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 convergent modulo E', 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. $\mathcal{R}/E'$). In other words, *compute in advance all possible reductions in an instance of t, independently of that instance.* This property is called hereafter the *finite variant property* and allows to reduce some problems in the equational theory defined by $(\mathcal{R}, E')$ to problems in the equational theory defined by E' alone.

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).

The finite variant property is related to the termination of equational narrowing: this paper is also an insight into equational narrowing.

1 Introduction

In our recent work on the verification of cryptographic protocols [3, 4] 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 reductions in any instance of t. 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

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

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

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:

1. 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 will give a proof (example) in Section 3.2. E. Viola in [17] shows that innermost reduction steps modulo AC cannot always be lifted to basic narrowing steps, hence the completeness proof of basic narrowing does not carry over the AC case. In the same paper E. Viola proposes another narrowing strategy, introducing extensions of rules. This notion of narrowing restores completeness. However, termination is lost, even in simple cases.
2. 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 7.

The first contribution of this paper is to design 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 [17]. We differ in two respects: first we consider only terms (not unification problems) and second, there is a quantifier switch. Roughly, in [17], 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 7) and prove that these conditions are met for several equational theories, which are relevant to cryptographic protocols. For instance, we show that the theory of Abelian Groups has the finite variant property, relying on the unusual orientation of the inverse rule (Section 7.2). We also show in Section 8 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 on equational rewriting in Section 2. We state in Section 3 some results on basic and equational narrowing, some of which we did not find in the literature (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. In Section 7 we give sufficient conditions for the boundedness property and then apply them to the relevant theories listed in Section 4. In Section 8, we prove that the theory *ACUNh* (Associativity, Commutativity, Unit, Nilpotence, homomorphism), for which unifiability is in PTIME [12], does not have the finite variant property. In Section 9, we show another applications of the finite variant property, and we conclude in Section 10.

2 Preliminaries

2.1 Terms, Substitutions, Unification

We use classical notations and terminology from [6] on terms, unification, rewrite systems. For sake of clarity, we recall here some important definitions. $\mathcal{T}(\mathcal{F},\mathcal{X})$ 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. A substitution σ is *grounding for* a term t when $t\sigma \in \mathcal{T}(\mathcal{F})$.

If E is a set of equations (unordered pair of terms), we denote by $sig(E)$ the set of all function symbols occurring in E and by $=_E$ the least congruence on $\mathcal{T}(\mathcal{F},\mathcal{X})$ such that $u\sigma =_E v\sigma$ for all pairs $u = v \in E$. 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 a rewrite rule $l \to r$ in $\mathcal{R}$, a position $p \in O(s)$ 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. We write $\xrightarrow{*}_{\mathcal{R}}$ for the reflexive and transitive closure of $\to_{\mathcal{R}}$ and $\xleftrightarrow{*}_{\mathcal{R}}$ for its reflexive, transitive and symmetric closure. 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 $t_1 \to_{\mathcal{R}} t_2 \to_{\mathcal{R}} \ldots$.

Given a set of rewrite rules $\mathcal{R}$ and a set of equations E, *rewriting modulo E*, is the relation $\to_{\mathcal{R}/E}$ defined as follows: $s \to_{\mathcal{R}/E} t$ iff there exists a position $p \in O(s)$ such that:

$$s|_p =_E l\sigma \text{ and } t = s[r\sigma]_p$$

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 $s \xrightarrow{*}_{\mathcal{R}/E} s'$, $t \xrightarrow{*}_{\mathcal{R}/E} t'$, and $s' =_E t'$. It said to be E-convergent if, in addition, $\to_{\mathcal{R}/E}$ is terminating.

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

3 Narrowing

Given a TRS $\mathcal{R}$, we say that a term t is narrowable into a term t' if there exists a position $p \in \bar{O}(t)$, a renaming of $l \to r \in \mathcal{R}$, and a substitution σ such that σ is a unifier of $t|_p$ and l. Then $t' = (t[r]_p)\sigma$ is the result of narrowing t by $l \to r$ at p. $\rightsquigarrow_\sigma$ is the narrowing relation with substitution σ. $t \rightsquigarrow t'$ if there exists a σ such that $t \rightsquigarrow_\sigma t'$. 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

Now, let E be a set of equations for which an E-unification algorithm is available, we define E-narrowing as expected (σ is an E-unifier of $t|_p$ and l).

The following lemma, whose proof can be found in Appendix A, states that every rewrite derivation ($\xrightarrow{*}_{\mathcal{R}/E'}$) can be lifted to a narrowing derivation.

Lemma 1 (lifting lemma). *Let E' be a regular presentation for which an E'-unification algorithm exists. Suppose we have a term t, a normalized substitution θ and we consider a reduction (w.r.t. $\mathcal{R}/E'$) from $t\theta$ to 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, we may assume that 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.

Actually, we do not know whether or not the lemma would still hold without the regularity assumption (which we use in the proof indeed).

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:*

$$\begin{aligned} B_1 &= \bar{O}(t) \\ B_{i+1} &= \mathcal{B}(B_i, p_i, r_i) \quad \textit{for } 1 \le i < n. \end{aligned}$$

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. $\mathcal{R}/E'$*)* $t_1 \to t_2 \to \ldots \to t_n$ *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.*

In case of non-equational narrowing, there are several well-known results; we recall the relevant ones.

Lemma 2 ([8]). *Let* $\mathcal{R}$ *be a convergent rewrite system such that any basic narrowing derivation starting from any right hand side of* $\mathcal{R}$ *terminates. Then any (basic) narrowing derivation terminates.*

Lemma 3 ([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 3 fails (contrary to what is suggested in [11]), as shown by the following example (this has also been noticed in [17]).

Example 1. We consider the rewrite system $\mathcal{R}_+$ consisting of the rules $x + 0 \to x$, $x + x \to 0$ and $x + x + y \to y$, which is known to be convergent modulo associativity and commutativity of $+$.

Let $t = x_1 + x_2$ and the normalized substitution $\sigma = \{x_1 \mapsto a + b, x_2 \mapsto a + b\}$. Consider the following innermost derivation (w.r.t. $\mathcal{R}_+/AC$) 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 3 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:

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

$\mathcal{R}$ is convergent modulo AC. $\sigma = \{x_1 \mapsto a + b;\ x_2 \mapsto a + b\}$ is a solution of the equation $x_1 + x_2 \stackrel{?}{=} 0$, 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, again, does not yield the solution we considered. 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 what we want.

