for every substitution σ, there is an index i and a substitution θ such that $t\sigma\!\downarrow \,=_{E'} t_i\theta$ (where $t\sigma\!\downarrow$ is the normal form of $t\sigma$ w.r.t. $\rightarrow_{E'\backslash\mathcal{R}}$).
The goal of this paper is to give equivalent (resp. sufficient) conditions for the finite variant property and to systematically investigate this property for equational theories, which are relevant to security protocols verification. For instance, we prove that the finite variant property holds for Abelian Groups, and a theory of modular exponentiation and does not hold for the theory *ACUNh* (Associativity, Commutativity, Unit, Nilpotence, homomorphism).

1 Introduction

In our recent work on the verification of cryptographic protocols [3, 5] we came twice across the following problem:

> Given an AC-convergent rewrite system $\mathcal{R}$, is it possible (and how) to compute from any term t a finite set of instances $t\sigma_1, \ldots, t\sigma_n$ such that
>
> $$\{t\sigma\!\downarrow_{\mathcal{R}} \mid \sigma \in \Sigma\} = \bigcup_{i=1}^{n} \{t\sigma_i\!\downarrow_{\mathcal{R}}\theta \mid \theta \in \Sigma\}$$
>
> where Σ is the set of normalized substitutions and $u\!\downarrow_{\mathcal{R}}$ is the AC-normal form of u w.r.t. $\mathcal{R}$.

In other words, the reductions in $t\sigma$ only depend on reductions in finitely many (fixed) instances of t. This is typically what we will call the *finite variant property*: compute in advance all possible normal forms of an instance of t,

* This work has been partly supported by the RNTL project PROUVÉ 03V360 and the ACI-SI Rossignol.

independently of that instance. In [3], this problem is solved in an ad hoc way when $\mathcal{R}$ is the theory of exclusive or (also called the *ACUN* theory), given by the rewrite rules:

$$\begin{aligned} x + x &\to 0 \\ x + x + y &\to y \\ x + 0 &\to x \end{aligned}$$

and the associativity and commutativity axioms for $+$. Such a property, together with the finiteness of equivalence classes modulo E' is claimed to be the key property for decidability results in cryptographic protocols verification, in presence of algebraic properties [2]. That is why we are especially interested in studying the finite variant property for equational theories which are relevant to cryptography and which define infinite equivalence classes.

When $E' = \emptyset$, it is not difficult to see that the finite variant property is implied by the termination of basic narrowing. This is not so easy in general. Assume for instance that E' consists in the axioms of associativity and commutativity and E is defined by an AC-convergent rewrite system $\mathcal{R}$. On one hand, general AC-narrowing does not terminate, even for a single rule $y + x + x \to y$ and, on the other hand, basic narrowing is incomplete for E-unification. We didn't find any reference for the incompleteness of basic AC-narrowing, hence we show it in Section 3.2. E. Viola already noticed in [19] that the standard completeness proof of basic narrowing does not extend to the AC-case and proposes another narrowing strategy, introducing extensions of rules. This notion of narrowing restores completeness. However, termination is lost, even in simple cases. Even for equational theories presented by E'-convergent rewrite systems, basic narrowing might not terminate, while E has the finite variant property. This is the case for Abelian Groups, as we will see in Section 6.2.

The first contribution of this paper is to state a property (called *boundedness*) equivalent to the finite variant property in case of theories defined by convergent rewrite systems (Section 5.2). This is very similar to the existence of "narrowing bounds" in [19]. We differ in two respects: first we consider only terms (not unification problems) and second, there is a quantifier switch. Roughly, in [19], the "narrowing bound" is equivalent to "there exists a normalized θ such that ($t\theta\!\downarrow\, =_{AC} u$ and) all (inner) derivations starting from $t\theta$ are bounded". In our case, boundedness is equivalent to "for every normalized θ, there is a derivation from $t\theta$ to its normal form whose length is bounded".

Second, we give sufficient conditions for the boundedness property, which do not necessarily imply the termination of narrowing (Section 6.2) and prove that these conditions are met for several equational theories, which are relevant to cryptographic protocols. Our sufficient criteria is related to the notion of *optimally reducing* (AC)-term rewriting system introduced in [14]. Indeed being an optimally reducing rewrite system is a sufficient condition to satisfy our criteria, and therefore the boundedness property. We provide however with strictly weaker sufficient conditions and therefore new applications. For instance, we show that the theory of Abelian Groups has the boundedness property, relying on the unusual orientation of the inverse rule (Section 6.2). We use proof techniques which are similar to those of [12]. We also show in Section 7 that there are equational theories for which unifiability is in PTIME, while there is no convergent AC-rewrite system for the theory yielding the finite variant property.

Finally, we give some side-applications of the finite variant property: for instance the existential fragment of the theory of $\mathcal{T}(\mathcal{F})/{=_E}$ is decidable for the theories E under study.

We start with recalling some definitions in Section 2. We state in Section 3 some results on basic and equational narrowing (for instance the incompleteness of basic AC-narrowing). Next, we list in Section 4, some examples of equational theories, which are relevant to cryptographic protocols, explaining briefly where they come from. In Section 5, we state formally a definition of the finite variant property and give a characterization (the *boundedness property*) when the equational theory is presented by a finite E'-convergent rewrite system. Then, we briefly consider the case of $E' = \emptyset$ in Section 6.1. In Section 6.2 we give sufficient conditions for the boundedness property and then apply them to the relevant theories listed in Section 4. In Section 7, we prove that the theory $ACUNh$ (Associativity, Commutativity, Unit, Nilpotence, homomorphism), for which unifiability is in PTIME [13], does not have the finite variant property. In Section 8, we show other applications of the finite variant property, and we conclude in Section 9.

