

Steve Kremer, Antoine Mercier,
Ralf Treinen

Reducing Equational Theories
for the Decision of Static Equivalence

Research Report LSV-09-19

july 2009

Laboratoire
Spécification
et
Vérification



CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Ecole Normale Supérieure de Cachan
61, avenue du Président Wilson
94235 Cachan Cedex France

Reducing Equational Theories for the Decision of Static Equivalence[★]

Steve Kremer¹, Antoine Mercier¹, and Ralf Treinen²

¹ LSV, ENS Cachan, CNRS, INRIA, France

² PPS, Université Paris Diderot, CNRS, France

Abstract. Static equivalence is a well established notion of indistinguishability of sequences of terms which is useful in the symbolic analysis of cryptographic protocols. Static equivalence modulo equational theories allows a more accurate representation of cryptographic primitives by modelling properties of operators by equational axioms. We develop a method that allows in some cases to simplify the task of deciding static equivalence in a multi-sorted setting, by removing a symbol from the term signature and reducing the problem to several simpler equational theories. We illustrate our technique at hand of bilinear pairings.

1 Introduction

Many formal models for analyzing cryptographic protocols have been developed over the last thirty years. Among them we find logical or symbolic models, based on the seminal ideas of Dolev and Yao [11], which represent cryptographic primitives in an abstract way. This is justified by the so-called *perfect cryptography assumption* which states that the intruder has no means to break the cryptographic primitives themselves, and that he can hence break security only by exploiting logical flaws in the protocol.

In symbolic models, messages of the protocol are represented by terms in an abstract algebra. The motivation this abstraction was the simplification and even automation of the analysis and the proof of security protocols. Since the assumption of perfect cryptography is not always realistic, some properties of cryptographic primitives (a survey can be found in [10]) have been taken into account in logical models by the means of equational theories on the terms.

In this paper we concentrate on *static equivalence*, a standard notion of indistinguishability of sequences of terms originating from the applied pi calculus [3]. Intuitively static equivalence asks whether or not an attacker can distinguish between two sequences of messages, later called *frames*, by exhibiting a relation which holds on one sequence but not on the other. Static equivalence provides an elegant means to express security properties on pieces of data, for instance those observed by a passive attacker during the run of a protocol. In the context of active attackers, static equivalence has also been used to characterize process equivalences [3] and off-line guessing attacks [9, 5]. There now exist exact [2],

[★] This work has been partially supported by the ANR-07-SESU-002 project AVOTÉ.

and approximate [1] algorithms to decide static equivalence for a large family of equational theories.

Our ultimate goal is to develop combination methods for deciding static equivalence, that is to develop means to algorithmically reduce a static equivalence problem modulo some equational theory to some other static equivalence problems modulo simpler equational theories.

Contribution of this paper. We exhibit criteria on equational theories allowing simplifications for the decision of static equivalence. The kind of simplification we describe is the removal of a particular symbol which we call a *valve*. More precisely, given a sorted signature, and two sorts r and s , a valve from r to s is a symbol expecting arguments of sort r and producing a term of another sort s . Moreover, it is the only function symbol which allows to build terms of sort s out of terms of sort r . Signatures of this kind occur when representing cryptographic primitives using elements of two distinct algebraic structures and a mapping function from one structure to the other. A concrete example occurs in the bilinear pairing operation [7, 12, 14]. We will use this operation as a running example throughout the paper.

We show that under some conditions a valve can be removed from the terms in the frames on which we want to decide the static equivalence, and from the equational theory. Hence our purpose is dual. First we show that deciding static equivalence of a pair of frames involving a given valve can be reduced to the decision of the static equivalence of pairs of frames without this symbol. Second, we show that deciding static equivalence on a pair of frames, not involving a given valve f , in the presence of an equational theory involving f , can be done in the presence of two other, generally simpler equational theories without f . Obviously this cannot be done in general and the first step of this work consists in identifying sufficient conditions on equational theories for which this kind of reduction is possible. The result is illustrated by reducing the decision of static equivalence for an equational theory modelling bilinear pairings between two groups to the decision of static equivalence on groups, yielding a new decidability result.

A completely different combination problem for deciding static equivalence was studied in [4], namely the combination of *disjoint* equational theories. On the one hand we do not require the two simpler signatures obtained by the reduction to be disjoint, on the other hand we are working in a well-sorted setting.

Structure of the paper. In Section 2 we introduce our formal model. Section 3 presents the running example used throughout the paper. In Section 4 we introduce the concepts of *valve* and *reducibility*. Section 5 is dedicated to the presentation of our reduction results. We give a first syntactic criterion for the applicability of our reduction results in Section 6, and conclude in Section 7. Exhaustive versions of some of the proofs are postponed to the appendix.

2 Model

2.1 Sorted term algebras

A *sorted signature* $(\mathcal{S}, \mathcal{F})$ is defined by a set of *sorts* $\mathcal{S} = \{s, s_1, s_2, \dots\}$ and a set of function symbols $\mathcal{F} = \{f, f_1, f_2, \dots\}$ with arities of the form $\text{arity}(f) = s_1 \times \dots \times s_k \rightarrow s$ where $k \geq 0$. If $k = 0$ the symbol is called a *constant* and its arity is simply written s . We fix an \mathcal{S} -indexed family of sorted *names* $\mathcal{N} = (\mathcal{N}_s)_{s \in \mathcal{S}}$ where $\mathcal{N}_s = \{n_{s_1}, n_{s_2}, \dots\}$ and an infinite ordered set of sorted *variables* \mathcal{X} .

The set of *terms of sort* s is defined inductively by :

$$\begin{array}{l} t ::= \text{term of sort } s \\ | x \quad \text{variable } x \text{ of sort } s \\ | n \quad \text{name } n \text{ of sort } s \\ | f(t_1, \dots, t_k) \text{ application of symbol } f \in \mathcal{F} \end{array}$$

where each t_i is a term of sort s_i and $\text{arity}(f) = s_1 \times \dots \times s_k \rightarrow s$. The set of terms $T(\mathcal{F}, \mathcal{N}, \mathcal{X})$ is the union of the sets of terms of sort s for every $s \in \mathcal{S}$. We denote by $\text{sort}(t)$ the sort of term t . We write $\text{var}(t)$ and $\text{names}(t)$ for the set of variables and names occurring in t , respectively. A term t is *ground* iff $\text{var}(t) = \emptyset$. The set of ground terms is denoted by $T(\mathcal{F}, \mathcal{N})$.

We extend the notion of arity to terms as follows. If t is a ground term of sort s then $\text{arity}(t) = s$, otherwise $\text{arity}(t) = s_1 \times \dots \times s_n \rightarrow s$ if the ordered sequence x_1, \dots, x_n of variables of t are of sort s_1, \dots, s_n respectively.

We write $|t|$ for the *size* of t , i.e. the number of symbols of t .

A *context* C is a term with distinguished variables sometimes called *holes*. It can be formalized as a lambda-term of the form $\lambda x_1. \dots \lambda x_n. t_C$ where the x_i may appear or not in t_C . For the sake of simplicity, in most cases we simply write $C[x_1, \dots, x_n]$ instead of $\lambda x_1. \dots \lambda x_n. t_C$ as well as $C[t_1, \dots, t_n]$ instead of $(\dots (\lambda x_1. \dots \lambda x_n. t_C) t_1 \dots) t_n$. Hence $C[t_1, \dots, t_n]$ is simply the result of replacing each x_i by t_i . A context is *public* if it does not involve any name.

The *positions* $\text{Pos}(t)$ of a term t are defined as usual by $\text{Pos}(u) = \{\Lambda\}$ when $u \in \mathcal{N} \cup \mathcal{X}$ and $\text{Pos}(f(t_1, \dots, t_n)) = \{\Lambda\} \cup \{i \cdot \pi \mid 1 \leq i \leq n, \pi \in \text{Pos}(t_i)\}$ otherwise. The subterm of t at position p is written $t|_p$, and the replacement in t at position p by u is written $t[u]_p$.

A *substitution* σ written $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ with domain $\text{dom}(\sigma) = \{x_1, \dots, x_n\}$ is a mapping from $\{x_1, \dots, x_n\} \subseteq \mathcal{X}$ to $T(\mathcal{F}, \mathcal{N}, \mathcal{X})$. We only consider *well sorted* substitutions in which x_i and t_i have the same sort. A substitution σ is *ground* if all t_i are ground. The *application* of a substitution σ to a term t is written $t\sigma$.

2.2 Equational theories and rewriting systems

An *equation* is an equality $t = u$ where t and u are two terms of the same sort. An *equational theory* E is a finite set of equations. We denote by $=_E$ the smallest congruence relation on $T(\mathcal{F}, \mathcal{N}, \mathcal{X})$ such that $t\sigma =_E u\sigma$ for any $t = u \in E$ and for any substitution σ . We say that a symbol f is *free* in E if f does not occur in E .

A *term rewriting system* \mathcal{R} is a finite set of *rewrite rules* $l \rightarrow r$ where $l \in T(\mathcal{F}, \mathcal{N}, \mathcal{X})$ and $r \in T(\mathcal{F}, \mathcal{N}, \text{var}(l))$. A term $u \in T(\mathcal{F}, \mathcal{N}, \mathcal{X})$ rewrites to v by \mathcal{R} , denoted $u \rightarrow_{\mathcal{R}} v$ if there is a rewrite rule $l \rightarrow r \in \mathcal{R}$, a position p and a substitution σ such that $u|_p = l\sigma$ and $v = u[r\sigma]_p$. We write \rightarrow^* for the transitive and reflexive closure of \rightarrow . Given a set of equations E , u rewrites modulo E by \mathcal{R} to v , denoted $u \rightarrow_{\mathcal{R}/E} v$, if $u =_E t[l\sigma]_p$ and $t[r\sigma]_p =_E v$ for some context t , position p in t , rule $l \rightarrow r$ in \mathcal{R} , and substitution σ . \mathcal{R} is *E-terminating* if there are no infinite chains $t_1 \rightarrow_{\mathcal{R}/E} t_2 \rightarrow_{\mathcal{R}/E} \dots$. \mathcal{R} is *E-confluent* iff whenever $t \rightarrow_{\mathcal{R}/E} u$ and $t \rightarrow_{\mathcal{R}/E} v$, there exist u', v' such that $u \rightarrow_{\mathcal{R}/E}^* u'$, $v \rightarrow_{\mathcal{R}/E}^* v'$, and $u' =_E v'$. \mathcal{R} is *E-convergent* if it is *E-terminating* and *E-confluent*. A term t is in *normal form* with respect to (\mathcal{R}/E) if there is no term s such that $t \rightarrow_{\mathcal{R}/E} s$. If $t \rightarrow_{\mathcal{R}/E}^* s$ and s is in normal form, we say that s is a normal form of t . When this normal form is unique (up to E) we write $s = t \downarrow_{\mathcal{R}/E}$.