4 Relevant Equational Theories

Before proceeding with the finite variant property, we list here some algebraic theories which are relevant to cryptographic protocols and which we will therefore investigate in Sections 6 and 7. 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 Axiomatized Dolev-Yao Theory (DYT)

This is essentially the classical Dolev-Yao model with explicit destructors such as decryption and projections. Here is a presentation of this theory:

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

It expresses roughly that 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 reflected in the intruder deduction capabilities. 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 DYT and the classical Dolev-Yao model; it is known that some protocols can be attacked if we consider explicit destructors, while they cannot otherwise (see for instance [5]). This is due to the fact that we accept the possibility 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 narrowing and hence basic narrowing w.r.t.* $\mathcal{R}_{\mathrm{DYT}}$ *terminates.*

Proof. $\mathcal{R}_{\mathrm{DYT}}$ is proved to terminate using any simplification ordering. It is convergent because there is no critical pair. Narrowing and basic narrowing w.r.t. $\mathcal{R}_{\mathrm{DYT}}$ terminates thanks to Lemma 2. □

4.2 Key Inverse Theory (KIT)

It 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 for instance when we assume that decryption is just an encryption with the inverse key, as for the cryptosystem RSA. For the same reasons as before:

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

4.3 Exclusive Or Theory (*ACUN*)

This theory has been given in introduction. It is mandatory when protocols rely on exclusive or; several protocols have been shown secure when the equational theory is not considered, while there is an attack when the properties are taken into account ([13] vs [15]).

As recalled in Example 1, the rewrite system $\mathcal{R}_+$ for this theory is AC-convergent.

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

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

$$x * (y * z) = (x * y) * z \qquad x * x^{-1} = 1$$
$$x * y = y * x \qquad x * 1 = x$$

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 basic narrowing derivation starting from x^{-1} by using repeatedly the rule $(x * y)^{-1} \rightarrow x^{-1} * y^{-1}$.

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

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

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

This theory allows to take into account simple properties of product and exponentiation operators, such as those of RSA and Diffie-Hellman exponentiation, which are widely used in protocol constructions (see for instance the famous Diffie-Hellman key exchange algorithm [7]). Obviously, the exponentiation operation has actually more properties, and all the algebraic properties of exp, such as distributivity property 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.

4.6 Homomorphisms

This theory allows to model encryption algorithm which used Electronic Code Book (ECB) mode. This mode is the most obvious way to use a block cipher: ECB consists in partitioning the message into n-bits blocks and encrypting each of them separately. If we assume that the size of every atomic messages is a multiple of n, the size of the block imposed by the encryption function, we can model this property of the encryption algorithm by the following equality: $\{\langle x, y\rangle\}_z = \langle\{x\}_z, \{y\}_z\rangle$. For this theory, as well as other relevant theories, the equivalence classes are finite: we do not have any application of the finite variant property in these cases.

4.7 Combinations

Some combinations are relevant for cryptographic protocols. This is the case in particular for $ACUNh$ which consists of the four 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 distinct 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 ($\mathcal{R}_2$).

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

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

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

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 (variants). *Given two sets of equations E, E', t' is a* variant *of a term t if there is a substitution θ such that $t\theta =_E t'$. A* complete set of variants *of t (w.r.t. $\geq$) is a set S of 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 variants 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 compute a finite complete set of variants.*

Now, we need a (uniform) way to compute the 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 $\to_{\mathcal{R}/E'} \subseteq \geq$. 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 $\to_{\mathcal{R}/E'} \subseteq \geq$ 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 $t\sigma{\downarrow_{\mathcal{R}/E'}} =_{E'} t_i\theta$.

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. Remains the second (and most interesting) part.

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 4. *A decomposition $(\mathcal{R}, E')$ satisfies the finite variant property if and only if*

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. The if part is straightforward. We are going to focus on the only if part only. Let $(\mathcal{R}, E')$ be a decomposition which satisfies the finite variant property and t be a term.

Let T be the term $\langle t, \langle x_0, \langle \ldots, x_n \rangle\rangle\rangle$ where $\{x_0, \ldots, x_n\} = \mathit{vars}(t)$ and $\langle \_, \_ \rangle$ is a binary function symbol without any algebraic properties. Since $(\mathcal{R}, E')$ satisfies the finite variant property, there is a finite set of substitutions $\Sigma_A(T)$ such that, for every normalized substitution σ, there is a $\theta \in \Sigma_A(T)$, there is a τ, such that $(T\sigma)\downarrow =_{E'} (T\theta)\downarrow\tau$. Let $\Sigma(t) = \{\theta\downarrow | \theta \in \Sigma_A(T)\}$. We are going to show that $\Sigma(t)$ satisfies the requirements.

Let σ be a substitution, by hypothesis $\exists \theta \in \Sigma_A(T)$ and $\exists \tau$ such that $(T\sigma)\downarrow =_{E'} (T\theta)\downarrow\tau$. Let $\theta' = \theta\downarrow$. By definition $\theta' \in \Sigma(t)$, hence it remains to show that $\sigma\downarrow =_{E'} \theta'\tau$ and $(t\sigma)\downarrow =_{E'} (t\theta')\downarrow\tau$. We have the following equalities:

$$\begin{aligned}
(T\sigma)\downarrow &=_{E'} (T\theta)\downarrow\tau \\
(T\sigma)\downarrow &=_{E'} (T\theta')\downarrow\tau \\
(\langle t, \langle x_0, \langle \ldots, x_n \rangle\rangle\rangle\sigma)\downarrow &=_{E'} (\langle t, \langle x_0, \langle \ldots, x_n \rangle\rangle\rangle\theta')\downarrow\tau \\
\langle (t\sigma)\downarrow, \langle (x_0\sigma)\downarrow, \langle \ldots, (x_n\sigma)\downarrow \rangle\rangle\rangle &=_{E'} \langle (t\theta')\downarrow\tau, \langle (x_0\theta')\downarrow\tau, \langle \ldots, (x_n\theta')\downarrow\tau \rangle\rangle\rangle
\end{aligned}$$

Moreover, we have $(x_i\theta')\downarrow = x_i\theta'$ since θ' is normalized, hence $x_i\theta'\tau = (x_i\theta')\downarrow\tau =_{E'} (x_i\sigma)\downarrow$. We deduce that $\sigma\downarrow =_{E'} \theta'\tau$ and $(t\sigma)\downarrow =_{E'} (t\theta')\downarrow\tau$. □

Note that, in the above proof, Σ and Σ_A may be different: $\Sigma_A(t)$ may be strictly included in $\Sigma(t)$.