Missing proofs can be found in [4].

2 Preliminaries

2.1 Terms, Substitutions, Unification

We use classical notations and terminology from [7] on terms, unification, rewrite systems. $\mathcal{T}(\mathcal{F}, \mathcal{X})$ is the set of terms built over the finite (ranked) alphabet $\mathcal{F}$ of function symbols and the set of variable symbols $\mathcal{X}$. $\mathcal{T}(\mathcal{F}, \emptyset)$ is also written $\mathcal{T}(\mathcal{F})$. The set of positions of a term t is written $O(t)$, and $\bar{O}(t)$ is the set of non-variable positions of t. The empty sequence Λ denotes the top-most position. The subterm of $t \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ at position $p \in O(t)$ is written $t|_p$. The term obtained by replacing $t|_p$ with u is denoted $t[u]_p$. The set of variables occurring in t is denoted $vars(t)$.

A substitution σ is a mapping from a finite subset of $\mathcal{X}$ called its domain and written $dom(\sigma)$ to $\mathcal{T}(\mathcal{F}, \mathcal{X})$. Substitutions are extended to endomorphisms of $\mathcal{T}(\mathcal{F}, \mathcal{X})$ as usual. We use a postfix notation for their application.

If E is a set of equations (unordered pair of terms), $=_E$ is the least congruence on $\mathcal{T}(\mathcal{F}, \mathcal{X})$ such that $u\sigma =_E v\sigma$ for all pairs $u = v \in E$ and substitutions σ. E is *regular* if, for every equation $t_1 = t_2 \in E$, $vars(t_1) = vars(t_2)$. Two terms s, t are E-unifiable if there is a substitution σ such that $s\sigma =_E t\sigma$. Such a substitution is called an E-unifier of s, t. We say that there is an E-unification algorithm if it is possible, for any two terms s, t, to compute a finite set $\sigma_1, \ldots, \sigma_n$ of E-unifiers of

s, t, such that, for every E-unifier σ of s, t, there is an index i and a substitution θ such that, for every variable $x \in vars(s) \cup vars(t)$, $x\sigma =_E x\sigma_i\theta$.

2.2 Equational Rewriting

A *term rewriting system* (TRS) is a finite set of *rewrite rules* $l \to r$ where $l \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ and $r \in \mathcal{T}(\mathcal{F}, vars(l))$. A term $s \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ rewrites to t by a TRS $\mathcal{R}$, denoted $s \to_{\mathcal{R}} t$, if there is $l \to r$ in $\mathcal{R}$, $p \in O(s)$ and a substitution σ such that $s|_p = l\sigma$ and $t = s[r\sigma]_p$. The term $l\sigma$ is called a redex and we say that t rewrites to s by contracting the redex $l\sigma$. An innermost redex does not contain other redexes and in an innermost reduction sequence only innermost redexes are contracted. $\mathcal{R}^=$ is the symmetric closure of $\mathcal{R}$. $\xrightarrow{*}_{\mathcal{R}}$ is the reflexive and transitive closure of $\to_{\mathcal{R}}$. We write $t \xrightarrow{\leq n}_{\mathcal{R}} u$ if there is a reduction sequence of at most n steps from t to u. A TRS $\mathcal{R}$ is *terminating* if there are no infinite chains $t_1 \to_{\mathcal{R}} t_2 \to_{\mathcal{R}} \ldots$.

As in [7], given a set of rewrite rules $\mathcal{R}$ and a set of equations E, *rewriting modulo* E, is the relation $\to_{E\backslash\mathcal{R}}$ (others have used $\to_{\mathcal{R},E}$) defined as follows: $s \to_{E\backslash\mathcal{R}} t$ iff there exists a position $p \in O(s)$ such that $s|_p =_E l\sigma$ and $t = s[r\sigma]_p$ for some substitution σ and rule $l \to r \in \mathcal{R}$.

A rewrite system $\mathcal{R}$ is E-confluent if and only if for every s, t such that $s =_{\mathcal{R}^= \cup E} t$, there exists s', t' such that $s \xrightarrow{*}_{E\backslash\mathcal{R}} s'$, $t \xrightarrow{*}_{E\backslash\mathcal{R}} t'$, and $s' =_E t'$. It said to be E-convergent if, in addition, $=_E \circ \to_{\mathcal{R}} \circ =_E$ is well founded.

A term t is in *normal form* (w.r.t. $\to_{E\backslash\mathcal{R}}$) if there is no term s such that $t \to_{E\backslash\mathcal{R}} s$. If $t \xrightarrow{*}_{E\backslash\mathcal{R}} s$ and s is in normal form then we say that s is a normal form of t. When this normal form is unique, we write $s = t{\downarrow}_{E\backslash\mathcal{R}}$ or shortly $s = t{\downarrow}$ when $E\backslash\mathcal{R}$ is clear from the context. A substitution σ is called *normalized* if for every $x \in dom(\sigma)$, $x\sigma$ is in normal form. We write $\sigma =_E \theta$ if $\forall x \in dom(\sigma) \cup dom(\theta)$ $x\sigma =_E x\theta$. For an E-convergent rewrite system $\mathcal{R}$ and a substitution σ, we write $\sigma{\downarrow}_{E\backslash\mathcal{R}}$ the substitution whose domain is $dom(\sigma)$ and such that $x(\sigma{\downarrow}_{E\backslash\mathcal{R}}) = (x\sigma){\downarrow}_{E\backslash\mathcal{R}}$ for all $x \in dom(\sigma)$.

