Reducing Equational Theories for the Decision of Static Equivalence

Steve Kremer, Antoine Mercier, Ralf Treinen

Journal of Automated Reasoning manuscript No.
(will be inserted by the editor)

Reducing Equational Theories for the Decision of Static Equivalence

Steve Kremer · Antoine Mercier · Ralf Treinen

April 22, 2010

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 for a more accurate representation of cryptographic primitives by modelling properties of operators by equational axioms. We develop a method that allows us 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 [14], 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 of 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 [13]) have been taken into account in logical models by the means of equational theories on the terms.

This work has been partially supported by the ANR-07-SESU-002 project AVOTÉ. A preliminary version has been published in [18]

Steve Kremer
LSV, ENS Cachan, CNRS, INRIA, France

Antoine Mercier
LSV, ENS Cachan, CNRS, INRIA, France

Ralf Treinen
PPS, Université Paris Diderot - Paris 7, CNRS UMR 7126, France

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 [12,5]. There now exist exact [2,6,10], 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, a valve is a function symbol taking arguments of respective sorts $s_1, \ldots, s_k$ and yielding a result of sort s. Moreover, it is the only function symbol which allows to build terms of sort s out of terms of any of the sorts $s_1, \ldots, s_k$. 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 [8,15,17]. 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 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 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 for groups, yielding a new decidability result.

A 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.

One may also mention [9] where a notion of *mode* is used to state a hierarchy on terms allowing to obtain a combination result for non disjoint theories. This result however differs from ours as it studies the problem of deducibility in the presence of an active attacker, not static equivalence. A technical difference is that unlike sorts, the notion of mode does not impose constraints on the terms, it only describes them and is mainly used to define a notion of locality.

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 5.1 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.

A preliminary version of this paper appeared in [18]. This full version contains all detailed proofs and considers a generalized notion of valves which can take arguments from a set of distinct sorts, rather than a single sort.

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 $\mathsf{arity}(f) = s_1 \times \cdots \times s_k \to s$ 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 $\mathcal{N}_s = \{n_{s1}, n_{s2}, \dots\}$ and an infinite ordered set of sorted *variables* $\mathcal{X}$.

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

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

where each t_i is a term of sort s_i and $\mathsf{arity}(f) = s_1 \times \cdots \times s_k \to s$. 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 $\mathsf{sort}(t)$ the sort of term t. We write $\mathsf{var}(t)$ and $\mathsf{names}(t)$ for the set of variables and names occurring in t, respectively. A term t is *ground* iff $\mathsf{var}(t) = \emptyset$. 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 $\mathsf{arity}(t) = s$, otherwise $\mathsf{arity}(t) = s_1 \times \cdots \times s_n \to s$ 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* $Pos(t)$ of a term t are defined as usual by $Pos(u) = \{\Lambda\}$ when $u \in \mathcal{N} \cup \mathcal{X}$ and $Pos(f(t_1, \dots, t_n)) = \{\Lambda\} \cup \{i \cdot \pi \mid 1 \leq i \leq n, \pi \in Pos(t_i)\}$ 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 $\mathrm{dom}(\sigma) = \{x_1, \dots, x_n\}$ 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* $l \to r$ where $l \in T(\mathcal{F},\mathcal{N},\mathcal{X})$ and $r \in T(\mathcal{F},\mathcal{N},\mathsf{var}(l))$. A term $u \in T(\mathcal{F},\mathcal{N},\mathcal{X})$ rewrites to v by $\mathcal{R}$, denoted $u \to_{\mathcal{R}} v$ if there is a rewrite rule $l \to r \in \mathcal{R}$, a position p and a substitution σ such that $u|_p = l\sigma$ and $v = u[r\sigma]_p$. We write $\to^*$ for the transitive and reflexive closure of $\to$. Given a set of equations E, u rewrites modulo E by $\mathcal{R}$ to v, denoted $u \to_{\mathcal{R}/E} v$, if $u =_E t[l\sigma]_p$ and $t[r\sigma]_p =_E v$ for some context t, position p in t, rule $l \to r$ in $\mathcal{R}$, and substitution σ. $\mathcal{R}$ is *E-terminating* if there are no infinite chains $t_1 \to_{\mathcal{R}/E} t_2 \to_{\mathcal{R}/E} \ldots$. $\mathcal{R}$ is *E-confluent* iff whenever $t \to_{\mathcal{R}/E} u$ and $t \to_{\mathcal{R}/E} v$, there exist u',v' such that $u \to^*_{\mathcal{R}/E} u'$, $v \to^*_{\mathcal{R}/E} v'$, 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 $t \to_{\mathcal{R}/E} s$. If $t \to^*_{\mathcal{R}/E} s$ and s is in normal form then we say that s is a normal form of t. When this normal form is unique (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 $\tilde{n}_\phi$ 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 $\mathrm{dom}(\sigma_\phi)$. σ_ϕ is called the *underlying substitution* of ϕ. We extend the notation *dom* to frames by $\mathrm{dom}(\nu\tilde{n}.\sigma) = \mathrm{dom}(\sigma)$. 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 $\mathrm{dom}(\phi) \cap \mathrm{dom}(\psi) = \emptyset$ and $\tilde{n}_\phi \cap \tilde{n}_\psi = \emptyset$ we write $\phi\psi$ for their *disjoint composition* defined as $\phi\psi = \nu(\tilde{n}_\phi \cup \tilde{n}_\psi).\sigma_\phi\sigma_\psi$. Note that $\tilde{n}_\phi \cap \tilde{n}_\psi = \emptyset$ can always be obtained by alpha-conversion of the bound names of ϕ and ψ. The sort of a frame ϕ is the set $S = \{\mathsf{sort}(x) | x \in \mathrm{dom}(\phi)\}$, and we say that ϕ is *S-sorted*. The application of a context C on a frame $\phi = \nu\tilde{n}.\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ is denoted $C\phi$ and defined as $C[t_1,\ldots,t_n]$.