5.2 The Boundedness Condition

In what follows we assume 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):*

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

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. The first implication is actually similar to a result in [17]: we use narrowing, however bounding the length of derivation.

Let t be a term. By hypothesis $\exists n, \forall \sigma.\ t(\sigma\!\downarrow) \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\sigma)\!\downarrow$. Let S be the set of terms which are reachable from t by a narrowing derivation whose length is less than or equal to n. S is finite, effectively computable and contains only variants of t. It remains to show that S is complete.

Let σ be a substitution. We have to show that there exists $t' \in S$ and a substitution θ such that $(t\sigma)\!\downarrow =_{E'} t'\theta$. By hypothesis, we have $t(\sigma\!\downarrow) \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\sigma)\!\downarrow$. Thanks to Lemma 1, we deduce that there exists t', a narrowing derivation $t \overset{*}{\leadsto} t'$ of length at most n and a normalized substitution θ such that $t(\sigma\!\downarrow)\!\downarrow =_{E'} t'\theta$. We easily deduce that $t' \in S$ and $(t\sigma)\!\downarrow =_{E'} t'\theta$.

Conversely, assume that $(\mathcal{R}, E')$ satisfies the finite variant property. Thanks to Lemma 4, for every term t, there is a finite set of substitutions $\Sigma(t)$ such that:

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

Let t be a term. Let n be such that $t\theta \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\theta)\!\downarrow$ for every $\theta \in \Sigma(t)$. Note that such an n exists since $\mathcal{R}/E'$ is terminating and $\Sigma(t)$ is finite.

It remains to prove that for every normalized substitution σ, we have $t\sigma \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\sigma)\!\downarrow$. Let σ be a normalized substitution. Let $\theta \in \Sigma(t)$ and τ be such that $\sigma\!\downarrow\!(= \sigma) =_{E'} \theta\tau$ and $(t\sigma)\!\downarrow =_{E'} (t\theta)\!\downarrow\!\tau$. By definition of n, $t(\theta\tau) \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\theta)\!\downarrow\!\tau$. The following lemma, which is proved in Appendix B allows us to conclude since $\sigma =_{E'} \theta\tau$: we get $t\sigma \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\sigma)\!\downarrow$. □

Lemma 5. *Let t be a term and σ_1, σ_2 be normalized substitutions such that $\sigma_1 =_{E'} \sigma_2$. Let $\mathcal{D}$: $t\sigma_1 \xrightarrow{*}_{\mathcal{R}/E'} s_1$ be a derivation (w.r.t. $\mathcal{R}/E'$). Then there exists s_2 and a derivation $\mathcal{D}'$: $t\sigma_2 \xrightarrow{*}_{\mathcal{R}/E'} s_2$ such that $s_1 =_{E'} s_2$ and both derivations $\mathcal{D}$ and $\mathcal{D}'$ use the same rewrite rules at the same positions.*

It must be emphasized that the proof of this theorem provides 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 when $E' = \emptyset$

Thanks to Lemma 3, 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.*

Proof. Let n be the length of the longest basic narrowing derivation starting from t and let σ be a substitution, we show that we have $t(\sigma{\downarrow}) \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\sigma){\downarrow}$.

Let $\mathcal{D}$ be an innermost derivation from $t\sigma$ to its normal form $(t\sigma){\downarrow}$. Let $\mathcal{D}'$ be the narrowing derivation associated to $\mathcal{D}$ by Lemma 1. We know that $\mathcal{D}$ and $\mathcal{D}'$ use the same rewrite rules at the same positions and hence have the same length. Since $\mathcal{D}$ is an innermost derivation, Lemma 3 allows us to deduce that $\mathcal{D}'$ is based on $\bar{O}(t)$, and hence is basic: its length is bounded by n. Finally, we deduce that the length of $\mathcal{D}$ is smaller or equal to n, and hence we have $t(\sigma{\downarrow}) \xrightarrow{\leq n}_{\mathcal{R}/E'} (t\sigma){\downarrow}$. □

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 (resp. 4.2) satisfy the boundedness property and, by Theorem 1 we conclude that these decompositions satisfy the finite variant property.

7 Proving Boundedness with Non-Orientable Axioms ($E' \neq \emptyset$)

Because of non-orientable equations (typically AC), we need to consider equational rewriting. Unfortunately, we can not extend directly the results of the previous section in presence of non-orientable axioms. Lemma 3 does not hold in the equational case as proved by Example 1.

Anyway, for Abelian Groups and Diffie-Hellman theories, independently of the orientation of the equation $x^{-1} * y^{-1} = (x * y)^{-1}$, 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 6. *If $(\mathcal{R}, E')$ is a decomposition of E which satisfies:*

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

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

Proof. Let t be a term and let c_{max} be such that $\forall f \in sig(E)\ \forall t_1, \ldots, t_n \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ we have $f(t_1{\downarrow}, \ \ldots, \ t_n{\downarrow}) \xrightarrow{\leq c_{max}}_{\mathcal{R}/E'} f(t_1, \ldots, t_n){\downarrow}$. Note that a such c_{max} exists since $sig(E)$ is finite. Let θ be a substitution , we are going to prove by structural induction on t that $t(\theta{\downarrow})$ can be reduced to its normal, using at most $c_{max} \times |t|$ reductions steps where $|t|$ denotes the size of a term t, *i.e.* the cardinal of $O(t)$. We reason by case analysis:

1. If t is a variable then $t(\theta{\downarrow})$ is already in normal form.
2. If $t = f(t_1, \ldots, t_n)$. By induction hypothesis $\quad t_i(\theta{\downarrow}) \xrightarrow{\leq c_{max} \times |t_i|}_{\mathcal{R}/E'} (t_i\theta){\downarrow} \quad 1 \leq i \leq n.$
   - Either $f \in sig(E)$ and, by hypothesis, $f((t_1\theta){\downarrow}, \ldots, (t_n\theta){\downarrow}) \xrightarrow{c_{max}}_{\mathcal{R}/E'} f(t_1\theta, \ldots, t_n\theta){\downarrow})$ which allows us to conclude.
   - Or $f \notin sig(E)$, and in such a case $f((t_1\theta){\downarrow}, \ldots, (t_n\theta){\downarrow})$ is already in normal, hence the result. □

Now, we are going to illustrate the technique described above on several equational theories. The missing proofs can be found in Appendix C.