3 Narrowing

Given a TRS $\mathcal{R}$, we say that a term t *narrows to* t' *with the substitution* σ, at $p \in \bar{O}(t)$, by $l \to r \in \mathcal{R}$ if there exists a renaming $l' \to r'$ of $l \to r \in \mathcal{R}$ such that σ is a unifier of $t|_p$ and l' and $t' = (t[r]_p)\sigma$. In this case, we write $t \rightsquigarrow_\sigma t'$. We write $t \overset{*}{\rightsquigarrow}_\sigma t'$ if there exists a narrowing derivation $t = t_1 \rightsquigarrow_{\sigma_1} t_2 \ldots \rightsquigarrow_{\sigma_{n-1}} t_n = t'$ such that $\sigma = \sigma_1 \ldots \sigma_{n-1}$.

3.1 Equational Narrowing

If E is a set of equations such that an E-unification algorithm exists, we define E-narrowing as expected (σ is an E-unifier of $t|_p$ and l).

The following lemma states that every rewrite derivation ($\xrightarrow{*}_{E\backslash\mathcal{R}}$) can be lifted to a narrowing derivation.

Lemma 1 (lifting lemma). *Let E be a regular presentation for which an E-unification algorithm exists. Let t be a term, θ be a normalized substitution and $t\theta \xrightarrow{*}_{E\backslash\mathcal{R}} s'$. Then there exists a term t', a substitution σ and a normalized substitution θ' such that:*

1. $t \overset{*}{\rightsquigarrow}_{\sigma} t'$,
2. $t'\theta' =_E s'$,

Furthermore, the narrowing derivation $t \overset{*}{\rightsquigarrow}_{\sigma} t'$ and the rewrite sequence from $t\theta$ to s' use the same rewrite rules at the same positions.

We didn't find this lemma in the litterature. A similar lemma, but only for a one step derivation, and without the regularity assumption, is proved in [11] for instance. The proof does not extend to an arbitrary derivation length. Actually, we do not know whether or not the lemma would still hold without the regularity assumption (which we indeed use in the proof).

3.2 Basic Narrowing

Definition 1 (basic positions). *Let $t_1 \rightsquigarrow_{\sigma_1} t_2 \rightsquigarrow_{\sigma_2} \ldots \rightsquigarrow_{\sigma_{n-1}} t_n$ be a narrowing derivation. We assume that the i^{th} step has been done at position p_i with the rule $l_i \to r_i$. We inductively define sets of positions $B_1, \ldots, B_n$ as follows:*

$$B_1 = \bar{O}(t) \qquad\qquad B_{i+1} = \mathcal{B}(B_i, p_i, r_i) \quad \text{for } 1 \leq i < n.$$

Here $\mathcal{B}(B_i, p_i, r_i)$ abbreviates $(B_i - \{q \in B_i | p_i \leq q\}) \cup \{p_i.q | q \in \bar{O}(r_i)\}$. Positions in B_i are referred to as basic positions. We say that the above narrowing derivation is basic if $p_i \in B_i$ for $1 \leq i < n$.

In the same way, a rewrite sequence (w.r.t. $E\backslash\mathcal{R}$) $t_1 \to t_2 \to \ldots \to t_n$ is based on a set of positions $B_1 \subseteq \bar{O}(t_1)$ if $p_i \in B_i$ for $1 \leq i < n$ with $B_2, \ldots, B_{n-1}$ defined as above.

Note that the latter is well-defined since $\to_{E\backslash\mathcal{R}}$ preserves the positions which are not in the redex.

In case of non-equational narrowing, there are several well-known results, for instance:

Lemma 2 ([8]). *Let t be a term and σ a normalized substitution. Every innermost derivation sequence (w.r.t $\mathcal{R}$) starting from $t\sigma$ is based on $\bar{O}(t)$.*

It follows that basic narrowing is a complete unification procedure when $\mathcal{R}$ is a convergent rewrite system. The situation is quite different for equational narrowing. For instance in the case of AC-narrowing, Lemma 2 fails (contrary to what is suggested in [11]), as shown by the following example (this has also been noticed in [19]).

Example 1. Let $\mathcal{R}_+ = \{x+0 \to x, x+x \to 0, x+x+y \to y\}$, which is known to be AC-convergent. Let $t = x_1 + x_2$ and $\sigma = \{x_1 \mapsto a+b, x_2 \mapsto a+b\}$. Consider the following innermost derivation (w.r.t. $AC\backslash\mathcal{R}_+$) starting from $t\sigma$.

$$(a+b)+(a+b) \quad \xrightarrow{\Lambda}_{x+(x+y)\to y} \quad b+b \quad \xrightarrow{\Lambda}_{x+x\to 0} \quad 0$$

The first rewriting step takes place at position $\Lambda \in B_1 = \bar{O}(t)$ with the rewriting rule $x+(x+y) \to y$. Hence the set B_2 is empty. So the above rewrite sequence is not based on $\bar{O}(t)$ although it is an innermost derivation.

This example can be generalized in such a way that there is a derivation from $t\sigma$ whose length is arbitrarily long. However, there is also another derivation whose length is short (1 in the above example).

Not only Lemma 2 fails, but actually basic AC-narrowing is not complete, as shown by the following example.

Example 2. We consider the following rewrite system $\mathcal{R}$, in which $+$ is an AC-symbol and a, b are constants:

$$\begin{array}{rcc} a+a \to 0 & b+b \to 0 & a+a+x \to x \\ b+b+x \to x & 0+x \to x & \end{array}$$

$\mathcal{R}$ is AC-convergent. $\sigma = \{x_1 \mapsto a+b;\ x_2 \mapsto a+b\}$ is a solution of the equation $x_1 + x_2 = 0$, whereas there is no narrowing derivation yielding a more general solution. Indeed, narrowing with one of the first two rules yields $x_1 = x_2 = a$ or $x_1 = x_2 = b$, narrowing with the last rule yields $x = 0 \wedge x + 0 = x_1 + x_2$, which do not subsume σ. Narrowing with one of the two other rules, for example $a+a+x \to x$, yields $x = 0 \wedge a+a+x = x_1 + x_2$, again not wanted.