For simplicity, we only consider frames $\phi = \nu\tilde{n}.\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ that bind every name in use, that is, for which $\tilde{n} = \mathsf{names}(t_1,\ldots,t_n)$. Note that even when a name n is bound it may still be disclosed by a frame, for instance when the substitution contains a mapping $x \mapsto n$ (see also Example 1).

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 for some $\nu\tilde{n}.\sigma =_\alpha \phi$ with $\tilde{n} \cap (\mathsf{names}(M) \cup \mathsf{names}(N)) = \emptyset$ we have that $M\sigma =_E N\sigma$.

Definition 2 (static equivalence [2]) Two frames ϕ and ψ are *statically equivalent* for the equational theory E, written $\phi \approx_E \psi$, iff $\mathrm{dom}(\phi) = \mathrm{dom}(\psi)$, 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 $(M \neq_E N)\psi$, or $(M \neq_E N)\phi$ and $(M =_E N)\psi$, are called *distinguishers* of ϕ and ψ.

Example 1 Consider the signature $(\{\mathsf{data}\}, \{\mathsf{enc}, \mathsf{dec}, 0, 1\})$ where enc and dec are two binary function symbols and $0, 1$ are constants. The equational theory E consists of the single equation

$$\mathsf{dec}(\mathsf{enc}(x, y), y) = x$$

and intuitively models symmetric encryption. Let

$$\phi_1 = \nu k.\{x_1 \mapsto \mathsf{enc}(0, k), x_2 \mapsto k\} \text{ and } \phi_2 = \nu k.\{x_1 \mapsto \mathsf{enc}(1, k), x_2 \mapsto k\}$$

We have that $\phi_1 \not\approx_E \phi_2$ because $(\mathsf{dec}(x_1, x_2) =_E 0)\phi_1$ and $(\mathsf{dec}(x_1, x_2) \neq_E 0)\phi_2$. Let

$$\psi_1 = \nu s, k.\{x_1 \mapsto \mathsf{enc}(s, k), x_2 \mapsto k\} \text{ and } \psi_2 = \nu s, k, k'.\{x_1 \mapsto \mathsf{enc}(s, k), x_2 \mapsto k'\}$$

Again we have that $\psi_1 \not\approx_E \psi_2$ because the test $(\mathsf{enc}(\mathsf{dec}(x_1, x_2), x_2) =_E x_1)$ holds in ψ_1 but not in ψ_2. However, if we take the equational theory E' defined by

$$E' = E \cup \{\mathsf{enc}(\mathsf{dec}(x, y), y) = x\}$$

we obtain that $\psi_1 \approx_{E'} \psi_2$.

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 definition in a cryptographic setting can be found in [8]. In general, a pairing operation maps elements of an additive group to elements of a multiplicative group in the following way.

$$\begin{aligned} e: \quad & \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2 \\ & e(ag_1, bg_2) = e(g_1, g_2)^{ab} \end{aligned}$$

In some protocols, e.g. [15], 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 $\mathcal{S}_{\mathsf{BP}}$ 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 $\mathcal{F}_{\mathsf{BP}}$ be the following set of symbols:

$+, \cdot : R \times R \to R$		addition, multiplication of exponents
$- : R \to R$		inverse of exponents
$0_R, 1_R : R$		constant exponents
$exp_i : R \to G_i$	$i \in \{1, 2\}$	exponentiation
$*_i : G_i \times G_i \to G_i$	$i \in \{1, 2\}$	multiplication in $\mathbb{G}_i$
$e : G_1 \times G_1 \to G_2$		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 $t * \ldots * t$ (i times). The properties of these function symbols are defined by the following equational theory E_{BP}.