2.3 Substitutions and frames

A *frame* is an expression $\phi = \nu\tilde{n}_\phi.\sigma_\phi$ where \tilde{n}_ϕ is a set of *bound names*, and σ_ϕ is a substitution. $|\phi|$ is the size of ϕ , i.e. the number of elements in $\text{dom}(\sigma_\phi)$. σ_ϕ is called the *underlying substitution* of ϕ . We extend the notation *dom* to frames by $\text{dom}(\nu\tilde{n}.\sigma) = \text{dom}(\sigma)$. We write $\phi =_\alpha \psi$ when the frames ϕ and ψ are equal up to alpha-conversion of bound names. For two frames $\phi = \nu\tilde{n}_\phi.\sigma_\phi$ and $\psi = \nu\tilde{n}_\psi.\sigma_\psi$ with $\text{dom}(\phi) \cap \text{dom}(\psi) = \emptyset$ and $\tilde{n}_\phi \cap \tilde{n}_\psi = \emptyset$ we write $\phi\psi$ for the *disjoint composition* of ϕ and ψ defined as $\phi\psi = \nu(\tilde{n}_\phi \cup \tilde{n}_\psi).\sigma_\phi\sigma_\psi$. Note that $\tilde{n}_\phi \cap \tilde{n}_\psi = \emptyset$ is always possible by alpha-conversion of the bound names of ϕ and ψ . The sort of a frame ϕ is the set $S = \{\text{sort}(x) \mid x \in \text{dom}(\phi)\}$, and we say that ϕ is *S-sorted*.

For simplicity, we only consider frames $\phi = \nu\tilde{n}\{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ that restrict every name in use, that is, for which $\tilde{n} = \text{names}(t_1, \dots, t_n)$. A name a may still be disclosed explicitly by adding a mapping $x_a \mapsto a$ to the frame.

2.4 Static equivalence

Definition 1 (equality in a frame [2]). We say that two terms M and N are equal in a frame ϕ for the equational theory E , and write $(M =_E N)\phi$, if and only if $\phi =_\alpha \nu\tilde{n}.\sigma$, $M\sigma =_E N\sigma$, and $\{\tilde{n}\} \cap (\text{names}(M) \cup \text{names}(N)) = \emptyset$.

Definition 2 (static equivalence [2]). Two frames ϕ and ψ are statically equivalent for the equational theory E , written $\phi \approx_E \psi$, iff $\text{dom}(\phi) = \text{dom}(\psi)$, and for all terms M and N , we have $(M =_E N)\phi$ if and only if $(M =_E N)\psi$.

For two frames ϕ and ψ , two terms M, N such that $(M =_E N)\phi$ and $(M \neq_E N)\psi$ are called *distinguishers* of ϕ and ψ .

3 Running example

We will illustrate our specific definitions and lemmas by a running example involving two distinct algebraic groups \mathbb{G}_1 and \mathbb{G}_2 and a pairing operation e

mapping two elements of \mathbb{G}_1 to an element of \mathbb{G}_2 . A concrete cryptographic definition can be found in [7]. In general, a pairing operation maps elements of an additive group to elements of a multiplicative group in the following way.

$$e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2 \\ e(ag_1, bg_2) = e(g_1, g_2)^{ab}$$

In some protocols, e.g. [12], one has in fact $g_1 = g_2$. We use this assumption in order to simplify our notations. Moreover, we use a multiplicative notation to represent elements of \mathbb{G}_1 , e.g. we write $exp_1(x)$ for both xg_1 and xg_2 .

Let \mathcal{S}_{BP} be the set of sorts $\{R, G_1, G_2\}$, R is the sort of the exponents of a chosen generator of the \mathbb{G}_i , and G_1 (resp. G_2) are the sorts of the elements of the groups \mathbb{G}_1 (resp. \mathbb{G}_2). Let \mathcal{F}_{BP} be the following set of symbols:

$+, \cdot : R \times R \rightarrow R$	add, mult
$- : R \rightarrow R$	inverse
$0_R, 1_R : R$	constants
$exp_i : R \rightarrow G_i$	$i \in \{1, 2\}$ exponentiation
$*_i : G_i \times G_i \rightarrow G_i$	$i \in \{1, 2\}$ mult in \mathbb{G}_i
$e : G_1 \times G_1 \rightarrow G_2$	pairing

We will write $*$ instead of $*_i$, the sort of $*$ being always clear from the context. As a convenient shortcut we sometimes write t^i for $\underbrace{t * \dots * t}_{i \times}$. The properties of

these function symbols are defined by the following equational theory E_{BP} .

$x + y = y + x$	$0_R + x = x$
$(x + y) + z = x + (y + z)$	$x + (-x) = 0_R$
$x \cdot y = y \cdot x$	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	$1_R \cdot x = x$
$exp_i(x) *_i exp_i(y) = exp_i(x + y) \quad i \in \{1, 2\}$ $e(exp_1(x), exp_1(y)) = exp_2(x \cdot y)$	

This signature and this equational theory represent operations realized in protocols where the exchanged messages are elements of the groups \mathbb{G}_i . The symbol e represents a pairing operation.

Example 1. Bilinear pairing is a central primitive of the Joux protocol [12], a three participant variation of the Diffie-Hellman protocol. It implicitly relies on the decisional Bilinear Diffie-Hellman Assumption (BDH) which can be formally modelled using static equivalence as follows:

$$\nu a, b, c, r. \{x_1 \mapsto exp_1(a), x_2 \mapsto exp_1(b), x_3 \mapsto exp_1(c), y_1 \mapsto exp_2(a \cdot b \cdot c)\} \\ \approx_{E_{BP}} \nu a, b, c, r. \{x_1 \mapsto exp_1(a), x_2 \mapsto exp_1(b), x_3 \mapsto exp_1(c), y_1 \mapsto exp_2(r)\}$$

4 Valves and reducibility

The main result of our paper concerns signatures involving a special function symbol which we call a *valve*. Intuitively, as it is suggested by the name “valve”, a valve f is a symbol such that applying f on terms of sort r , we obtain a term t of sort s and such that t cannot be a subterm of a term of sort r .

We borrow here some useful notions from graph theory.

Definition 3 (Signature graph). Let $(\mathcal{S}, \mathcal{F})$ be a sorted signature. The graph $\mathcal{G}(\mathcal{S}, \mathcal{F})$ is the directed labelled graph (V, E) where $V = \mathcal{S}$, $E \subseteq V \times V \times \mathcal{F}$ and $(r, s, f) \in E$ iff $\text{sort}(f) = s_1 \times \cdots \times s_n \rightarrow s$ and $s_i = r$ for some i .

We recall that a *path* in a graph is a sequence of edges such that for two consecutive edges (r, s, f) and (r', s', f') we have $s = r'$.

Definition 4 (valve). A symbol f of arity $\cdots \times r \times \cdots \rightarrow s$ is a valve from r to s iff every path from r to s in $\mathcal{G}(\mathcal{S}, \mathcal{F})$ contains (r, s, f) and there is no path from s to r .

Example 2 (continued). Let us consider the sorted signature $(\mathcal{S}_{\text{BP}}, \mathcal{F}_{\text{BP}})$ introduced in our running example in Section 3. $\mathcal{G}(\mathcal{S}_{\text{BP}}, \mathcal{F}_{\text{BP}})$ is given in Figure 1.

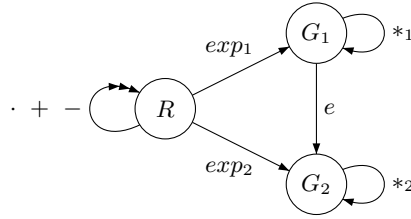


Fig. 1. $\mathcal{G}(\mathcal{S}_{\text{BP}}, \mathcal{F}_{\text{BP}})$

In the signature of Figure 1, e is a valve from G_1 to G_2 as (G_1, G_2, e) lies on every path from G_1 and G_2 , and since no path leads from G_2 to G_1 . We also have that exp_1 is a valve from R to G_1 . However, exp_2 is not a valve from R to G_2 as the sequence $(R, G_1, exp_1), (G_1, G_2, e)$ is a path from R to G_2 .

We are now able to present the central notion of reducibility.

Definition 5 (reducible). Let r and s be two sorts and f a valve from r to s . An equational theory E is reducible for f iff for every $n \geq 0$ there exist m public contexts $T_1[x_1, \dots, x_n], \dots, T_m[x_1, \dots, x_n]$ of arity $r \times \cdots \times r \rightarrow s$ such that for all public contexts $C_1[x_1, \dots, x_n], \dots, C_k[x_1, \dots, x_n]$ of arity $r \times \cdots \times r \rightarrow r$ there exists a public context $D[y_1, \dots, y_m]$ of arity $s \times \cdots \times s \rightarrow s$ such that for any ground terms t_1, \dots, t_n of sort r

$$f(C_1, \dots, C_k)[t_1, \dots, t_n] =_E D[T_1, \dots, T_m][t_1, \dots, t_n]$$

Intuitively, reducibility for a value f means that given a cardinality n of sets of ground terms of sort r , we can construct in a uniform way a set of terms such that any sequence of operations performed before applying f , there will be a way to reproduce these operations on the terms obtained with the context T_i . The uniformity lies in the fact that the contexts T_i depend only on the number n but *not* on the contexts C_i . We illustrate this notion by showing the reducibility for e of the theory of our running example E_{BP} in case $\mathcal{N}_{G_1} = \emptyset$.

Proposition 1. E_{BP} is reducible for e if $\mathcal{N}_{G_1} = \emptyset$.

Proof. Let n be an integer. We define $m = n + \frac{n*(n+1)}{2}$ contexts

$$\begin{aligned} T_i &= \lambda x_1. \dots \lambda x_n. e(x_i, \text{exp}_1(1_R)) \text{ for } 1 \leq i \leq n \\ T_{ij} &= \lambda x_1. \dots \lambda x_n. e(x_i, x_j) \text{ for } 1 \leq i \leq j \leq n \end{aligned}$$

Every public context $C_i[x_1, \dots, x_n]$ of arity $G_1 \times \dots \times G_1 \rightarrow G_1$ is of the form $\lambda x_1. \dots \lambda x_n. x_1^{e_{i1}} * \dots * x_n^{e_{in}} * \text{exp}_1(p_i)$ where $p_i =_{E_{BP}} 1_R + \dots + 1_R$ (l_i times). Hence $\text{exp}_1(p_i) =_{E_{BP}} \text{exp}_1(1_R)^{l_i}$.