4 Some Relevant Equational Theories

We list here some algebraic theories which are relevant to cryptographic protocols and which we investigate in Section 6. We only consider theories for which equivalence classes are infinite. We use the notations which are customary in cryptographic protocol descriptions. In particular, the pairing symbol $\langle \_, \_ \rangle$ is used in infix notation and encrypting m with k is written $\{m\}_k$.

4.1 Explicit Destructors

The *Axiomatized Dolev-Yao Theory* (DYT) is the classical Dolev-Yao model with explicit destructors such as decryption and projections. Here is a presentation of this theory:

$$\pi_i(\langle x_1, x_2 \rangle) = x_i \ \text{ for } i = 1,2 \qquad d(\{x\}_y, y^{-1}) = x \qquad {x^{-1}}^{-1} = x$$

In words, projections are inverses of pairing, and decrypting with k^{-1} a message encrypted with a key k gives back the plain text message. Alternatively, projections and decryption symbols are not part of the alphabet and such properties are part of the intruder deduction rules. Putting such rules in the equational theory or in the intruder deduction rules seems to be a matter of taste. However, there are subtle differences between the two approaches; some protocols can be attacked if we consider explicit destructors, while they cannot otherwise (see for instance [6]). This relies on the ability to apply the decryption algorithm $d(\_,\_)$ on a message x with a key y, even when x is not a cyphertext.

Proposition 1. *Orienting equations of* DYT *from left to right and adding* $d(\{x\}_{y^{-1}}, y) \rightarrow x$*, we get a convergent rewrite system* $\mathcal{R}_{\mathrm{DYT}}$*. Furthermore (basic) narrowing w.r.t.* $\mathcal{R}_{\mathrm{DYT}}$ *terminates.*

The *Key Inverse Theory* (KIT) is obtained by extending DYT with the equation $\{d(x,y)\}_{y^{-1}} = x$. It expresses that decryption and encryption with the inverse key are inverse of each other. This property holds when decryption is just an encryption with the inverse key, as for the cryptosystem RSA.

Proposition 2. *Orienting equations of* KIT *from left to right and adding the rules* $d(\{x\}_{y^{-1}}, y) \rightarrow x$ *and* $\{d(x, y^{-1})\}_y \rightarrow x$*, we get a convergent rewrite system* $\mathcal{R}_{\mathrm{KIT}}$*. Furthermore (basic) narrowing w.r.t.* $\mathcal{R}_{\mathrm{KIT}}$ *terminates.*

4.2 Exclusive Or Theory ($\boldsymbol{ACUN}$)

This theory has been given in introduction. It is mandatory when protocols rely on exclusive or ([15] vs [17]). As recalled in Example 1, the rewrite system $\mathcal{R}_+$ for this theory is AC-convergent.

4.3 Abelian Groups Theory ($\mathcal{AG}$)

The Abelian Groups theory is defined by the following set of equations:

$$\begin{array}{cc} x * (y * z) = (x * y) * z & x * x^{-1} = 1 \\ x * y = y * x & x * 1 = x \end{array}$$

Proposition 3. *Adding the consequences:* $1^{-1} = 1$, $x^{-1^{-1}} = x$, $(x * y)^{-1} = x^{-1} * y^{-1}$, $x * (y * x^{-1}) = y$ *and orienting the rules from left to right, we get* $\mathcal{R}_*$*, an* AC*-convergent rewrite system for* $\mathcal{AG}$*.*

Note that, AC-narrowing (even basic) is not terminating w.r.t. $\mathcal{R}_*$, as we have an infinite derivation starting from x^{-1} by using repeatedly $(x * y)^{-1} \rightarrow x^{-1} * y^{-1}$.

4.4 Diffie-Hellman Theory ($\mathcal{DH}$)

This theory contains the axioms of the Abelian Groups theory for the symbol $*$ and two others equations concerning the modular exponentiation's symbol:

$$exp(x, 1) = x \qquad exp(exp(x, y), z) = exp(x, y * z)$$

This theory takes into account simple properties of product and exponentiation, which are widely used in protocol constructions. Exponentiation has more properties, which should be considered to capture to whole power of an attacker. However, we only consider the two above axioms since, as shown in [10], many extensions yield undecidable unification problems, hence undecidability of confidentiality, even for a bounded number of sessions.

4.5 Combinations

The theory *ACUNh* consists of the axioms of *ACUN* for $+$ and the equation $h(x+y) = h(x) + h(y)$. This theory is used in protocols such as the TMN protocol (h is used to model an encryption with the public-key of the server S).

The equation $h(x+y) = h(x) + h(y)$ can be oriented in both directions, yielding two AC-convergent rewrite systems, which are displayed in Figure 1: depending on the orientation, we get either 5 rules ($\mathcal{R}_1$) or 6 rules ($\mathcal{R}_2$).

$$\begin{array}{rcl} x+0 \rightarrow x & \qquad & \mathcal{R}_1 : h(x+y) \rightarrow h(x)+h(y) \\ x+x \rightarrow 0 & & \\ x+x+y \rightarrow y & & \mathcal{R}_2 : h(x)+h(y) \rightarrow h(x+y) \\ h(0) \rightarrow 0 & & \qquad h(x)+h(y)+z \rightarrow h(x+y)+z \end{array}$$

Fig. 1. The Rewrite Systems $\mathcal{R}_1$ and $\mathcal{R}_2$ for the *ACUNh* Theory.