7.1 Exclusive Or Theory

Lemma 7. *Let t_1 and t_2 be irreducible terms (w.r.t. $\mathcal{R}_+/AC$), $t_1 + t_2$ can be reduced to its normal form, using at most 1 reduction step.*

Lemma 6 allows us to say that (R_+, AC) is a decomposition of $ACUN$ satisfying the boundedness property and therefore the finite variant property holds by Theorem 1. Moreover, for every term t, we can effectively get a finite set of variants by narrowing at most $|t|_+$ times t (where $|t|_+$ is the number of occurrences of $+$ in t).

7.2 Abelian Group Theory

Unfortunately, we cannot apply Theorem 1 on the presentation $(\mathcal{R}_*, AC)$ of the Abelian group theory. Indeed, because of the rule $(x * y)^{-1} \to x^{-1} * y^{-1}$, this decomposition of $\mathcal{AG}$ theory does not satisfy the boundedness property: consider the term $t = x^{-1}$ and the substitution $\sigma = \{x \mapsto a_0 * \ldots * a_n\}$. $t\sigma$ requires at least n reduction steps before we reach its normal form. This implies that this usual presentation of $\mathcal{AG}$ doesn't satisfy the finite variant property.

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]). The rewrite system obtained $\mathcal{R}'_*$ contains more rules than the classical one, its presentation is given in Figure 2.

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

Fig. 2. A Rewrite System for the Abelian Group Theory.

This rewrite system is an AC-convergent system for $\mathcal{AG}$ [9] and even though basic narrowing does not terminate, we are going to show that this presentation satisfies the finite variant property.

Lemma 8. *Let t_1 and t_2 be irreducible terms (w.r.t. $\mathcal{R}'_*/AC$), 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}.

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

As a consequence of Theorem 1, Lemmas 6 and 8:

Corollary 1. *$(\mathcal{R}'_*, AC)$ satisfies the finite variant property.*

$$exp(x, 1) \to x$$
$$exp(exp(x, y), z) \to exp(x, y * z)$$

Fig. 3. Rewrite System $\mathcal{R}_{exp}$

7.3 Diffie-Hellman Theory

To obtain a rewrite system representing the Diffie-Hellman theory, we just need to add two rules (see Figure 3) to the rewrite system $\mathcal{R}_*$ or $\mathcal{R}'_*$. Let $\mathcal{R}_{\mathcal{DH}} = \mathcal{R}'_* \cup \mathcal{R}_{exp}$.

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

Proof. This results has been obtained thanks to the CiME's tool.

Lemma 9. *Let t_1 and t_2 be irreducible terms (w.r.t. $\mathcal{R}_{\mathcal{DH}}/AC$), 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 (w.r.t. $\mathcal{R}_{\mathcal{DH}}/AC$) form by a derivation using at 4 reduction steps. Indeed, we have:

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

As a consequence of Theorem 1, Lemmas 6 and 9:

Corollary 2. *$(\mathcal{R}_{\mathcal{DH}}, AC)$ satisfies the finite variant property.*

8 A Theory which does not Satisfy the Finite Variant Property

We prove here that the theory *ACUNh*, introduced in Section 4.7 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 10. *The decompositions $(\mathcal{R}_1, AC)$ and $(\mathcal{R}_2, AC)$ of the theory ACUNh do not satisfy the boundedness property, and hence the finite variant 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 $\forall \sigma.\ h(x)(\sigma{\downarrow}) \xrightarrow{\leq n}_{\mathcal{R}/E'} (h(x)\sigma){\downarrow}$.

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 $\sigma = \{x \mapsto h^n(a); y \mapsto h^n(b)\}$. □

Actually, 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. $\mathcal{R}/AC$).*

The full proof of this result can be found in Appendix D. The idea is to prove first that, for any $\mathcal{R}$ such that $\rightarrow_{\mathcal{R}/AC}$ is convergent, $\rightarrow_{\mathcal{R}_1/AC} \subseteq \xrightarrow{*}_{\mathcal{R}/AC}$ or $\rightarrow_{\mathcal{R}_2/AC} \subseteq \xrightarrow{*}_{\mathcal{R}/AC}$. Next, we prove that there is an integer n such that $\rightarrow_{\mathcal{R}/AC} \subseteq \xrightarrow{\leq n}_{\mathcal{R}_1/AC}$ or $\rightarrow_{\mathcal{R}/AC} \subseteq \xrightarrow{\leq n}_{\mathcal{R}_2/AC}$ and we conclude by Lemma 10.

Corollary 3. *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. $\mathcal{R}/AC$).*

9 Other Applications of the Finite Variant Property

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

Theorem 3. *The Σ_1 fragment of the first-order theory of $\mathcal{T}(\mathcal{F})/\!=_E$ is decidable as soon as 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 4. *The Σ_1 fragments of the theories of quotient term algebras $\mathcal{T}(\mathcal{F})/\!=_{ACUN}$, $\mathcal{T}(\mathcal{F})/\!=_{\mathcal{AG}}$, $\mathcal{T}(\mathcal{F})/\!=_{\mathcal{DH}}$ are decidable.*

Note that 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 [14]. 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 of [16] does not apply 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 [16].

10 Conclusion

We believe that the finite variant property is important in many applications. It allows 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 ([4]) or disunification problems mentioned in the previous section, this property can be crucial.

We designed some criteria for the finite variant property, which have been applied to several equational theories. The techniques are inspired by narrowing, though, as in [17], 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.

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 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.
5. 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.
6. 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.
7. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Society*, 22(6):644–654, 1976.
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. 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.
13. 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.
14. 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.
15. 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.
16. R. Treinen. A new method for undecidability proofs of first order theories. *Journal of Symbolic Computation*, 14(5):437–457, 1992.
17. 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.

Appendix A Lifting Lemma

Lemma 1 (lifting lemma). *Let E' be a regular presentation for which an E'-unification algorithm exists. Suppose we have a term t, a normalized substitution θ and we consider a reduction (w.r.t. $\mathcal{R}/E'$) from $t\theta$ to 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, we may assume that 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.