Let us show by induction on the size of the contexts C_i that there exists a context D such that for any sequence of ground terms t_1, \dots, t_n

$$e(C_1, C_2)[t_1, \dots, t_n] =_{E_{BP}} D[T_1, \dots, T_n, T_{11}, \dots, T_{nn}][t_1, \dots, t_n]$$

Base case. We distinguish four cases:

1. $C_1 = \lambda x_1. \dots \lambda x_n. x_i$ and $C_2 = \lambda x_1. \dots \lambda x_n. x_j$

For any sequence of terms t_1, \dots, t_n we have that $e(C_1, C_2)[t_1, \dots, t_n] = e(t_i, t_j)$. As $\mathcal{N}_{G_1} = \emptyset$ there exist terms t'_i and t'_j of sort R such that $t_i =_{E_{BP}} \text{exp}_1(t'_i)$ and $t_j =_{E_{BP}} \text{exp}_1(t'_j)$. Hence

$$\begin{aligned} e(C_1, C_2)[t_1, \dots, t_n] &=_{E_{BP}} e(\text{exp}_1(t'_i), \text{exp}_1(t'_j)) \\ &=_{E_{BP}} \text{exp}_2(t'_i \cdot t'_j) =_{E_{BP}} T_{ij}[t_1, \dots, t_n] \end{aligned}$$

Let $D = \lambda y_1. \dots \lambda y_n. \lambda y_{11}. \dots \lambda y_{nn}. y_{ij}$. We have that $e(C_i, C_j)[t_1, \dots, t_n] =_{E_{BP}} D[T_1, \dots, T_n, T_{11}, \dots, T_{nn}][t_1, \dots, t_n]$.

2. $C_1 = \lambda x_1. \dots \lambda x_n. x_i$ and $C_2 = \text{exp}_1(1_R)^l$

For any sequence of terms t_1, \dots, t_n we have that $e(C_1, C_2)[t_1, \dots, t_n] = e(t_i, \text{exp}_1(1_R)^l)$. As $\mathcal{N}_{G_1} = \emptyset$ there exists a term t'_i of sort R such that $t_i =_{E_{BP}} \text{exp}_1(t'_i)$. Hence

$$\begin{aligned} e(C_1, C_2)[t_1, \dots, t_n] &=_{E_{BP}} e(\text{exp}_1(t'_i), \underbrace{\text{exp}_1(1_R + \dots + 1_R)}_{l \times}) \\ &=_{E_{BP}} \text{exp}_2(t'_i \cdot \underbrace{(1_R + \dots + 1_R)}_{l \times}) \\ &=_{E_{BP}} \text{exp}_2(t'_i)^l =_{E_{BP}} (T_i[t_1, \dots, t_n])^l \end{aligned}$$

Let $D = \lambda y_1. \dots \lambda y_n. \lambda y_{11}. \dots \lambda y_{nn}. y_i^l$. We have that $e(C_i, C_j)[t_1, \dots, t_n] =_{E_{BP}} D[T_1, \dots, T_n, T_{11}, \dots, T_{nn}][t_1, \dots, t_n]$.

3. $C_1 = \text{exp}_1(1_R)^l$ and $C_2 = \lambda x_1 \dots \lambda x_n . x_i$
As $C_1 * C_2 =_{E_{\text{BP}}} C_2 * C_1$ this case is similar to case 2.
4. $C_1 = \text{exp}_1(1_R)^{l_1}$ and $C_2 = \text{exp}_1(1_R)^{l_2}$
We immediately conclude by defining $D = \text{exp}_2(1_R)^{l_1 \cdot l_2}$.

Inductive case : $C_i = C_{i1} * C_{i2}$. Let $i = 1$. The case where $i = 2$ is similar. We note that every term of sort R can be written as a sum of products of names of sort R . More formally for any contexts $C_{11}[x_1, \dots, x_n]$, $C_{12}[x_1, \dots, x_n]$, $C_2[x_1, \dots, x_n]$, for any term t_1, \dots, t_n we have that $C_{11}[t_1, \dots, t_n] = \text{exp}_1(p_{11})$, $C_{12}[t_1, \dots, t_n] = \text{exp}_1(p_{12})$ and $C_2[t_1, \dots, t_n] = \text{exp}_1(p_2)$, for some elements of sort R described as above. We note that the equational theory implies that $e(C_{11} * C_{12}, C_2) = e(C_{11}, C_2) * e(C_{12}, C_2)$.

By induction there are D_1 and D_2 such that $e(C_{11} * C_2)[t_1, \dots, t_n] =_E D_1[T_1, \dots, T_m][t_1, \dots, t_n]$ and $e(C_{12} * C_2)[t_1, \dots, t_n] =_E D_2[T_1, \dots, T_m][t_1, \dots, t_n]$. Hence defining D as $D_1 * D_2$ we conclude. \square

Example 3. For $n = 2$ we have that

$$\begin{aligned} T_1 &= e(x_1, \text{exp}_1(1)) & T_2 &= e(x_2, \text{exp}_1(1)) \\ T_{1,1} &= e(x_1, x_1) & T_{1,2} &= e(x_1, x_2) & T_{2,2} &= e(x_2, x_2) \end{aligned}$$

Let $C_1 = \lambda x_1 \lambda x_2 . x_1$ and $C_2 = \lambda x_1 \lambda x_2 . x_2 * x_2 * \text{exp}_1(1 + 1)$. We define

$$D = \lambda y_1 \lambda y_2 \lambda y_{1,1} \lambda y_{1,2} \lambda y_{2,2} . y_{1,2} * y_{1,2} * y_1 * y_1$$

since $e(t_1, t_2 * t_2 * \text{exp}_1(1 + 1)) = e(t_1, t_2) * e(t_1, t_2) * e(t_1, \text{exp}_1(1)) * e(t_1, \text{exp}_1(1))$ for any *ground* terms t_1, t_2 .

Remark 1. Proposition 1 requires that we do not have names of sort G_1 . We argue that this is not restrictive in the context of protocols. As we expect that terms of sort G_1 represent the elements of a group with a given generator each element of the group G_1 can indeed be written as $\text{exp}_1(r)$ for some element of R .

One might have expected reducibility for a symbol f to be related to being *sufficiently complete w.r.t. f* as defined in [8].

Definition 6 (sufficiently complete). *E is a sufficiently complete equational theory with respect to $f \in \mathcal{F}$ if for every ground term $t \in T(\mathcal{F}, \mathcal{N})$ there exists a ground term $u \in T(\mathcal{F} \setminus \{f\}, \mathcal{N})$ such that $t =_E u$.*

The next two lemmas show, however, that these two notions are in fact independent of each other.

Lemma 1. *Reducibility of an equational theory E for a symbol f does not imply sufficient completeness of E w.r.t. f .*

Proof. Let $\mathcal{S} = \{r, s\}$ and $\mathcal{F} = \{f\}$, with $\text{sort}(f) = r \rightarrow s$, and $E = \emptyset$. We show that E is reducible for f but not sufficiently complete w.r.t. f . Consider an integer n and the contexts $T_1 = \lambda x_1 \dots \lambda x_n . f(x_1), \dots, T_n = \lambda x_1 \dots \lambda x_n . f(x_n)$.

As the only ground terms t_i of sort r are names n_i , we consider w.l.o.g. that any sequence of terms t_1, \dots, t_n is equal to n_1, \dots, n_n , and as the only possible contexts C of sort r are of the form $\lambda x_1 \dots \lambda x_n. x_i$, we have $f(C[t_1, \dots, t_n]) = f(n_i)$. Hence we only have to verify that for any i there exists a context D such that $f(n_i) =_E D[T_1, \dots, T_n][n_1, \dots, n_n]$. We choose $D = \lambda y_1 \dots \lambda y_n. y_i$.

To show that E is not sufficiently complete w.r.t. f , we note that as f is free, for any i the term $f(n_i)$ is not equivalent to a term without f . \square

Lemma 2. *Sufficient completeness of E w.r.t. a symbol f does not imply reducibility of E for f .*

Proof. We define a signature with two sorts r and s , no names, and the function symbols $0_r: r$, $s_r: r \rightarrow r$, $f: r \rightarrow s$, $0_s: s$, $s_s: s \rightarrow s$. The function symbol f is the valve. We have the following equational theory:

$$f(s_r(x), y) = s_s(f(x, y)) \quad f(0_r, s_r(y)) = f(s_r(y), y) \quad f(0_r, 0_r) = 0_s$$

Identifying any ground term of sort r or s with a natural number, the function f satisfies $f(n, m) = n + \frac{m*(m+1)}{2}$. Since there are no names E is sufficiently complete for f . The fact that f has a quadratic growth contradicts reducibility. A detailed proof can be found in Appendix C. \square

5 Getting rid of reducible symbols

We now present the central result of our work and show that if an equational theory E is *reducible* for f then it is possible to get rid of f when deciding static equivalence.

First, we show that deciding static equivalence on $\{r, s\}$ -sorted frames in the presence of a valve from r to s can be reduced to deciding two equivalences, one on r -sorted frames and one on s -sorted frames (Lemma 4).

Second, we show that under some conditions on the equational theory, deciding static equivalence for a given equational theory can be reduced to deciding static equivalence for an equational theory that does not involve a reducible symbol (Theorem 1). As a corollary we get the possibility of splitting the equational theory into simpler equational theories.

Definition 7 (reduction). *Let the equational theory E be reducible for f , where f is a valve from r to s , and let $\phi = \nu \tilde{n} \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ be a frame of sort $\{r\}$. The reduction of ϕ is defined as $\bar{\phi} = \nu \tilde{n} \{y_1 \mapsto T_1[t_1, \dots, t_n], \dots, y_m \mapsto T_m[t_1, \dots, t_n]\}$ where T_i are contexts as defined in Definition 5.*

We note that $\bar{\phi}$ is $\{s\}$ -sorted. Before giving an example illustrating the construction of $\bar{\phi}$ we define the following useful notation.