Proposition 4. *$\mathcal{R}_1$ and $\mathcal{R}_2$ are AC-convergent.*

5 The Finite Variant Property

We come to the central notion of our paper: a property, which allows to reduce equational theories to some (supposedly simpler) other theory. Let us first recall the definitions given in introduction.

5.1 Definition and a First Characterization

We assume given a well founded ordering $\geq$ on terms, which is total on ground terms. Given a theory E and a ground term t, we write $t{\downarrow_E}$ the smallest term in the equivalence class of t. It will serve as a representative of the class.

Definition 2 (E-variants). *Given two sets of equations E, E', t' is an E-*variant *of a term t if there is a substitution θ such that $t\theta =_E t'$. A* complete set of E-variants modulo E' *of t (w.r.t. $\geq$) is a set S of E-variants of t such that, for every substitution σ, there is a term $t' \in S$ and a substitution θ such that $t\sigma{\downarrow_E} =_{E'} t'\theta$.*

Example 3. Assume $E = ACUN$ and $E' = AC$. Consider the term $x + f(x+y)$. A complete set of E-variants modulo AC is given by the single variable z. Indeed,

$$(x+f(x+y))\{x \mapsto f(z)+z; y \mapsto f(z)\} =_{AC} f(z)+z+f(f(z)+z+f(z)) =_{ACUN} z$$

hence z is a variant of $x + f(x + y)$. This is a complete set since, for every normalized substitution σ, $(x + f(x + y))\sigma\!\downarrow =_{AC} z\theta$ for some θ.

Definition 3 (finite variant property). *The pair (E, E') has the* finite variant property *(w.r.t. $\geq$) if for every term t, we can effectively compute a finite complete set of E-variants modulo E'.*

Sometimes, we will simply say variants and complete set of variants when E and E' are clear from the context.

Now, we need a (uniform) way to compute the E-variants of a term. That is why we will restrict our attention to theories E for which there exists $\mathcal{R}$ and E' such that $\mathcal{R}$ is an E'-convergent system for E. Then the ordering $\geq$ will be chosen in such a way that $\rightarrow_{E'\backslash\mathcal{R}} \subseteq \geq$. To summarize now, our aim is, given a theory E, to find a splitting of E in $(\mathcal{R}, E')$ and an ordering $\geq$ such that:

1. $\mathcal{R}$ is an E'-convergent system for E and $\rightarrow_{E'\backslash\mathcal{R}} \subseteq \geq$ is a decidable relation,
2. for every term t, there is a finite set of variants $t_1, \ldots, t_n$, effectively computable, such that, for every substitution σ, there is an index i and a substitution θ such that $t\sigma\!\downarrow_{E'\backslash\mathcal{R}} =_{E'} t_i\theta$.

We will simply say that $(\mathcal{R}, E')$ is a *decomposition* of E satisfying the *finite variant property* if the two above properties are satisfied. There are several well-known techniques to obtain presentations satisfying the first condition. Hence, we focus on the second condition.

The following lemma shows that, if $(\mathcal{R}, E')$ has the finite variant property, we may not only compute in advance some instances t_i of t such that $t\sigma\!\downarrow$ is always an instance of some t_i, but actually compute in advance substitutions θ_i such that $t_i = t\theta_i\!\downarrow$ is a complete set of variants and every normalized substitution can be factorized through θ_i.

Lemma 3. *A decomposition $(\mathcal{R}, E')$ has the finite variant property iff*

For every term t, there is a finite set of substitutions $\Sigma(t)$ such that

$$\forall \sigma\ \exists \theta \in \Sigma(t),\ \exists \tau.\ \sigma\!\downarrow =_{E'} \theta\tau \quad \wedge \quad (t\sigma)\!\downarrow =_{E'} (t\theta)\!\downarrow\!\tau$$

Proof sketch: The if part is straightforward. Conversely, let T be the term $\langle t, \langle x_0, \langle \ldots, x_n \rangle\rangle\rangle$ where $\{x_0, \ldots, x_n\} = vars(t)$ and $\langle \_, \_ \rangle$ is a free binary function symbol. We apply the hypothesis to T. This yields a definition of $\Sigma(t)$. $\square$

5.2 The Boundedness Condition

In what follows we assume we are given a theory E for which there exists $\mathcal{R}$ and E' such that $\mathcal{R}$ is an E'-convergent system for E.

Definition 4 (boundedness property). *$(\mathcal{R}, E')$ satisfies the* boundedness property *if for every term t, there exists an integer n such that for every normalized substitution σ, the normal form of $t\sigma$ is reachable by a derivation whose length can be bounded by n (thus independently of σ):*

$$\forall t, \exists n, \forall \sigma.\ t(\sigma\downarrow) \xrightarrow{\leq n}_{E'\backslash\mathcal{R}} (t\sigma)\downarrow$$

The following theorem shows the relationships between the boundedness condition and the finite variant property.

Theorem 1. *Let E' be a regular presentation for which an E'-unification algorithm exists. If moreover $(\mathcal{R}, E')$ satisfies the boundedness property then $(\mathcal{R}, E')$ is a decomposition of E satisfying the finite variant property.*
Conversely, if $(\mathcal{R}, E')$ satisfies the finite variant property, then it satisfies the boundedness property.