Proof. We use an induction on the length of the derivation from $t\theta$ to s', which is finite since $\mathcal{R}$ is E'-convergent. The case of the length zero is trivial.

Let V be a set of variables such that $vars(t) \cup dom(\theta) \subseteq V$. Suppose that

$$\mathcal{D}: \qquad s = t\theta \rightarrow_{\mathcal{R}/E'} s_1 \overset{*}{\rightarrow}_{\mathcal{R}/E'} s'$$

is a reduction sequence of length $n+1$ and the first reduction step takes place at position p with the rewrite rule $l \rightarrow r \in \mathcal{R}$. We may also assume that $vars(l) \cap V = \emptyset$. We have $(t\theta)|_p =_{E'} l\tau$ for some substitution τ with $dom(\tau) \subseteq vars(l)$ and $s_1 = s[r\tau]_p$ by definition of a step of rewriting with $\rightarrow_{\mathcal{R}/E'}$. Since θ is normalized, p is a non variable position in t and hence $(t\theta)|_p = (t|_p)\theta$. Let $\mu = \tau \cup \theta$, we have $(t|_p)\mu = (t|_p)\theta =_{E'} l\tau = l\mu$, so $t|_p$ and l are E'-unifiable. Let σ_1 be an E'-mgu of $t|p$ and l more general than μ. By definition of σ_1, there exists a substitution ρ such that $\rho \circ \sigma_1 =_{E'} \mu$ for all $x \in V \cup vars(l)$. Let $V_1 = (V \setminus dom(\sigma_1)) \cup \{vars(x\sigma_1) | x \in V\}$ and define θ_1 by:

$$\theta_1(x) = \begin{cases} \rho(x) & \text{for all } x \in V_1 \\ x & \text{otherwise} \end{cases}$$

Since $\rho \circ \sigma_1 =_{E'} \mu$ for all $x \in V \cup vars(l)$, we deduce that $\rho \circ \sigma_1 =_{E'} \theta$ for all $x \in V$ and finally we obtain:

$$\theta_1 \circ \sigma_1 =_{E'} \theta \quad \text{ for all } x \in V \tag{1}$$

Let $t_1 = (t[r]_p)\sigma_1$. By definition we have:

$$t \rightsquigarrow_{\sigma_1} t_1 \tag{2}$$

$$\begin{array}{lll} \text{We have} & vars(t_1) = vars((t[r]_p)\sigma_1) & \\ & \subseteq vars((t[l]_p)\sigma_1) & \text{since } vars(r) \subseteq vars(l) \\ & = vars(t\sigma_1) & \text{since } t\sigma_1 =_{E'} t[l]_p\sigma_1 \text{ and } E' \text{ is a regular theory} \\ & \subseteq V_1 & \text{since } vars(t) \subseteq V \text{ and by definition of } V_1 \end{array}$$

Now, we are going to show that $t_1\theta_1 =_{E'} s_1$.

$$\begin{array}{lll}
\text{We have} & t_1\theta_1 = t_1\rho & \text{since } x\theta_1 = x\rho \text{ for all } x \in V_1 \text{ and } vars(t_1) \subseteq V_1 \\
& = (t[r]_p)\sigma_1\rho & \text{by definition of } t_1 \\
& =_{E'} (t[r]_p)\mu & \text{since } (x\sigma_1)\rho =_{E'} x\mu \text{ for all } x \in V \cup vars(l) \\
& & \text{and } vars(t[r]_p) \subseteq V \cup vars(l) \\
& = (t\mu)[r\mu]_p & \\
& = (t\theta)[r\tau]_p & \text{since we have } x\mu = x\theta \text{ for all } x \in V \\
& & \text{and } x\mu = x\tau \text{ for all } x \in vars(r) \\
& = s[r\tau]_p & \text{since } s = t\theta \\
& = s_1 &
\end{array}$$

Thus,

$$t_1\theta_1 =_{E'} s_1 \tag{3}$$

Before we can apply the induction hypothesis, we have to verify that θ_1 is normalized. Since $dom(\theta_1) \subseteq V_1$, it suffices to show that for all $x \in V_1$, $x\theta_1$ is irreducible. There are two cases, (remember that $V_1 = (V \setminus dom(\sigma_1)) \cup \{vars(x\sigma_1) | x \in V\}$):

- If $x \in V \setminus dom(\sigma_1)$, we have $x\sigma_1 = x$. Moreover, thanks to (1), we have $x\theta =_{E'} (x\sigma_1)\theta_1$. Hence, we deduce that $x\theta =_{E'} x\theta_1$. Since $x\theta$ is irreducible, we deduce that $x\theta_1$ is irreducible thanks to the E'-convergence of $\mathcal{R}$.
- If $x \in \{vars(y\sigma_1) | y \in V\}$ then there exists $y \in V$ such that $x \in vars(y\sigma_1)$, hence $x\theta_1$ is a subterm of $(y\sigma_1)\theta_1$. We have $(y\sigma_1)\theta_1 =_{E'} y\theta$ thanks to (1), this latter is irreducible by hypothesis. Hence, we deduce that $(y\sigma_1)\theta_1$ is irreducible as well as its subterms. In particular $x\theta_1$ is irreducible.

Now we can apply the induction hypothesis, we have a term t_1 and a normalized substitution θ_1. We consider $\mathcal{D}'$ the end of the derivation $\mathcal{D}$, $\mathcal{D}'$ is a derivation from $s_1 =_{E'} t_1\theta_1$ (thanks to (3)) to its normal form s'. Then there exists a term t', a substitution σ'_1 and a normalized substitution θ' such that:

(a) $t_1 \overset{*}{\rightsquigarrow}_{\sigma'_1} t'$
(b) $t'\theta' =_{E'} s'$

Moreover, we may assume that $t_1 \overset{*}{\rightsquigarrow}_{\sigma'} t'$ and $s_1 \xrightarrow{*}_{\mathcal{R}/E'} s'$ apply the same rewrite rules at the same positions.