Definition 8 (s -restriction). *Let $\phi = \nu \tilde{n}. \sigma_\phi$ be an $\{s_1, \dots, s_n\}$ -sorted frame. The s_i -restriction of ϕ , denoted $\phi|_{s_i}$ is the frame $\nu \tilde{n}. \sigma_{\phi|_{s_i}}$ where $\sigma_{\phi|_{s_i}}$ is the substitution σ_ϕ restricted to the variables of sort s_i .*

Example 4. Let ϕ_{BDH} be the G_1 -restriction of the frames presented in Example 1 : $\phi_{BDH} = \nu a, b, c, r. \{x_1 \mapsto \text{exp}_1(a), x_2 \mapsto \text{exp}_1(b), x_3 \mapsto \text{exp}_1(c)\}$. Using the set of terms T_i and T_{ij} defined in the proof of Proposition 1, we get

$$\begin{aligned} \overline{\phi}_{BDH} = \nu a, b, c, r. \{ & y_1 \mapsto e(\text{exp}_1(a), \text{exp}_1(1)), y_{12} \mapsto e(\text{exp}_1(a), \text{exp}_1(b)), \\ & y_2 \mapsto e(\text{exp}_1(b), \text{exp}_1(1)), y_{13} \mapsto e(\text{exp}_1(a), \text{exp}_1(c)), \\ & y_3 \mapsto e(\text{exp}_1(c), \text{exp}_1(1)), y_{23} \mapsto e(\text{exp}_1(b), \text{exp}_1(c)) \} \end{aligned}$$

We now prove a technical lemma which will be used to transfer tests on a frame to tests on its reduction.

Lemma 3. *Let $(\mathcal{S}, \mathcal{F})$ be a signature such that $f \in \mathcal{F}$ is a valve from r to s , and E an equational theory that is reducible for f . For any integer n , and for any public context M of sort s there exists a public context M' such that for any $\{r, s\}$ -sorted frame ϕ of size n , $M\phi =_E M'\overline{\phi}_{|r}\phi_{|s}$.*

Proof. Let us show this by induction on the height of M . If M is a variable or a constant then we define $M' = M$. If $M = y \in \mathcal{X}$ then $y(\overline{\phi}_{|r}\phi_{|s}) = y\phi$ since the sort of y is s . If $M = c$ is a constant then $M\phi =_E M'\overline{\phi}_{|r}\phi_{|s}$ holds trivially.

If the height of M is non-null then the top symbol of M can be the valve f , or some function symbol $f' \neq f$.

If $M = f(C_1[x_1, \dots, x_n], \dots, C_k[x_1, \dots, x_n])$ then all variables of M are of sort r , and hence $M\phi = M\overline{\phi}_{|r}$ where $\overline{\phi}_{|r} = \{x_1 \mapsto t_1, \dots, x_{n'} \mapsto t_{n'}\}$. As E is reducible for f , we can define $\overline{\phi}_{|r}$ as $\{y_1 \mapsto T_1[t_1, \dots, t_{n'}], \dots, y_m \mapsto T_m[t_1, \dots, t_{n'}]\}$. By Definition 5 there exists a public context $D[y_1, \dots, y_m]$ such that

$$f(C_1, \dots, C_k)[t_1, \dots, t_{n'}] = D[T_1, \dots, T_m][t_1, \dots, t_{n'}$$

With $M' = D$ we have that $M\overline{\phi}_{|r} =_E M'\overline{\phi}_{|r}$, and hence $M\phi =_E M'\overline{\phi}_{|r}\phi_{|s}$.

If $M = f'(C_1[x_1, \dots, x_n, y_1, \dots, y_m], \dots, C_{k'}[x_1, \dots, x_n, y_1, \dots, y_m])$ with $f' \neq f$ then $\text{sort}(C_i) = s$. By induction there exist public contexts $M_1 \dots M_{k'}$ such that for any $\{r, s\}$ -sorted frame ϕ of size n , $C_{i'}\phi =_E M_{i'}\overline{\phi}_{|r}\phi_{|s}$. We define $M' = f'(M_1 \dots M_{k'})$, and obtain $M\phi =_E M'\overline{\phi}_{|r}\phi_{|s}$. \square

The following lemma allows us to split the decision of static equivalence of $\{r, s\}$ -sorted frames into two equivalences on r -sorted frames and s -sorted frames.

Lemma 4. *For any $\{r, s\}$ -sorted frames ϕ_1 and ϕ_2 built on $(\mathcal{S}, \mathcal{F})$, and for a valve f from r to s , if E is a reducible equational theory for f then $\phi_1 \approx_E \phi_2$ iff $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi}_{1|r}\phi_{1|s} \approx_E \overline{\phi}_{2|r}\phi_{2|s}$.*

Proof (Sketch). We prove the two directions of the equivalence separately.

(\Rightarrow) If $\phi_1 \approx_E \phi_2$, then $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi}_{1|r}\phi_{1|s} \approx_E \overline{\phi}_{2|r}\phi_{2|s}$. The proof is done by contraposition. We obviously have that $\phi_{1|r} \not\approx_E \phi_{2|r}$ implies $\phi_1 \not\approx_E \phi_2$ as $M\phi_{i|r} = M\phi_i$ for any term M having only variables of sort r . Furthermore, we have that $\overline{\phi}_{1|r}\phi_{1|s} \not\approx_E \overline{\phi}_{2|r}\phi_{2|s}$ implies $\phi_1 \not\approx_E \phi_2$. The proof uses the fact that the elements $\overline{\phi}_{i|r}$ are obtained by some fixed contexts T_i in order to build distinguishers for ϕ_1 and ϕ_2 .

(\Leftarrow) If $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_E \overline{\phi_{2|r}\phi_{2|s}}$ then $\phi_1 \approx_E \phi_2$. The proof is done by contraposition. Suppose that $\phi_1 \not\approx_E \phi_2$ and consider the two possibilities for the sorts of the distinguishers M and N . If $\text{sort}(M) = r$, by the fact that f is a valve, we have that M and N distinguish $\phi_{1|r}$ and $\phi_{2|r}$. If $\text{sort}(M) = s$, by invoking Lemma 3, we infer the existence of distinguishers for $\overline{\phi_{1|r}\phi_{1|s}}$ and $\overline{\phi_{2|r}\phi_{2|s}}$. \square

A detailed proof can be found in Appendix A.

By the following definition we identify a sufficient condition to get rid of the symbol f for deciding static equivalence between frames that do not involve this symbol. In the following section we exhibit a syntactic condition that is sufficient to obtain such a theory.

Definition 9 (sufficient equational theory). *Let $(\mathcal{S}, \mathcal{F} \uplus \{f\})$ be a sorted signature and E an equational theory. An equational theory E' is sufficient for E without f iff for any terms $u, v \in T(\mathcal{F}, \mathcal{N})$, $u =_E v$ iff $u =_{E'} v$ and E' does not involve f .*

Theorem 1. *Let E be an equational theory on the sorted signature $(\mathcal{S}, \mathcal{F} \uplus \{f\})$ such that*

- f is a valve,
- E is a reducible equational theory for f ,
- E is sufficiently complete w.r.t. $\{f\}$.

If there exists an equational theory E' sufficient for E without f then for any $\{r, s\}$ -sorted frames ϕ_1 and ϕ_2 , we have that $\phi_1 \approx_E \phi_2$ iff $\phi_{1|r} \approx_{E'} \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}$.

The proof of Theorem 1 relies on Lemma 5.

Lemma 5. *Let ϕ_1 and ϕ_2 be two $\{r\}$ -sorted frames, E an equational theory, and f a valve from r to a distinct sort s , which is free in E . If for any two terms M, N of sort r $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$, then for any two terms M and N of sort s , $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$.*

Proof (sketch). We will exhibit two replacements functions σ_1 (resp. σ_2) defined on pairs (α, p) where α identifies M or N and p is a position in $M\phi_1$ or $N\phi_1$ (resp. $M\phi_2, N\phi_2$) such that $M\phi_1|_p$ or $N\phi_1|_p$ is headed by f . The co-domain of σ_1 (resp. σ_2) is a set of fresh names w.r.t. ϕ_1 (resp. ϕ_2). We show the two following assertions

1. $M\phi_1\sigma_1 =_E M\phi_2\sigma_2$ and $N\phi_1\sigma_1 =_E N\phi_2\sigma_2$,
2. $M\phi_i =_E N\phi_i$ iff $M\phi_i\sigma_i =_E N\phi_i\sigma_i$ for $i \in \{1, 2\}$.

Their conjunction implies that for any two terms M, N of sort s , $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$.

To show that $M\phi_1\sigma_1 =_E M\phi_2\sigma_2$ and $N\phi_1\sigma_1 =_E N\phi_2\sigma_2$ we rely on the hypothesis that for any two terms M, N of sort r we have that $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$ as well as the construction of σ_1 and σ_2 .

To show that $M\phi_i =_E N\phi_i$ implies $M\phi_i\sigma_i =_E N\phi_i\sigma_i$, we use the notion of *cut function* introduced in [6]. Showing that σ_1 (resp. σ_2) corresponds to a sequence of applications of a cut function allows us to conclude using Lemma 15 of [6]. To show that $M\phi_i\sigma_i =_E N\phi_i\sigma_i$ implies $M\phi_i =_E N\phi_i$ we use the fact that σ_1 and σ_2 are bijective. \square

A complete proof is given in in Appendix B.

Proof (of Theorem 1). We suppose that $\phi_1 \approx_E \phi_2$. By Lemma 4 we have that $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_E \overline{\phi_{2|r}\phi_{2|s}}$.

We will show that

$$\begin{aligned} \phi_{1|r} \approx_E \phi_{2|r}(p) \wedge \overline{\phi_{1|r}\phi_{1|s}} \approx_E \overline{\phi_{2|r}\phi_{2|s}}(q) \\ \Leftrightarrow \\ \phi_{1|r} \approx_{E'} \phi_{2|r}(p_1) \wedge \overline{\phi_{1|r}\phi_{1|s}} \approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}(q_1) \end{aligned}$$

We will prove the three following assertions separately :

$$(1) \neg q \Leftrightarrow \neg q_1 \quad (2) \neg p \Rightarrow \neg p_1 \vee \neg q_1 \quad (3) \neg p_1 \Rightarrow \neg p$$

The conjunction of these three assertions implies the fact that $(p \wedge q) \Leftrightarrow (p_1 \wedge q_1)$.