Proof sketch: The first implication is actually similar to a result in [19]: we use narrowing, however bounding the length of derivation. For the converse, let t be any term. We first apply Lemma 3. Then we let n be such that $t\theta \xrightarrow{\leq n}_{E'\backslash\mathcal{R}} (t\theta)\downarrow$ for every $\theta \in \Sigma(t)$. Then we prove that, for every normalized substitution σ, $t\sigma \xrightarrow{\leq n}_{E'\backslash\mathcal{R}} (t\sigma)\downarrow$. □

It must be emphasized that the proof of this theorem provides us with an effective way of computing the variants: simply narrow t at most n times, where n is given by the boundedness property.

6 Proving Boundedness

6.1 The case $E' = \emptyset$

Thanks to Lemma 2, the narrowing derivation associated by Lemma 1 to an innermost derivation is basic. Moreover, since $\mathcal{R}$ is a convergent system, we can always choose an innermost derivation. Hence we have the following proposition:

Proposition 5. *If basic narrowing terminates for $\mathcal{R}$ then $(\mathcal{R}, \emptyset)$ is a decomposition of E satisfying the boundedness property.*

This proposition allows us to conclude that the decomposition $(\mathcal{R}_{\mathrm{DYT}}, \emptyset)$ (resp. $(\mathcal{R}_{\mathrm{KIT}}, \emptyset)$) of DYT (resp. KIT) presented in Section 4.1 satisfies the boundedness property and, by Theorem 1 we conclude that these decompositions satisfy the finite variant property.

6.2 Non-Orientable Axioms

Because of non-orientable equations (typically AC), we need to consider equational rewriting. Unfortunately, we cannot extend directly the results of the previous section, as shown by Example 1. Anyway, for Abelian Groups and Diffie-Hellman theories, independently of the orientation of $x^{-1} * y^{-1} = (x * y)^{-1}$,

AC-narrowing (even basic) does not terminate. That is why we need to develop refined criteria, which will be satisfied by these two theories, yielding a finite variant property.

Let us first give a simple decidable sufficient condition for boundedness.

Lemma 4. *If $(\mathcal{R}, E')$ is a decomposition of E which satisfies:*

$$\forall f \in \mathcal{F}\ \exists c\ \forall t_1, \dots t_n \in \mathcal{T}(\mathcal{F}, \mathcal{X}).\ f(t_1{\downarrow}, \dots, t_n{\downarrow}) \xrightarrow{\leq c}_{E' \backslash \mathcal{R}} f(t_1, \dots, t_n){\downarrow}.$$

Then $(\mathcal{R}, E')$ satisfies the boundedness property.

Note that being an optimally reducing rewrite systems (see [14]) is a sufficient condition for the boundedness property. Indeed such systems actually satisfy the conditions of Lemma 4, with a constant $c = 1$. However, we are going to need (for instance for Abelian Groups) to apply Lemma 4 with constants larger than 1. Furthermore, even if we can apply Lemma 4, with $c = 1$, the rewrite system might not be optimally reducing, simply because there are extra rules not satisfying the required condition. Finally, in [14], the authors assume that the root symbol of any left hand side is not associative-commutative, which we do not. So, our condition, which is strictly weaker, provides us with new applications.

We show successively that Lemma 4 can be applied to the theories of exclusive or, Abelian Groups and Diffie-Hellman.

Lemma 5. *Let t_1 and t_2 be irreducible terms (w.r.t. $AC \backslash \mathcal{R}_+$), $t_1 + t_2$ can be reduced to its normal form, using at most 1 reduction step.*

A similar lemma does not hold for the Abelian Groups decomposition $(\mathcal{R}_*, AC)$ of Section 4.3. Even worse, this decomposition does not satisfy the boundedness property: consider the term $t = x^{-1}$ and the substitution $\sigma = \{x \mapsto a_0 * \dots * a_n\}$, $t\sigma$ requires at least n reduction steps before we reach its normal form.

However, an unusual orientation of some rules yields a presentation for which the finite variant property holds. This orientation has first been proposed by Lankford (see [9]). We get the following rewrite system:

$$\mathcal{R}'_* = \left\{ \begin{array}{cc} x * 1 \to x & {x^{-1}}^{-1} \to x \\ 1^{-1} \to 1 & (x^{-1} * y)^{-1} \to x * y^{-1} \\ x * x^{-1} \to 1 & x * (x^{-1} * y) \to y \\ x^{-1} * y^{-1} \to (x * y)^{-1} & x^{-1} * (y^{-1} * z) \to (x * y)^{-1} * z \\ (x * y)^{-1} * y \to x^{-1} & (x * y)^{-1} * (y * z) \to x^{-1} * z \end{array} \right.$$

This rewrite system is an AC-convergent system for $\mathcal{AG}$ [9] and even though basic narrowing does not terminate, we can show that:

Lemma 6. *Let t_1 and t_2 be irreducible terms (w.r.t. $AC \backslash \mathcal{R}'_*$), t_1^{-1} and $t_1 * t_2$ can be reduced to their normal form, using at most 1 (resp. 2) reduction step.*

Example 4. Let $t_1 = a * (b * c)^{-1}$ and $t_2 = a^{-1} * b$. We have the following derivation from $t_1 * t_2$ to its normal form c^{-1}.

$$(a * (b * c)^{-1}) * (a^{-1} * b) \rightarrow_{AC\backslash\mathcal{R}'_*} ((b * c) * a)^{-1} * (a * b) \rightarrow_{AC\backslash\mathcal{R}'_*} c^{-1}$$

Now consider the Diffie-Hellman theory. We orient the two additional equations and get the following rewrite system:

$$\mathcal{R}_{\mathcal{DH}} = \mathcal{R}'_* \cup \begin{cases} exp(x, 1) \rightarrow x \\ exp(exp(x, y), z) \rightarrow exp(x, y * z) \end{cases}$$

Proposition 6. *$\mathcal{R}_{\mathcal{DH}}$ is an AC-convergent rewrite system for $\mathcal{DH}$.*

Lemma 7. *Let t_1 and t_2 be irreducible terms (w.r.t. $AC\backslash\mathcal{R}_{\mathcal{DH}}$), t_1^{-1}, $t_1 * t_2$ and $exp(t_1, t_2)$ can be reduced to their normal form, using at most 1 (resp. 2 and 4) reduction step.*

We illustrate the worst case for which we need the 4 reduction steps to obtain the normal form.