Let $\sigma = \sigma'_1 \circ \sigma_1$. Concatenating (2) and (a) yields $t \overset{*}{\rightsquigarrow}_\sigma t'$. By construction this narrowing derivation employs the same rewrite rules at the same positions as the rewrite sequence $t\theta \xrightarrow{*}_{\mathcal{R}/E'} s'$. Lastly, we have $t'\theta' =_{E'} s'$ and θ' normalized by induction hypotheses. □

Appendix B Variant vs Boundedness

Lemma 5. *Let t be a term and σ_1, σ_2 be normalized substitutions such that $\sigma_1 =_{E'} \sigma_2$. Let $\mathcal{D}$: $t\sigma_1 \xrightarrow{*}_{\mathcal{R}/E'} s_1$ be a derivation (w.r.t. $\mathcal{R}/E'$). Then there exists s_2 and a derivation $\mathcal{D}'$: $t\sigma_2 \xrightarrow{*}_{\mathcal{R}/E'} s_2$ such that $s_1 =_{E'} s_2$ and both derivations $\mathcal{D}$ and $\mathcal{D}'$ use the same rewrite rules at the same positions.*

Proof. We use an induction on the length of the derivation $\mathcal{D}$ from $t\sigma_1$ to s_1. The case of length zero is trivial. Suppose that:

$$\mathcal{D}: \quad t\sigma_1 \rightarrow_{\mathcal{R}/E'} s'_1 \xrightarrow{*}_{\mathcal{R}/E'} s_1$$

is a reduction sequence of length $n+1$ and the first reduction step takes place at position p by using the rewrite rule $l \rightarrow r \in \mathcal{R}$. We consider *w.l.o.g.* a fresh renaming of the rewriting rule. We have $(t\sigma_1)|_p =_{E'} l\tau$ for some substitution τ with $dom(\tau) \subseteq vars(l)$ and $s'_1 = (t\sigma_1)[r\tau]_p$ by definition of a step of rewriting with $\rightarrow_{\mathcal{R}/E'}$. Since σ_1 is normalized, p is a non variable position in t and hence $(t\sigma_1)|_p = (t|_p)\sigma_1$. Hence, we have $s'_1 = (t[r\tau]_p)\sigma_1$. Since $\sigma_1 =_{E'} \sigma_2$, we have $(t|_p)\sigma_1 =_{E'} (t|_p)\sigma_2$ and we deduce that $(t|_p)\sigma_2 =_{E'} l\tau$.

Hence we have $t\sigma_2 \rightarrow_{\mathcal{R}/E'} (t[r\tau]_p)\sigma_2$. Now, we can apply the induction hypothesis. We have a term $t[r\tau]_p$ and two normalized substitutions σ_1, σ_2 such that $\sigma_1 =_{E'} \sigma_2$. We have a derivation $\mathcal{D}_1$ from $(t[r\tau]_p)\sigma_1$ to s_1. Then, by induction hypothesis, there exists s_2 such that $s_1 =_{E'} s_2$ and a derivation $\mathcal{D}'_1 : (t[r\tau]_p)\sigma_2 \xrightarrow{*}_{\mathcal{R}/E'} s_2$. Moreover, both derivations $\mathcal{D}_1$ and $\mathcal{D}'_1$ use the same rewrite rules at the same positions. Hence we deduce the expected result.

Appendix C Boundedness Property

If $*$ is an AC symbol and t, u are terms such that $t =_{AC} t_1 * \cdots * t_n$, $u =_{AC} u_1 * \cdots * u_m$ with $t_1, \ldots, t_n, u_1, \ldots, u_m$ not headed with $*$, we use the following notations:

$$t \wedge u \stackrel{\text{def}}{=} \prod_{s \in \{t_1,\ldots,t_n\} \cap \{u_1,\ldots,u_m\}} s$$
$$t \setminus u \stackrel{\text{def}}{=} w_1 \text{ s.t. } w_1 * (t \wedge u) =_{AC} t$$

Lemma 7. *Let t_1 and t_2 be irreducible terms (w.r.t. $\mathcal{R}_+/AC$), $t_1 + t_2$ can be reduced to its normal form, using at most 1 reduction step.*

Proof. The set NF of terms in normal form is the least set such that:

$$\begin{aligned} NF &= NF_0 \cup NF_+ \\ NF_0 &= \{0\} \\ NF_f &= \textstyle\bigcup_{f \in \mathcal{F} \setminus sig(E)} f(NF, \cdots, NF) \\ NF_+ &= \{u_1 + \ldots + u_m \mid u_1, \ldots, u_m \in NF_f \cup X, \forall i \neq j, u_i \neq u_j\} \end{aligned}$$

Let t_1, t_2 be irreducible terms, we are going to prove that $t_1 + t_2$ can be reduced to its normal form using at most 1 reduction step.

- If $t_1 \in NF_0$ (resp. $t_2 \in NF_0$): $t_1 + t_2 \rightarrow_{x+0 \rightarrow x} t_2$ (resp. t_1) which is in normal form by hypothesis.
- Otherwise $t_1 = u_1 + \cdots + u_n$, $t_2 = v_1 + \cdots + v_m$ with $u_1, \ldots, u_n \in NF_f \cup X$ and pairwise distinct and $v_1, \ldots, v_m \in NF_f \cup X$ and pairwise distinct. Then, either $u_1, \ldots, u_n, v_1, \ldots, v_m$ are pairwise distinct, in which case $t_1 + t_2$ is in normal form, or else:

  $$t_1 + t_2 = (t_1 \wedge t_2) + (t_1 \wedge t_2) + (t_1 \setminus t_2) + (t_2 \setminus t_1)$$

  and is reducible in one step to $(t_1 \setminus t_2) + (t_2 \setminus t_1)$ or 0 (depending on $(t_1 \setminus t_2)$ and $(t_2 \setminus t_1)$ are empty or not) which are in normal form. ◻

Lemma 8. *Let t_1 and t_2 be irreducible terms (w.r.t. $\mathcal{R}'_*/AC$), t_1^{-1} and $t_1 * t_2$ can be reduced to their normal form, using at most 1 (resp. 2) reduction step.*

Proof. The set NF of terms in normal form is the least set such that:

$$\begin{aligned} NF &= NF_1 \cup NF_{inv} \cup NF_p \cup NF_* \\ NF_1 &= \{1\} \\ NF_f &= \textstyle\bigcup_{f\in\mathcal{F}\setminus sig(E)} f(NF,\ldots,NF) \\ NF_{inv} &= NF_p^{-1} \\ NF_p &= NF_f \cup X \cup NF_p * NF_p \\ NF_* &= \{u^{-1} * v \mid u,v \in NF_p, u \wedge v = 1\} \end{aligned}$$

Let t_1 be an irreducible term, we are going to prove that t_1^{-1} can be reduced to its normal form using at most 1 reduction step.