(1) $\overline{\phi_{1|r}\phi_{1|s}} \not\approx_E \overline{\phi_{2|r}\phi_{2|s}}$ iff $\overline{\phi_{1|r}\phi_{1|s}} \not\approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}$

As $\overline{\phi_{1|r}\phi_{1|s}} \not\approx_E \overline{\phi_{2|r}\phi_{2|s}}$ there exist two terms M and N distinguishing $\overline{\phi_{1|r}\phi_{1|s}}$ and $\overline{\phi_{2|r}\phi_{2|s}}$. As f is a valve, there exist M and N that do not involve any symbol f . As E is sufficiently complete w.r.t. $\{f\}$ we can suppose that frames $\overline{\phi_{1|r}\phi_{1|s}}$ and $\overline{\phi_{2|r}\phi_{2|s}}$ do not involve f . Hence $M\overline{\phi_{i|r}\phi_{i|s}}$ and $N\overline{\phi_{i|r}\phi_{i|s}}$ also do not involve f . As E' is sufficient for E without f we have that $M\overline{\phi_{i|r}\phi_{i|s}} =_E N\overline{\phi_{i|r}\phi_{i|s}}$ iff $M\overline{\phi_{i|r}\phi_{i|s}} =_{E'} N\overline{\phi_{i|r}\phi_{i|s}}$. Hence $\overline{\phi_{1|r}\phi_{1|s}} \not\approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}$.

(2) if $\phi_{1|r} \not\approx_E \phi_{2|r}$ then $\phi_{1|r} \not\approx_{E'} \phi_{2|r}$ or $\overline{\phi_{1|r}\phi_{1|s}} \not\approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}$

Let M and N be two terms distinguishing $\phi_{1|r}$ and $\phi_{2|r}$.

If M is of sort r , as f is a valve, we can suppose w.l.o.g. that M , N , $\phi_{1|r}$ and $\phi_{2|r}$ do not involve any f . Hence $M\phi_{i|r}$ and $N\phi_{i|r}$ do not involve f . As E' is sufficient for E without f we have that $M\phi_{i|r} =_E N\phi_{i|r}$ iff $M\phi_{i|r} =_{E'} N\phi_{i|r}$. Hence $\phi_{1|r} \not\approx_{E'} \phi_{2|r}$.

If M is of sort s , by Lemma 3 there exist terms M' and N' such that $M\phi_{i|r} =_E M'\overline{\phi_{i|r}}$ and $N\phi_{i|r} =_E N'\overline{\phi_{i|r}}$. As f is a valve, M' and N' do not involve any symbol f . By sufficient completeness of E w.r.t. $\{f\}$, we can consider frames $\overline{\phi_{1|r}}$ and $\overline{\phi_{2|r}}$ that do not involve f , $M'\overline{\phi_{i|r}}$ and $N'\overline{\phi_{i|r}}$ do not involve f either. As E' is sufficient without f we have that $M'\overline{\phi_{i|r}} =_E N'\overline{\phi_{i|r}}$ iff $M'\overline{\phi_{i|r}} =_{E'} N'\overline{\phi_{i|r}}$. Hence $\overline{\phi_{1|r}} \not\approx_{E'} \overline{\phi_{2|r}}$ and $\overline{\phi_{1|r}\phi_{1|s}} \not\approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}$.

(3) if $\phi_{1|r} \not\approx_{E'} \phi_{2|r}$ then $\phi_{1|r} \not\approx_E \phi_{2|r}$

As $\phi_{1|r} \not\approx_{E'} \phi_{2|r}$ there exist terms M and N distinguishing $\phi_{1|r}$ and $\phi_{2|r}$.

If there are no terms M and N of sort r distinguishing $\phi_{1|r}$ and $\phi_{2|r}$, by Lemma 5 there are no terms of sort s distinguishing $\phi_{1|r}$ and $\phi_{2|r}$. Hence if $\phi_{1|r} \not\approx_{E'} \phi_{2|r}$ then there are terms M and N distinguishing $\phi_{1|r}$ and $\phi_{2|r}$ of sort r .

If M is of sort r , as f is a valve, $M, N, \phi_{1|r}$ and $\phi_{2|r}$ do not involve any f . Hence $M\phi_{i|r}$ and $N\phi_{i|r}$ do not involve f . As E' is sufficient without f we have that $M\phi_{i|r} =_{E'} N\phi_{i|r}$ iff $M\phi_{i|r} =_E N\phi_{i|r}$. Hence $\phi_{1|r} \not\approx_E \phi_{2|r}$. \square

We denote by E^{-r} the equational theory E without equations of sort r .

Corollary 1. *Let E be an equational theory on the sorted signature $(\mathcal{S}, \mathcal{F} \cup \{f\})$ such that (i) f is a valve, (ii) E is a reducible equational theory for f , and (iii) E is sufficiently complete w.r.t. $\{f\}$. If there exists an equational theory E' sufficient for E without f then for any $\{r, s\}$ -sorted frames ϕ_1 and ϕ_2 , we have that $\phi_1 \approx_E \phi_2$ iff $\phi_{1|r} \approx_{E'^{-s}} \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_{E'^{-r}} \overline{\phi_{2|r}\phi_{2|s}}$.*

Proof. By Theorem 1, we have $\phi_1 \approx_E \phi_2$ iff $\phi_{1|r} \approx_{E'} \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}$.

By Lemma 5, we have that if for any two terms M and N of sort r ($M =_E N$) ϕ_1 iff ($M =_E N$) ϕ_2 , then for any two terms M and N of sort s , ($M =_E N$) ϕ_1 iff ($M =_E N$) ϕ_2 . Hence it is sufficient to consider terms of sort r to decide static equivalence between $\phi_{1|r}$ and $\phi_{2|r}$. As f is a valve for any term M , no subterms of M are of sort s . We can consider only E'^{-r} to decide static equivalence between $\phi_{1|r}$ and $\phi_{2|r}$.

Let us show that $\overline{\phi_{1|r}\phi_{1|s}} \approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}$ iff $\overline{\phi_{1|r}\phi_{1|s}} \approx_{E'^{-r}} \overline{\phi_{2|r}\phi_{2|s}}$.

$\overline{\phi_{1|r}\phi_{1|s}} \not\approx_{E'} \overline{\phi_{2|r}\phi_{2|s}}$ iff there are two terms M and N distinguishing $\overline{\phi_{1|r}\phi_{1|s}}$ and $\overline{\phi_{2|r}\phi_{2|s}}$. As f is a valve, there exist M and N that do not involve any symbol f . As E is sufficiently complete w.r.t. $\{f\}$ we can suppose that frames $\overline{\phi_{1|r}\phi_{1|s}}$ and $\overline{\phi_{2|r}\phi_{2|s}}$ do not involve f . Hence $M\overline{\phi_{i|r}\phi_{i|s}}$ and $N\overline{\phi_{i|r}\phi_{i|s}}$ do not involve f either. As f is a valve $M\overline{\phi_{i|r}\phi_{i|s}}$ and $N\overline{\phi_{i|r}\phi_{i|s}}$ do not involve subterms of sort r we have that $M\overline{\phi_{i|r}} =_{E'} N\overline{\phi_{i|r}}$ iff $M\overline{\phi_{i|r}\phi_{i|s}} =_{E'^{-r}} N\overline{\phi_{i|r}\phi_{i|s}}$. Hence $\overline{\phi_{1|r}\phi_{1|s}} \not\approx_{E'^{-r}} \overline{\phi_{2|r}\phi_{2|s}}$. \square

6 A criterion for sufficient equational theories

In this section we make a first attempt to find sufficient criteria for applying Theorem 1. Future work includes finding broader criteria. We also briefly explain how our running example fits this criterion.

Definition 10 (decomposition). *A pair (\mathcal{R}, E') is a decomposition of an equational theory E iff*

- E' is an equational theory,
- \mathcal{R} is a rewriting system convergent modulo E' ,
- for any terms u and v $u =_E v$ iff $u \downarrow_{\mathcal{R}/E'} = v \downarrow_{\mathcal{R}/E'}$.

Definition 11 (exclusively define). *Let $(\mathcal{S}, \mathcal{F} \uplus \{f\})$ be a sorted signature. A rewriting system \mathcal{R} exclusively defines f if any term in normal form modulo \mathcal{R}/E' is in $T(\mathcal{F}, \mathcal{N})$ and if for any rewrite rule $l \rightarrow r \in \mathcal{R}$, f appears in l .*

Lemma 6. *Let $(\mathcal{S}, \mathcal{F} \uplus \{f\})$ be a signature. If a theory E on this signature has a decomposition (\mathcal{R}, E') and if \mathcal{R} exclusively defines f then E' is sufficient for E without f .*

Proof. Let u and v be two terms not involving f . As \mathcal{R} exclusively defines f and as u and v do not involve any f symbol, no rule of \mathcal{R} can be applied. Hence $u =_E v$ iff $u =_{E'} v$. \square

Example 5 (continued). We define \mathcal{R}_{BP} to be the rewriting system obtained by orienting the rule $e(\text{exp}_1(x), \text{exp}_1(y)) = \text{exp}_2(x \cdot y)$ from left to right, and E'_{BP} the equational theory E_{BP} without this rule. We remark that $(\mathcal{R}, E'_{\text{BP}})$ is a decomposition of E_{BP} and it is easy to see that \mathcal{R} exclusively defines e .

Corollary 2. *If the set of names of sorts G_1 and G_2 are empty, static equivalence for E_{BP} is decidable for $\{G_1, G_2\}$ -sorted frames.*

Proof. As \mathcal{R}_{BP} exclusively defines e , by Lemma 6, we have that E'_{BP} is sufficient for E_{BP} without e . By Proposition 1 we have that E_{BP} is reducible for f . Finally, as the set of names of sorts G_1 and G_2 is empty, E_{BP} is sufficiently complete for e . Hence by Corollary 1, for two frames ϕ_1 and ϕ_2 , $\phi_1 \approx_E \phi_2$ iff $\phi_1|_{G_1} \approx_{E'_{\text{BP}}-G_2} \phi_2|_{G_1}$ and $\overline{\phi_1|_{G_1} \phi_1|_{G_2}} \approx_{E'_{\text{BP}}-G_1} \overline{\phi_2|_{G_1} \phi_2|_{G_2}}$.

As $E'_{\text{BP}}-G_2$ and $E'_{\text{BP}}-G_1$ correspond both to the classical equational theory modelling Diffie-Hellman, which is known to be decidable [13] for frames whose only names are of sort R we have that static equivalence is decidable for E_{BP} on $\{G_1, G_2\}$ -sorted frames. \square

7 Conclusion and future work

In this paper we have defined the notions of valve and reducibility which allow to simplify equational theories for the decision of static equivalence. This constitutes a first step towards finding generic criteria. Our results apply to the case of bilinear pairing. We believe that this result may apply to other situations where several algebraic structures are used in the model of the same cryptographic operator. In the short term we are investigating the following directions:

(1) We are trying to identify criteria for reducibility which are easier to decide. Even on our quite simple example, proving reducibility is a bit technical. Hence we are trying to determine either syntactic criteria on the equational theory, or more classical properties as a constrained form of sufficient completeness, that would imply reducibility.