Example 5. Let $t_1 = exp(e, a^{-1} * b)$ and $t_2 = b^{-1} * a$, $t = exp(t_1, t_2)$ can be reduced to its normal form (w.r.t. $AC\backslash\mathcal{R}_{\mathcal{DH}}$) by a derivation using 4 reduction steps. Indeed, we have:

$$\begin{aligned} exp(exp(e, a^{-1} * b), b^{-1} * a) &\rightarrow exp(e, (a^{-1} * b) * (b^{-1} * a)) \\ &\rightarrow exp(e, (a * b)^{-1} * (a * b)) \\ &\rightarrow exp(e, 1) \\ &\rightarrow e \end{aligned}$$

To sum up, as consequences of Theorem 1, Lemmas 4, 5, 6 and 7:

Corollary 1. *The decompositions $(\mathcal{R}_+, AC)$, $(\mathcal{R}'_*, AC)$ and $(\mathcal{R}_{\mathcal{DH}}, AC)$ have the finite variant property.*

7 *ACUNh* does not Satisfy the Finite Variant Property

We prove here that the theory *ACUNh*, introduced in Section 4.5 does not have the finite variant property.

Let us recall that, depending on the orientation of $h(x + y) = h(x) + h(y)$, we get two *AC*-convergent rewrite systems displayed in Figure 1. However, none of them yields an appropriate decomposition:

Lemma 8. *The decompositions $(\mathcal{R}_1, AC)$ and $(\mathcal{R}_2, AC)$ of the theory ACUNh do not satisfy the boundedness property.*

Proof: First, we consider the case of $(\mathcal{R}_1, AC)$, and we show the result by contradiction. Let $t = h(x)$ and n be such that $\forall\sigma.\ h(x)(\sigma\downarrow) \xrightarrow{\leq n}_{E'\backslash\mathcal{R}} (h(x)\sigma)\downarrow$. We consider the substitution $\sigma = \{x \mapsto a + h(a) + \ldots + h^{n+1}(a)\}$. It is easy to see that we need $n+1$ rewriting steps (with the rule $h(x+y) \to h(x) + h(y)$) to rewrite $h(x)\sigma$ to its normal form $h(a) + \ldots + h^{n+2}(n)$. Hence contradiction.

The result for $(\mathcal{R}_2, AC)$ can be obtained in a similar way with the term $t = x + y$ and the substitution $\sigma = \{x \mapsto h^n(a); y \mapsto h^n(b)\}$. □

There are not many other choices than $\mathcal{R}_1$ and $\mathcal{R}_2$ and we get the following:

Theorem 2. *There is no decomposition $(\mathcal{R}, AC)$ of ACUNh which satisfies the boundedness property and such that the right members of the rules in $\mathcal{R}$ are irreducible (w.r.t. $AC\backslash\mathcal{R}$).*

The idea is to prove first that, for any AC-convergent rewrite system $\mathcal{R}$, either $\to_{AC\backslash\mathcal{R}_1} \subseteq \xrightarrow{*}_{AC\backslash\mathcal{R}}$ or $\to_{AC\backslash\mathcal{R}_2} \subseteq \xrightarrow{*}_{AC\backslash\mathcal{R}}$. Next, we prove that there is an integer n such that $\to_{AC\backslash\mathcal{R}} \subseteq \xrightarrow{\leq n}_{AC\backslash\mathcal{R}_1}$ or $\to_{AC\backslash\mathcal{R}} \subseteq \xrightarrow{\leq n}_{AC\backslash\mathcal{R}_2}$ and we conclude by Lemma 8.

Corollary 2. *There is no decomposition $(\mathcal{R}, AC)$ of ACUNh which satisfies the finite variant property and such that the right members of the rules in $\mathcal{R}$ are irreducible (w.r.t. $AC\backslash\mathcal{R}$).*

The property required on the right members of the rules of $\mathcal{R}$ seems to be unnecessary. This assumption has been taken to make easier the proof.

8 Other Applications of the Finite Variant Property

Assume that (E, E') has the finite variant property. This can be used to reduce disunification problems modulo E to disunification problems modulo E':

Theorem 3. *The Σ_1 fragment of the first-order theory of $\mathcal{T}(\mathcal{F})/{=_E}$ is decidable whenever the Σ_1 fragment of the first-order theory of $\mathcal{T}(\mathcal{F})/{=_{E'}}$ is decidable.*

To prove this, simply compute the variants $\phi_1, \ldots, \phi_n$ of the formula ϕ. (In such a computation, logical connectives are seen as free symbols). For every substitution σ, there is an index i and a substitution θ such that $\phi\sigma\downarrow_E =_{E'} \phi_i\theta$. In particular, ϕ is solvable modulo E iff one of the ϕ_i is solvable modulo E'.