- $t_1 \in NF_p$: $t_1^{-1} \in NF_{inv} \subseteq NF$
- $t_1 \in NF_1$: $t_1^{-1} \rightarrow_{1^{-1}\rightarrow 1} 1 \in NF$
- $t_1 \in NF_{inv}$: $t_1 = u^{-1}$ with $u \in NF_p$ and we have $t_1^{-1} \rightarrow_{(x^{-1})^{-1}\rightarrow x} u \in NF_p \subseteq NF$
- $t_1 \in NF_*$: $t_1 = u^{-1} * v$, with $u, v \in NF_p$ and $u \wedge v = 1$ and hence we have the following one step reduction: $t_1^{-1} \rightarrow_{(x^{-1}*y)^{-1}\rightarrow x*y^{-1}} u * v^{-1} \in NF_* \subseteq NF$

Let t_1, t_2 be irreducible terms, we are going to prove that $t_1 * t_2$ can be reduced to its normal form using at most 2 reduction steps, *i.e.* $\exists u \in NF.\ t_1 * t_2 \xrightarrow{\leq 2}_{\mathcal{R}'_*/AC} u$.

1. if $t_1 \in NF_1$ (resp. $t_2 \in NF_1$), then $t_1 * t_2 \rightarrow_{x*1\rightarrow x} t_2$ (resp. t_1), which is in normal form by hypothesis.
2. if $t_1, t_2 \in NF_p$, then $t_1 * t_2 \in NF_p \subseteq NF$.
3. if $t_1, t_2 \in NF_{inv}$, then $t_1 = u_1^{-1}$ and $t_2 = u_2^{-1}$ with $u_1, u_2 \in NF_p$ and hence we have $t_1 * t_2 \rightarrow_{x^{-1}*y^{-1}\rightarrow(x*y)^{-1}} (u_1 * u_2)^{-1} \in NF_{inv}$.
4. if $t_1 \in NF_p$ and $t_2 \in NF_{inv}$ (or the converse, which is symmetric), then $t_2 = u_2^{-1}$ with $u_2 \in NF_p$ and either $t_1 \wedge u_2 = 1$, in which case $t_1 * t_2 \in NF_* \subseteq NF$, or else $t_1 \wedge u_2 = v$ and, depending on whether $t_1 \setminus u_2$ and $u_2 \setminus t_1$ are empty or not, we are in one of the following 4 cases:
   (a) $t_1 = u_2$: $t_1 * t_2 \rightarrow_{x*x^{-1}\rightarrow 1} 1 \in NF$
   (b) $t_1 = u_2 * u_1$: $t_1 * t_2 \rightarrow_{x*(x^{-1}*y)\rightarrow y} u_2 \in NF_p \subseteq NF$
   (c) $u_2 = t_1 * u_1$ with $u_1 \in NF_p$: $t_1 * t_2 \rightarrow_{(x*y)^{-1}*y\rightarrow x^{-1}} u_1^{-1} \in NF_{inv} \subseteq NF$
   (d) otherwise: $t_1 * t_2 \rightarrow_{(x*y)^{-1}*(y*z)\rightarrow x^{-1}*z} (u_2 \setminus t_1)^{-1} * (t_1 \setminus u_2) \in NF$
5. $t_1 \in NF_*$ and $t_2 \in NF_{inv}$ (or the converse, which is symmetric): $t_1 = u_1^{-1} * v_1$ and $t_2 = u_2^{-1}$ with $u_1, v_1, u_2 \in NF_p$, $t_1 * t_2 \rightarrow_{x^{-1}*(y^{-1}*z)\rightarrow(x*y)^{-1}*z} (u_1 * u_2)^{-1} * v_1$ which can be normalized in one step, thanks to case 4.
6. $t_1 \in NF_*$ and $t_2 \in NF_p$ (or the converse, which is symmetric): $t_1 = u_1^{-1} * v_1$ with $u_1, v_1 \in NF_p$ and $t_1 * t_2 =_{AC} u_1^{-1} * (v_1 * t_2)$, which can be normalized in one step, thanks to case 4.
7. $t_1 \in NF_*$ and $t_2 \in NF_*$: $t_1 = u_1^{-1} * v_1$ and $t_2 = u_2^{-1} * v_2$ with $u_1, v_1, u_2, v_2 \in NF_p$. Then $t_1 * t_2 \rightarrow_{x^{-1}*(y^{-1}*z)\rightarrow(x*y)^{-1}*z} (u_1 * u_2)^{-1} * (v_1 * v_2)$ and we are back again to case 4. □

Lemma 9. *Let t_1 and t_2 be irreducible terms (w.r.t. $\mathcal{R}_{\mathcal{DH}}/AC$), 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.*

Proof. The set NF of terms in normal form is the least set such that:

$$NF = NF_1 \cup NF_{inv} \cup NF_p \cup NF_*$$

where $NF_{inv}, NF_1, NF_*, NF_f$ are defined as in the proof of Lemma 8 and NF_p and NF_{exp} are defined as below:

$$\begin{aligned} NF_p &= NF_f \cup NF_{exp} \cup X \cup NF_p * NF_p \\ NF_{exp} &= exp(NF_f \cup X \cup NF_{inv} \cup NF_1 \cup NF_p \cup NF_*, NF_f \cup X \cup NF_{inv} \cup NF_p \cup NF_* \cup NF_{exp}) \end{aligned}$$

Then for any terms $t_1, t_2 \in NF$, $t_1^{-1} \xrightarrow{\leq 1}_{\mathcal{R}'_*/AC} t \in NF$ and $t_1 * t_2 \xrightarrow{\leq 2}_{\mathcal{R}'_*/AC} t \in NF$ are proved as in Lemma 8. Remains the case of the function symbol exp.

Let t_1, t_2 be irreducible terms, we are going to prove that $exp(t_1, t_2)$ can be reduced to its normal form using at most 4 reduction steps, *i.e.* $\exists t \in NF.\ exp(t_1, t_2) \xrightarrow{\leq 4}_{\mathcal{R}'_*/AC} t$.