(2) In this paper we have analyzed the case where there is only one reducible valve in an equational theory. Extending reducibility to the case where several valves belong to the theory seems possible. However it requires defining a priority order on the reductions of the different valves.

(3) We are also trying to widen the notion of valve. In the definition we propose here, a valve is defined from a given sort to another. Yet cases where

a valve takes as argument terms of different sorts can be considered. We think that such a notion could give rise to a wider notion of reducibility than the one we have analyzed. It seems that we need conditions on the links between the arguments of such valves.

References

1. M. Abadi, B. Blanchet, and C. Fournet. Verification of selected equivalences for security protocols. *Journal of Logic and Algebraic Programming*, 75(1):3–51, 2008.
2. M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 367(1):2–32, 2006.
3. M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115. ACM Press, 2001.
4. M. Arnaud, V. Cortier, and S. Delaune. Combining algorithms for deciding knowledge in security protocols. In *Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07)*, volume 4720 of *LNCS*, pages 103–117. Springer, 2007.
5. M. Baudet. Deciding security of protocols against off-line guessing attacks. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 16–25. ACM Press, 2005.
6. M. Baudet, V. Cortier, and S. Kremer. Computationally sound implementations of equational theories against passive adversaries. *Information and Computation*, 207(4):496–520, 2009.
7. D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'01)*, volume 2139 of *LNCS*, pages 213–229. Springer, 2001.
8. H. Common. Inductionless induction. In *Handbook of Automated Reasoning*. Elsevier, 2001.
9. R. Corin, J. Doumen, and S. Etalle. Analysing password protocol security against off-line dictionary attacks. In *Proceedings of the 2nd International Workshop on Security Issues with Petri Nets and other Computational Models (WISP 2004)*, volume 121 of *ENTCS*, pages 47–63. Elsevier, 2004.
10. V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.
11. D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
12. A. Joux. A one round protocol for tripartite Diffie-Hellman. In *Proceedings of the 4th International Symposium on Algorithmic Number Theory (ANTS-IV)*, volume 1838 of *LNCS*, pages 385–394. Springer, 2000.
13. S. Kremer and L. Mazaré. Adaptive soundness of static equivalence. In *Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS'07)*, volume 4734 of *LNCS*, pages 610–625. Springer, 2007.
14. S. Kremer and L. Mazaré. Computationally sound analysis of protocols using bilinear pairings. *Journal of Computer Security*, 2009. To appear.

A Proof of Lemma 4

Lemma 4. *For any $\{r, s\}$ -sorted frames ϕ_1 and ϕ_2 built on $(\mathcal{S}, \mathcal{F})$, and for a value f from r to s , if E is a reducible equational theory for f then $\phi_1 \approx_E \phi_2$ iff $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_E \overline{\phi_{2|r}\phi_{2|s}}$.*

Proof. Let us prove the two directions of the equivalence separately. For a frame ϕ we denote the variables of $\phi|_r$ by \vec{x}_ϕ , the variables of $\overline{\phi|_r}$ by \vec{y}_ϕ and the variables of $\phi_{i|s}$ by \vec{z}_ϕ . As in most cases the frame ϕ we are dealing with is clear from the context, we simply write \vec{x} , \vec{y} and \vec{z} . We extend this notation to vectors of terms.

(\Rightarrow) *If $\phi_1 \approx_E \phi_2$, then $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_E \overline{\phi_{2|r}\phi_{2|s}}$.*

Let us first suppose that $\phi_{1|r} \not\approx_E \phi_{2|r}$. Then, w.l.o.g. there are two terms $M[\vec{x}]$ and $N[\vec{x}]$ such that $(M =_E N)\phi_{1|r}$ and $(M \neq_E N)\phi_{2|r}$. As $\text{dom}(\phi_{i|r}) \subseteq \text{dom}(\phi_i)$ and $\text{dom}(\phi_{1|r}) = \text{dom}(\phi_{2|r})$, we have that $(M =_E N)\phi_1$ and $(M \neq_E N)\phi_2$, and then $\phi_1 \not\approx_E \phi_2$.

Let us now suppose that $\overline{\phi_{1|r}\phi_{1|s}} \not\approx_E \overline{\phi_{2|r}\phi_{2|s}}$. Then there exist two terms $M[\vec{y}, \vec{z}]$ and $N[\vec{y}, \vec{z}]$ such that w.l.o.g. $(M =_E N)\overline{\phi_{1|r}\phi_{1|s}}$ and $(M \neq_E N)\overline{\phi_{2|r}\phi_{2|s}}$.

As $\overline{\phi_{1|r}}$ (resp. $\overline{\phi_{2|r}}$) is a reduction of $\phi_{1|r}$ (resp. $\phi_{2|r}$) and $\text{dom}(\phi_1) = \text{dom}(\phi_2)$, there exists a set of terms $T_j[\vec{x}]$ such that $M[\vec{y}, \vec{z}]\overline{\phi_{i|r}\phi_{i|s}} =_E M[\overline{T[\vec{x}]}, \vec{z}]\phi_i$ and $N[\vec{y}, \vec{z}]\overline{\phi_{i|r}\phi_{i|s}} =_E N[\overline{T[\vec{x}]}, \vec{z}]\phi_i$. We then conclude that $M[\overline{T[\vec{y}]}, \vec{z}]$ and $N[\overline{T[\vec{y}]}, \vec{z}]$ distinguish ϕ_1 and ϕ_2 .

Then supposing that the conjunction of the two assertions $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_E \overline{\phi_{2|r}\phi_{2|s}}$ is false, we have that one of these is false. As the negation of each of them imply that $\phi_1 \not\approx_E \phi_2$, we have that $\phi_1 \approx_E \phi_2$ implies that $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_E \overline{\phi_{2|r}\phi_{2|s}}$.

(\Leftarrow) *If $\phi_{1|r} \approx_E \phi_{2|r}$ and $\overline{\phi_{1|r}\phi_{1|s}} \approx_E \overline{\phi_{2|r}\phi_{2|s}}$ then $\phi_1 \approx_E \phi_2$.*

Let us suppose that $\phi_1 \not\approx_E \phi_2$. Hence there exist two terms $M[\vec{x}, \vec{y}]$ and $N[\vec{x}, \vec{y}]$ such that w.l.o.g. $(M =_E N)\phi_1$ and $(M \neq_E N)\phi_2$. As $(M =_E N)\phi_1$, M and N have the same sort. We consider both cases :

If $\text{sort}(M) = r$, as the only sort transition possibility is directed from r to s (by the second item of the lemma), all variables of M are of sort r . Hence, M and N distinguish $\phi_{1|r}$ and $\phi_{2|r}$.

If $\text{sort}(M) = s$, as $\text{dom}(\phi_{1|r}) = \text{dom}(\phi_{2|r})$ by Lemma 3 there exists terms M' and N' such that $M\phi_i =_E M'\overline{\phi_{i|r}\phi_{i|s}}$ and $N\phi_i =_E N'\overline{\phi_{i|r}\phi_{i|s}}$, for $i \leq 2$. Then if M and N distinguish ϕ_1 and ϕ_2 then w.l.o.g. $(M =_E N)\phi_1$ and $(M \neq_E N)\phi_2$. Hence, $(M =_E N)\overline{\phi_{1|r}\phi_{1|s}}$ and $(M \neq_E N)\overline{\phi_{2|r}\phi_{2|s}}$. \square

B Proof of Lemma 5

We use the following notation and lemma introduced in [6].

Given $u = f(u_1, \dots, u_n)$ where f is free and a name a of the same sort as u , the *cutting function* $\text{cut}_{u,a}$ is defined recursively as follows: $\text{cut}_{u,a}(u) = u$ if u is a variable or a name, and

$$\text{cut}_{u,a}(g(t_1, \dots, t_n)) = \begin{cases} a & \text{if } g = f, k = n \text{ and } \forall 1 \leq i \leq n, u_i =_E t_i \\ g(\text{cut}_{u,a}(t_1), \dots, \text{cut}_{u,a}(t_n)) & \text{otherwise} \end{cases}$$

Thus, the effect of function $\text{cut}_{u,a}(t)$ is to substitute some (but not all) subterms of t equal to u modulo E with a . In the case where f is a valve, the effect of $\text{cut}_{u,a}(t)$ is to substitute every subterm of t equal to u modulo E with a .

Lemma 7 ([6]). *Let E be an equational theory where f is free. Let $u = f(u_1, \dots, u_n)$ be a term such that f is a free symbol. Let a be a name of the same sort as u . For any two terms M and N ,*

$$M =_E N \text{ implies } \text{cut}_{u,a}(M) =_E \text{cut}_{u,a}(N)$$

Lemma 8. *Let ϕ_1 and ϕ_2 be two $\{r\}$ -typed frames, f be a valve from r to s and E be an equational theory where f is free. If for any two terms M' and N' of type r $M'\phi_1 =_E N'\phi_1$ iff $M'\phi_2 =_E N'\phi_2$, then for any two terms M and N of type s headed by f , $M\phi_1 =_E N\phi_1$ iff $M\phi_2 =_E N\phi_2$.*

Proof. Let $M := f(C_1^M, \dots, C_k^M)$ and $N := f(C_1^N, \dots, C_k^N)$. As f is free $M\phi_1 =_E N\phi_1$ iff $C_i^M\phi_1 =_E C_i^N\phi_1$. As for any two terms M' and N' of type r ($M' =_E N'$) ϕ_1 iff $(M' =_E N')\phi_2$, in particular $C_i^M\phi_1 =_E C_i^N\phi_1$ iff $C_i^M\phi_2 =_E C_i^N\phi_2$. Again, as f is free $C_i^M\phi_2 =_E C_i^N\phi_2$ iff $M\phi_2 =_E N\phi_2$. \square

Lemma 5. *Let ϕ_1 and ϕ_2 be two $\{r\}$ -sorted frames, E an equational theory, and f a valve from r to a distinct sort s , which is free in E . If for any two terms M, N of sort r $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$, then for any two terms M and N of sort s , $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$.*

Proof. We will exhibit two replacements functions σ_1 (resp. σ_2) defined on pairs (α, p) where α identifies M (or N) and p is a position in $(M\phi_1)$ (or $N\phi_1$) (resp. $M\phi_2, N\phi_2$) such that $M\phi_1|_p$ (or $N\phi_1|_p$) is headed by f . The co-domain of σ_1 (resp. σ_2) is a set of fresh names w.r.t. ϕ_1 (resp. ϕ_2). We first show that $M\phi_1\sigma_1 =_E M\phi_2\sigma_2$ and $N\phi_1\sigma_1 =_E N\phi_2\sigma_2$ under the condition that for any two terms M, N of type r $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$. Afterwards we show that $M\phi_i =_E N\phi_i$ iff $M\phi_i\sigma_i =_E N\phi_i\sigma_i$ for $i \in \{1, 2\}$. For this we first show that σ_1 (resp. σ_2) corresponds to a sequence of cutting function applications, and we use Lemma 7 and the fact that σ_1 and σ_2 are bijective. The conjunction of these assertions implies that for any two terms M, N of type s , $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$.