Then, since the Σ_1 fragment of the theory of $\mathcal{T}(\mathcal{F})/{=_{AC}}$ is decidable [1], we get the following new results:

Corollary 3. *The Σ_1 fragments of the first-order theories of quotient term algebras $\mathcal{T}(\mathcal{F})/{=_{ACUN}}$, $\mathcal{T}(\mathcal{F})/{=_{\mathcal{AG}}}$, $\mathcal{T}(\mathcal{F})/{=_{\mathcal{DH}}}$ are decidable.*

Such results cannot be derived from the decidability of unification. Even in the dismatching case this is not so trivial to get a decision procedure. Consider for instance $x + f(x + y) \neq a$ in the theory *ACUN*. A most general solution of the matching problem is $x = f(z) + a \wedge y = a + z + f(z)$. Complementing the solutions of the matching equation involves quantifier elimination : $\forall z. x \neq a + f(z) \vee y \neq a + z + f(z)$.

In the case of Abelian Groups, it is actually known that the first-order theory of finitely generated Abelian Groups is decidable [16]. However, adding a binary free function symbol, it might become undecidable. Actually, the status of the first order theories of above-mentioned quotient algebras is unknown. On the undecidability side, the method described in [18] can not be applied in a straightforward way. On the decidability side, the finite variant property does not help since the first-order theory of $\mathcal{T}(\mathcal{F})/{=_{AC}}$ is undecidable [18].

9 Conclusion

We believe that the finite variant property is important in many applications. It allows us to reduce problems modulo an equational theory E to problems modulo an equational theory $E' \subseteq E$. It is often useless for solving equations; for instance, unification modulo $ACUN$ is simpler than unification modulo AC. However, for other constraint solving problems such as intruder derivability constraints [5] or disunification problems mentioned in the previous section, this property can be crucial.

We have proposed some criteria for the finite variant property, which have been applied to several equational theories. The techniques are inspired by narrowing, though, as in [19], we do not rely directly on narrowing sequences, but rather on innermost reductions of instances.

An open question is to design other criteria (both for the finite variant property or its negation), which would not assume an E'-convergent rewrite system for E. For instance, does $(AC, \emptyset)$ have the finite variant property ? We are tempted to answer no, but the proof is challenging.

Acknowledgement

We would like to acknowledge P. Narendran and the anonymous referees who gave relevant comments which helped in improving the paper.

References

1. H. Comon. Complete axiomatizations of some quotient term algebras. *Theoretical Computer Science*, 118(2):167–191, 1993.
2. H. Comon-Lundh. Intruder theories (ongoing work). In *7th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'04)*, Barcelona, Spain, 2004. Invited talk, slides available at http://www.lsv.ens-cachan.fr/ comon/biblio.html.
3. H. Comon-Lundh and V. Cortier. New decidability results for fragments of first-order logic and application to cryptographic protocols. In *Proc. 14th International Conference on Rewriting Techniques and Applications (RTA'03)*, volume 2706 of *LNCS*, pages 148–164, Valencia, Spain, 2003. Springer-Verlag.

4. H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. Research Report LSV-04-17, Laboratoire Spécification et Vérification, ENS Cachan, France, 2004. 21 pages.
5. H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *Proc. of 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03)*, pages 271–280, Ottawa, Canada, 2003. IEEE Comp. Soc. Press.
6. S. Delaune and F. Jacquemard. A decision procedure for the verification of security protocols with explicit destructors. In *Proc. 11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 278–287, Washington, USA, 2004. ACM.
7. N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 6. Elsevier and MIT Press, 1990.
8. J.-M. Hullot. Canonical forms and unification. In *Proc. 5th Conference on Automated Deduction, (CADE'80)*, volume 87 of *LNCS*, pages 318–324, Les Arcs, France, 1980. Springer.
9. J.-M. Hullot. A catalogue of canonical term rewriting systems. Technical Report CSL-114, Computer Science Laboratory, SRI, CA, USA, 1980.
10. D. Kapur, P. Narendran, and L. Wang. An E-unification algorithm for analyzing protocols that use modular exponentiation. In *Proc. 14th International Conference on Rewriting Techniques and Applications (RTA'03)*, volume 2706 of *LNCS*, pages 165–179, Valencia, Spain, 2003. Springer-Verlag.
11. C. Kirchner. *Méthodes et Outils de Conception Systématique d'Algorithmes d'Unification dans les Théories Équationnelles.* PhD thesis, Université de Nancy I, 1985.
12. C. Meadows and P. Narendran. A unification algorithm for the group Diffie-Hellman protocol. In *Proc. of the Workshop on Issues in the Theory of Security (WITS'02)*, Portland, USA, 2002.
13. P. Narendran, Q. Guo, and D. Wolfram. Unification and matching modulo nilpotence. In *Proc. of the 13th International Conference on Automated Deduction, (CADE'96)*, volume 1104 of *LNCS*, pages 261–274, New Brunswick, USA, 1996. Springer-Verlag.
14. P. Narendran, F. Pfenning, and R. Statman. On the unification problem for cartesian closed categories. *Journal of Symbolic Logic*, 62(2):636–647, 1997.
15. L. Paulson. Mechanized proofs for a recursive authentication protocol. In *Proc. 10th Computer Security Foundations Workshop (CSFW'97)*, pages 84–95, Rockport, USA), 1997. IEEE Comp. Soc. Press.
16. C. Rackoff. On the complexity of the theories of weak direct products (preliminary report). In *Proc. of the 6th Annual ACM Symposium on Theory of Computing*, pages 149–160. ACM Press, 1974.
17. P. Y. A. Ryan and S. A. Schneider. An attack on a recursive authentication protocol: A cautionary tale. *Information Processing Letters*, 65(1):7–10, 1998.
18. R. Treinen. A new method for undecidability proofs of first order theories. *Journal of Symbolic Computation*, 14(5):437–457, 1992.
19. E. Viola. E-unifiability via narrowing. In *Proc. of the 7th Italian Conference on Theoretical Computer Science, (ICTCS'01)*, volume 2202 of *LNCS*, pages 426–438, Torino, Italy, 2001. Springer.