- If $t_1 \notin NF_{exp}$ and $t_2 \notin NF_1$, then $exp(t_1, t_2) \in NF_{exp} \subseteq NF$.
- If $t_2 \in NF_1$, then $exp(t_1, t_2) \rightarrow_{exp(x,1) \rightarrow x} t_1$
- If $t_1 \in NF_{exp}$ then $t_1 = exp(u_1, v_1)$ with $u_1 \in NF \setminus NF_{exp}$, $v_1 \in NF \setminus NF_1$ and $exp(t_1, t_2) \rightarrow_{exp(exp(x,y),z) \rightarrow exp(x,y*z)} exp(u_1, v_1 * t_2)$. Next, thanks to (the proof of) Lemma 8, $v_1 * t_2 \xrightarrow{\leq 2}_{\mathcal{R}_{\mathcal{DH}}/AC} w \in NF$ and, either $w \notin NF_1$, in which case the resulting term is in normal form, or else $exp(u_1, w) \rightarrow_{exp(x,1) \rightarrow x} u_1$, which is in normal form. In the worst case, we need 4 reduction steps. □

Appendix D Non-Boundedness Property

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. $\mathcal{R}/AC$).*

Proof. First, we are going to show that an AC-convergent rewriting system $\mathcal{R}$ with irreducible right members necessarily contains $\mathcal{R}_1$ or $\mathcal{R}_2$, *i.e.* $\rightarrow_{\mathcal{R}_1/AC} \subseteq \xrightarrow{*}_{\mathcal{R}/AC}$ or $\rightarrow_{\mathcal{R}_2/AC} \subseteq \xrightarrow{*}_{\mathcal{R}/AC}$. Indeed, since $0 =_{ACUNh} h(0)$, we have either $0 \xrightarrow{*}_{\mathcal{R}/AC} h(0)$ or $h(0) \xrightarrow{*}_{\mathcal{R}/AC} 0$. The first case is impossible because $\mathcal{R}$ must be terminating, hence we have necessarily $h(0) \xrightarrow{*}_{\mathcal{R}/AC} 0$. By a similar reasoning, we obtain:

$$\begin{aligned} x + (x + y) &\xrightarrow{*}_{\mathcal{R}/AC} y \\ x + x &\xrightarrow{*}_{\mathcal{R}/AC} 0 \\ x + 0 &\xrightarrow{*}_{\mathcal{R}/AC} x \end{aligned}$$

Only remains the case of $h(x+y)$ and $h(x)+h(y)$ which are in the same equivalence class. Hence they rewrite to a common normal form (modulo AC) by $\mathcal{R}$. We consider two cases (which are *a priori* not disjoint):

1. $h(x+y)$ is reducible by $\mathcal{R}$. In such a case, there exists a rule of the form $h(x+y) \rightarrow r$ in $\mathcal{R}$ with r irreducible (w.r.t. $\mathcal{R}/AC$). By investigating the left members of the rewrite rules in $\mathcal{R}$, we deduce that r is necessarily irreducible by $\mathcal{R}_1$ and then that $r = h(x) + h(y)$.
2. $h(x)+h(y)$ is reducible by $\mathcal{R}$. In such a case, $h(x+y)$ is necessarily irreducible by $\mathcal{R}$. Indeed, we have seen that if $h(x+y)$ was reducible, there would be a rule of the form $h(x+y) \rightarrow h(x) + h(y)$ in $\mathcal{R}$, which means that $h(x) + h(y)$ is irreducible. Hence contradiction. So, we deduce that:
$$h(x) + h(y) \xrightarrow{*}_{\mathcal{R}/AC} h(x+y)$$

Hence, we obtain either $\rightarrow_{\mathcal{R}_1/AC} \subseteq \xrightarrow{*}_{\mathcal{R}/AC}$ or $\rightarrow_{\mathcal{R}_2/AC} \subseteq \xrightarrow{*}_{\mathcal{R}/AC}$. In the following, we assume we are in the first case, *i.e* $\rightarrow_{\mathcal{R}_1/AC} \subseteq \xrightarrow{*}_{\mathcal{R}/AC}$ (the other case is similar).

The next step consists in showing that $\exists n. \rightarrow_{\mathcal{R}/AC} \subseteq \xrightarrow{\leq n}_{\mathcal{R}_1/AC}$. In other words, a rewriting step of $\rightarrow_{\mathcal{R}/AC}$ can be simulated by at most n (which depends only on $\mathcal{R}$) rewriting steps of $\mathcal{R}_1$. Let $l \rightarrow r \in \mathcal{R}$. Since $\mathcal{R}_1$ is an AC-convergent rewriting system, there exists l' and r' such that $l \xrightarrow{*}_{\mathcal{R}_1/AC} l'$, $r \xrightarrow{*}_{\mathcal{R}_1/AC} r'$ and $l' =_{AC} r'$. We have already seen that $\rightarrow_{\mathcal{R}_1/AC} \subseteq \xrightarrow{*}_{\mathcal{R}/AC}$, and moreover r is irreducible (w.r.t. $\mathcal{R}$), hence we deduce that $l \xrightarrow{*}_{\mathcal{R}_1/AC} l'(=_{AC} r)$. So we have, $\forall l \rightarrow r \in \mathcal{R}, \exists\, l' =_{AC} r$ such that $l \xrightarrow{*}_{\mathcal{R}_1/AC} l'$, hence we have proved that $\rightarrow_{\mathcal{R}/AC} \subseteq \xrightarrow{*}_{\mathcal{R}_1/AC}$. Let n be such that $l \xrightarrow{\leq n}_{\mathcal{R}_1/AC} l{\downarrow}_{R_1/AC}$ for all $l \rightarrow r \in \mathcal{R}$. Such a n exists since $\mathcal{R}_1$ is AC-convergent and $\mathcal{R}$ contains a finite number of rewrite rules. Hence we have proved that $\exists n. \rightarrow_{\mathcal{R}/AC} \subseteq \xrightarrow{\leq n}_{\mathcal{R}_1/AC}$.

Now, we can conclude. Indeed, if $\mathcal{R}$ has the boundedness property, then we can easily deduce that $\mathcal{R}_1$ (or $\mathcal{R}_2$) satisfies also this property. This is impossible thanks to Lemma 10. Hence we deduce that $\mathcal{R}$ doesn't satisfy the boundedness property. $\square$