Let us define σ_1 and σ_2 . We consider a set of fresh names of the form $a_{\alpha,\beta}$ where $\alpha \in \{\mathcal{M}, \mathcal{N}\}$ and $\beta \in Pos(M) \cup Pos(N)$. Intuitively, the functions σ_i replace a same (up to $=_E$) term $f(C_1, \dots, C_k)$ by a same fresh name $a_{\alpha,\beta}$. Here α, β identifies the first occurrence of $f(C_1, \dots, C_k)$ during a breadth-first traversal of $M\phi_i$ followed by a breadth-first traversal of $N\phi_i$. More formally we define the total order $<$ on the cartesian product $\{\mathcal{M}, \mathcal{N}\} \times Pos(M) \cup Pos(N)$ as follows. Let p_1 and p_2 two positions in $Pos(M) \cup Pos(N)$. $(\alpha_1, p_1) < (\alpha_2, p_2)$ iff

- $\alpha_1 = \mathcal{M}$ and $\alpha_2 = \mathcal{N}$,
- or $|p_1| < |p_2|$,
- or $|p_1| = |p_2|$ and $p_1 <_{lex} p_2$ where $<_{lex}$ is the lexicographic order.

Note that M (resp. N) is of the form $C_{\mathcal{M}}[f(C_{\mathcal{M}1}^1, \dots, C_{\mathcal{M}k}^1), \dots, f(C_{\mathcal{M}1}^m, \dots, C_{\mathcal{M}k}^m)]$ (resp. $C_{\mathcal{N}}[f(C_{\mathcal{N}1}^1, \dots, C_{\mathcal{N}k}^1), \dots, f(C_{\mathcal{N}1}^l, \dots, C_{\mathcal{N}k}^l)]$) where every variables of M (resp. N) are in the $f(C_{\mathcal{M}1}^i, \dots, C_{\mathcal{M}k}^i)$ (resp. $f(C_{\mathcal{N}1}^i, \dots, C_{\mathcal{N}k}^i)$). We then have that $M\phi_i = C_{\mathcal{M}}[f(C_{\mathcal{M}1}^1, \dots, C_{\mathcal{M}k}^1)\phi_i, \dots, f(C_{\mathcal{M}1}^m, \dots, C_{\mathcal{M}k}^m)\phi_i]$ and $N\phi_i = C_{\mathcal{N}}[f(C_{\mathcal{N}1}^1, \dots, C_{\mathcal{N}k}^1)\phi_i, \dots, f(C_{\mathcal{N}1}^l, \dots, C_{\mathcal{N}k}^l)\phi_i]$. We write $Pos(M\phi_i) \cup Pos(N\phi_i)|_f$ for the set of positions of $M\phi_i, N\phi_i$ headed by f . Hence we can do the following remarks.

Remark 2. We have that $Pos(M\phi_1)|_f = Pos(M\phi_2)|_f = Pos(M)|_f$ and $Pos(N\phi_1)|_f = Pos(N\phi_2)|_f = Pos(N)|_f$.

Remark 3. $M\phi_1|_p = f(C_1, \dots, C_k)\phi_1$ iff $M\phi_2|_p = f(C_1, \dots, C_k)\phi_2$ for some M, C_1, \dots, C_k .

We define σ_i on the domain $\mathcal{M} \times Pos(M)|_f \cup \mathcal{N} \times Pos(N)|_f$ (remark 2). We denote by τ the function associating M to \mathcal{M} and N to \mathcal{N} . Let $(\alpha, p) \in \text{dom}(\sigma_i)$.

- If for every pair (α', p') such that $(\alpha', p') < (\alpha, p)$, $\tau(\alpha')\phi_i|_{p'} \neq_E \tau(\alpha)\phi_i|_p$ then $\sigma_i(\alpha, p) = a_{\alpha,p}$,
- else let (α', p') be the minimal element such that $\tau(\alpha')\phi_i|_{p'} =_E \tau(\alpha)\phi_i|_p$, $\sigma_i(p, \alpha) = a_{\alpha',p'}$.

For any term M , we note $M\phi_i\sigma_i$ the term $M\phi_i[\sigma_i((\mathcal{M}, p))]_p$ for $p \in Pos(M)|_f$.

We show by induction on the structure of C_α that $\tau(\alpha)\phi_1\sigma_1 = \tau(\alpha)\phi_2\sigma_2$, for $\alpha \in \{\mathcal{M}, \mathcal{N}\}$.

Base case : C_α is a variable. We distinguish two cases :

- $\alpha = \mathcal{M}$. In this case we have that $M\phi_1 = f(C_{\mathcal{M}1}^1, \dots, C_{\mathcal{M}k}^1)\phi_1$. By definition of σ_1 $M\phi_1\sigma_1 = a_{\mathcal{M},A}$. We also have that $M\phi_2 = f(C_{\mathcal{M}1}^1, \dots, C_{\mathcal{M}k}^1)\phi_2$. By definition of σ_2 $M\phi_2\sigma_2 = a_{\mathcal{M},A}$. Straightforwardly $M\phi_1\sigma_1 = M\phi_2\sigma_2$.
- $\alpha = \mathcal{N}$. In this case we have that $N\phi_1 = f(C_{\mathcal{N}1}^1, \dots, C_{\mathcal{N}k}^1)\phi_1$. We distinguish two sub-cases :

- Either for any (\mathcal{M}, p) , $M\phi_1|_p \neq_E f(C_{N_1}^1, \dots, C_{N_k}^1)\phi_1$. Hence $N\phi_1\sigma_1 = a_{N, \Lambda}$. Note that $M\phi_1|_p$ are of the form $f(C_{\mathcal{M}_1}^i, \dots, C_{\mathcal{M}_k}^i)\phi_1$, such that by Remark 3 $M\phi_2|_p = f(C_{\mathcal{M}_1}^i, \dots, C_{\mathcal{M}_k}^i)\phi_2$. By Remark 3, we also have that $N\phi_2 = f(C_{N_1}^1, \dots, C_{N_k}^1)\phi_2$. As by Lemma 8, $f(C_{N_1}^1, \dots, C_{N_k}^1)\phi_1 \neq_E f(C_{\mathcal{M}_1}^i, \dots, C_{\mathcal{M}_k}^i)\phi_1$ iff $f(C_{N_1}^1, \dots, C_{N_k}^1)\phi_2 \neq_E f(C_{\mathcal{M}_1}^i, \dots, C_{\mathcal{M}_k}^i)\phi_2$, we have that $M\phi_2|_p \neq_E N\phi_2$ for all (\mathcal{M}, p) . Hence $T_j\phi_2\sigma_2 = a_{N, \Lambda}$.
- Or let (\mathcal{M}, p) be the minimal pair such that $M\phi_1|_p =_E f(C_{N_1}^1, \dots, C_{N_k}^1)\phi_1$. Hence $N\phi_1\sigma_1 = a_{\mathcal{M}, p}$. Note that $M\phi_1|_p$ is of the form $f(C_{\mathcal{M}_1}^i, \dots, C_{\mathcal{M}_k}^i)\phi_1$, such that by Remark 3 $M\phi_2|_p = f(C_{\mathcal{M}_1}^i, \dots, C_{\mathcal{M}_k}^i)\phi_2$. By Remark 3, we also have that $N\phi_2 = f(C_{N_1}^1, \dots, C_{N_k}^1)\phi_2$. As by Lemma 8, $N\phi_1 =_E f(C_{\mathcal{M}_1}^i, \dots, C_{\mathcal{M}_k}^i)\phi_1$ iff $N\phi_2 =_E f(C_{\mathcal{M}_1}^i, \dots, C_{\mathcal{M}_k}^i)\phi_2$, we have that $M\phi_2|_p =_E N\phi_2$. Now if there was a pair $(\mathcal{M}, p') < (\mathcal{M}, p)$ such that $M\phi_2|_{p'} =_E M\phi_2|_p$, it would contradict the fact that (\mathcal{M}, p) is the minimal pair such that $M\phi_1|_p =_E N\phi_1$. We then conclude that $N\sigma_2 = a_{\mathcal{M}, p}$.

In both sub-cases we have $N\phi_1\sigma_1 = N\phi_2\sigma_2$.

In both cases we have that $\tau(\alpha)\phi_1\sigma_1 = \tau(\alpha)\phi_2\sigma_2$.

Inductive case. $C_\alpha := g(T_1, \dots, T_n)$. where $\text{sort}(T_i) = s$.

- Either for any T_i , T_i is not headed by f . Hence by induction $T_i\phi_1\sigma_1 = T_i\phi_2\sigma_2$. Hence $\tau(\alpha)\phi_1\sigma_1 = \tau(\alpha)\phi_2\sigma_2$.
- Or for some T_i , $T_i := x$. We do an induction on the number of T_i of this form :
 - If there are no such T_i , we are in the previous case, and we conclude in the same way.
 - There are some T_i such that T_i is a variable. Let I be the set of indexes of the T_i that are variables. Let T_j be a variable such that j is maximal in I . Let us consider $T_j\phi_1\sigma_1$. Note that $T_j\phi_1$ is of the form $f(C_{\alpha_1}^i, \dots, C_{\alpha_k}^i)\phi_1$ such that by Remark 3 $T_j\phi_2 = f(C_{\alpha_1}^i, \dots, C_{\alpha_k}^i)\phi_2$ for some i .
 - * Either for any $(\alpha', p) < (\alpha, \Lambda, j)$ $\tau(\alpha')\phi_1|_p \neq_E \tau(\alpha)\phi_1|_{\Lambda, j}$. Hence $T_j\phi_1\sigma_1 = a_{\alpha, \Lambda, j}$. Note that $\tau(\alpha')\phi_1|_p$ are of the form $f(C_{\alpha'_1}^{i'}, \dots, C_{\alpha'_k}^{i'})\phi_1$, such that by Remark 3 $\tau(\alpha')\phi_2|_p = f(C_{\alpha'_1}^{i'}, \dots, C_{\alpha'_k}^{i'})\phi_2$. As by Lemma 8, $f(C_{\alpha_1}^i, \dots, C_{\alpha_k}^i)\phi_1 \neq_E f(C_{\alpha'_1}^{i'}, \dots, C_{\alpha'_k}^{i'})\phi_1$ iff $f(C_{\alpha_1}^i, \dots, C_{\alpha_k}^i)\phi_2 \neq_E f(C_{\alpha'_1}^{i'}, \dots, C_{\alpha'_k}^{i'})\phi_2$, we have that $\tau(\alpha')\phi_2|_p \neq_E N\phi_2|_{\Lambda, j}$ for all $(\mathcal{M}, p) < (\mathcal{M}, \Lambda, j)$. Hence $T_j\phi_2\sigma_2 = a_{\mathcal{M}, \Lambda, j}$.
 - * Or let (α', p) be the minimal pair such that $(\alpha', p) < (\alpha, \Lambda, j)$ and $\tau(\alpha')\phi_1|_p =_E \tau(\alpha)\phi_1|_{\Lambda, j}$. Hence $T_j\phi_1\sigma_1 = a_{\alpha', p}$. Note that $\tau(\alpha')\phi_1|_p$ is of the form $f(C_{\alpha'_1}^{i'}, \dots, C_{\alpha'_k}^{i'})\phi_1$, such that by Remark 3 $\tau(\alpha')\phi_2|_p = f(C_{\alpha'_1}^{i'}, \dots, C_{\alpha'_k}^{i'})\phi_2$. As by Lemma 8, $f(C_{\alpha_1}^i, \dots, C_{\alpha_k}^i)\phi_1 =_E f(C_{\alpha'_1}^{i'}, \dots, C_{\alpha'_k}^{i'})\phi_1$ iff $f(C_{\alpha_1}^i, \dots, C_{\alpha_k}^i)\phi_2 =_E f(C_{\alpha'_1}^{i'}, \dots, C_{\alpha'_k}^{i'})\phi_2$, we have that $\tau(\alpha')\phi_2|_p =_E \tau(\alpha)\phi_2|_{\Lambda, j}$. Now if there was a pair $(\alpha'', p') < (\alpha', p)$ such that $\tau(\alpha'')\phi_2|_{p'} =_E \tau(\alpha)\phi_2|_{\Lambda, j}$, it would imply by a similar reasoning that $\tau(\alpha'')\phi_1|_{p'} =_E \tau(\alpha)\phi_1|_{\Lambda, j}$ which would contradict the fact that (α', p) is the minimal pair such that $\tau(\alpha')\phi_1|_p =_E \tau(\alpha)\phi_1|_{\Lambda, j}$. We then conclude that $T_j\phi_2\sigma_2 = a_{\alpha', p}$.

In both case we have that $T_j\phi_1\sigma_1 =_E T_j\phi_2\sigma_2$. As by induction we suppose that for any $i < j$ $T_i\phi_1\sigma_1 =_E T_i\phi_2\sigma_2$ we have that for any i $T_i\phi_1\sigma_1 =_E T_i\phi_2\sigma_2$, and then $\tau(\alpha)\phi_1\sigma_1 = \tau(\alpha)\phi_2\sigma_2$.

Let us show by induction on the number of names in the co-domain of σ_i , there is a sequence $\text{cut}_{u_1, a_1}, \dots, \text{cut}_{u_n, a_n}$ such that $M\phi_i\sigma_i = \text{cut}_{u_n, a_n}(\dots(\text{cut}_{u_1, a_1}(M\phi_i))\dots)$ and $N\phi_i\sigma_i = \text{cut}_{u_n, a_n}(\dots(\text{cut}_{u_1, a_1}(N\phi_i))\dots)$.

Base case. There are no names in the co-domain of σ_i . Hence σ_i is empty and $M\phi_i\sigma_i = M\phi_i$, and $N\phi_i\sigma_i = N\phi_i$.

Inductive case. Let us consider the name $a_{\alpha, p}$ such that for any name $a_{\alpha', p'}$ in the co-domain of σ_i $(\alpha, p) > (\alpha', p')$. We write $\sigma_i \setminus a_{\alpha, p}$ the function σ_i where we have removed the elements of the form $(t, a_{\alpha, p})$ for some t and $\sigma_i|_{a_{\alpha, p}}$ the set of elements of σ_i of the form $(t, a_{\alpha, p})$ for some t . By induction we have that there is a sequence of $\text{cut}_{u_1, a_1}, \dots, \text{cut}_{u_n, a_n}$ such that $M\phi_i\sigma_i \setminus a_{\alpha, p} = \text{cut}_{u_n, a_n}(\dots(\text{cut}_{u_1, a_1}(M\phi_i))\dots)$ and $N\phi_i\sigma_i \setminus a_{\alpha, p} = \text{cut}_{u_n, a_n}(\dots(\text{cut}_{u_1, a_1}(N\phi_i))\dots)$. Now by definition of σ_i if there are several pairs $(\alpha_1, p_1), \dots, (\alpha_n, p_n)$ mapped to $a_{\alpha, p}$, it means that $\tau(\alpha_1)\phi_i|_{p_1} = \dots = \tau(\alpha_n)\phi_i|_{p_n} = \tau(\alpha_1)\phi_i|_p$ and we also have that $\tau(\alpha_1)\phi_i|_{p_1}$ is headed by f by definition of σ_i . Hence applying $\sigma_i|_{a_{\alpha, p}}$ is identical to applying $\text{cut}_{\tau(\alpha)\phi_i|_p, a_{\alpha, p}}$. As $M\phi_i\sigma_i = M\phi_i\sigma_i \setminus a_{\alpha, p}\sigma_i|_{a_{\alpha, p}}$. As $M\phi_i\sigma_i \setminus a_{\alpha, p} = \text{cut}_{u_n, a_n}(\dots(\text{cut}_{u_1, a_1}(M\phi_i))\dots)$, we have that $M\phi_i\sigma_i = \text{cut}_{\tau(\alpha)\phi_i|_p, a_{\alpha, p}}(\text{cut}_{u_n, a_n}(\dots(\text{cut}_{u_1, a_1}(M\phi_i))\dots))$. We do the same for N .

By iterating Lemma 7 we have that if $M\phi_i =_E N\phi_i$ then $M\phi_i\sigma_i =_E N\phi_i\sigma_i$. On the other hand, as σ_1 is bijective we have that if $M\phi_i\sigma_i =_E N\phi_i\sigma_i$ then $M\phi_i =_E N\phi_i$. (It is sufficient to replace the fresh names we introduced by the terms at the position determined by their pre-image by σ_i). Hence $M\phi_i =_E N\phi_i$ iff $M\phi_i\sigma_i =_E N\phi_i\sigma_i$. As $M\phi_1\sigma_1 =_E M\phi_2\sigma_2$ and $N\phi_1\sigma_1 =_E N\phi_2\sigma_2$, we have $M\phi_1\sigma_1 =_E N\phi_1\sigma_1$ iff $M\phi_2\sigma_2 =_E N\phi_2\sigma_2$. Hence $M\phi_1 =_E N\phi_1$ iff $M\phi_2 =_E N\phi_2$. \square

C Proof of Lemma 2

Lemma 9. *There exists an equational theory E and a valve f such that E is sufficiently complete for E but not reducible for E .*

Proof. We define a signature with two sorts r and s , no names, and function and constant symbols like this:

$$\begin{aligned} 0_r &: r \\ s_r &: r \rightarrow r \\ f &: r \rightarrow s \\ 0_s &: s \\ s_s &: s \rightarrow s \end{aligned}$$

The function symbol f is the valve. We have the following equational theory:

$$\begin{aligned} f(s_r(x), y) &= s_s(f(x, y)) \\ f(0_r, s_r(y)) &= f(s_r(y), y) \\ f(0_r, 0_r) &= o_s \end{aligned}$$

We identify ground terms build of only 0_r and s_r , as well as ground terms build only of 0_s and s_s , with natural numbers. In this notation one easily sees that for all $n, m \in \mathbf{N}$:

$$f(n, m) = n + \frac{m * (m + 1)}{2}$$

In particular note that E is sufficiently complete for f since there are no names of sort r . Now let us assume that E is reducible for f . We choose $n = 1$. Note that, due to the sort restrictions, any context $C[x]$ is of the form $s_r^c(x)$ for some constant c , which we write according to our notation as $c + x$. A context $D[y_1, \dots, y_m]$ is of the form $\lambda y_1, \dots, y_m. s_s^d(y_i)$, which we now write as $d + y_i$, and any context $T_i[x]$ is of the form $s_s^{n_i}(f(s_r^{m_i}(x), s_r^{k_i}(x)))$.

According to the definition of reducibility, there are finitely many n_i, m_i , and k_i (for $1 \leq i \leq m$) such that for all c (we choose the identity for the first context, the second context is $\lambda x. s_r^c(x)$) there exists an index i_0 and a context $D = \lambda y_1, \dots, y_m. s_s^d(y_i)$ such that for all t :

$$f(t, c + t) = d + n_{i_0} + f(m_{i_0} + t, k_{i_0} + t)$$

With the above equation for f this yields:

$$t + \frac{(c + t) * (c + t + 1)}{2} = d + n_{i_0} + m_{i_0} + t + \frac{(k_{i_0} + t) * (k_{i_0} + t + 1)}{2}$$

which simplifies to

$$\frac{c^2}{2} + ct + \frac{c}{2} = d + n_{i_0} + m_{i_0} + \frac{k_{i_0}^2}{2} + k_{i_0}t + \frac{k_{i_0}}{2}$$

By the definition of reducibility, for all c there exist d and i_0 such that the above equation is true for all t . Choose a value c_0 which is different from all the k_i . We obtain that for some d and i_0

$$\forall t. \left(\frac{c_0^2}{2} + c_0t + \frac{c_0}{2} = d + n_{i_0} + m_{i_0} + \frac{k_{i_0}^2}{2} + k_{i_0}t + \frac{k_{i_0}}{2} \right)$$

Instantiating this for the values of $t = 0$ and $t = 1$ we obtain

$$\begin{aligned} \frac{c_0^2}{2} + \frac{c_0}{2} &= d + n_{i_0} + m_{i_0} + \frac{k_{i_0}^2}{2} + \frac{k_{i_0}}{2} \\ \frac{c_0^2}{2} + c_0 + \frac{c_0}{2} &= d + n_{i_0} + m_{i_0} + \frac{k_{i_0}^2}{2} + k_{i_0} + \frac{k_{i_0}}{2} \end{aligned}$$

Subtraction of these two equations yields

$$c_0 = k_{i_0}$$

which contradicts our choice of c_0 being different to all the values k_i . □