$$\begin{aligned} x + y &= y + x & 0_R + x &= x \\ (x + y) + z &= x + (y + z) & x + (-x) &= 0_R \\ x \cdot y &= y \cdot x & x \cdot (y + z) &= (x \cdot y) + (x \cdot z) \\ (x \cdot y) \cdot z &= x \cdot (y \cdot z) & 1_R \cdot x &= x \end{aligned}$$

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

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 2 Bilinear pairing is a central primitive of the Joux protocol [15], 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:

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

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, a valve f is a symbol that allows to go into one direction, but such that there is no way to go back. More exactly, a valve f takes arguments of sorts $s_1, \ldots, s_k$, and yields a result of sort s, such that no term of sort s_i has a subterm of sort s.

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 $V = \mathcal{S}$ and $E \subseteq V \times V \times \mathcal{F}$. We write $r \xrightarrow{f} s$ for $(r, s, f) \in E$ and require that $\mathsf{sort}(f) = s_1 \times \ldots \times s_k \to s$ 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 $r \xrightarrow{f} s$ and $r' \xrightarrow{f'} s'$ we have $s = r'$. When S_1 and S_2 are sets of vertices we say that there exists a path from S_1 to S_2 iff there exist $s_1 \in S_1$, $s_2 \in S_2$ such that there is a path from s_1 to s_2.

Definition 4 (valve) A symbol f of arity $s_1 \times \ldots \times s_k \to s$ is a *valve* iff

1. for every path π from $\{s_1, \ldots, s_k\}$ to $\{s\}$ in $\mathcal{G}(\mathcal{S}, \mathcal{F})$ there is a j, $1 \leq j \leq k$, such that π contains $s_j \xrightarrow{f} s$;
2. and there is no path from $\{s\}$ to $\{s_1, \ldots, s_k\}$.

In other words, f is a valve iff every path from $\{s_1, \ldots, s_k\}$ to $\{s\}$ contains exactly one f. When f of arity $s_1 \times \ldots \times s_k \to s$ is a valve, we also say that f is a valve from $\{s_1, \ldots, s_k\}$ to s.

Example 3 Let us consider the sorted signature $(\mathcal{S}_{\mathsf{BP}}, \mathcal{F}_{\mathsf{BP}})$ introduced in our running example in Section 3. The signature graph $\mathcal{G}(\mathcal{S}_{\mathsf{BP}}, \mathcal{F}_{\mathsf{BP}})$ is given in Figure 1. The symbol e is a valve from $\{G_1\}$ to $\{G_2\}$ as $G_1 \xrightarrow{e} G_2$ lies on every path from $\{G_1\}$ to $\{G_2\}$, 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 $R \xrightarrow{exp_1} G_1, G_1 \xrightarrow{e} G_2$ is a path from $\{R\}$ to $\{G_2\}$ not involving exp_2.

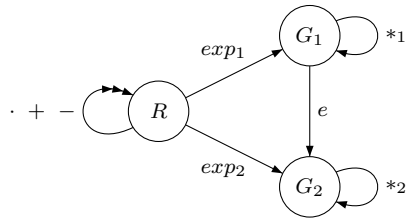

Fig. 1 The signature graph $\mathcal{G}(\mathcal{S}_{\mathsf{BP}}, \mathcal{F}_{\mathsf{BP}})$.

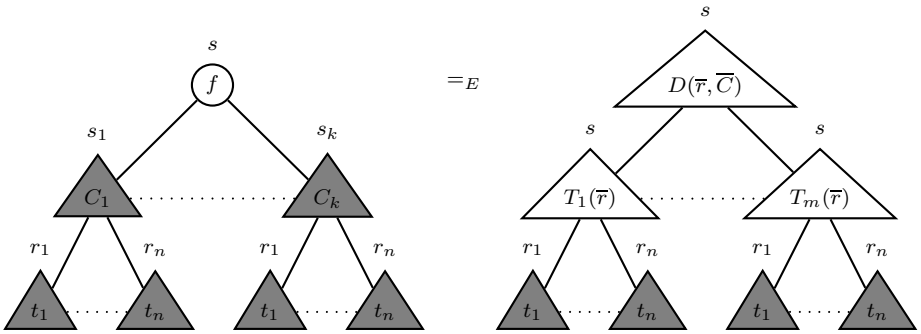

Fig. 2 Reducibility. Grey objects are of sort $s_1, \ldots, s_n$, while clear objects are of sort s. The choice of the T_i only depends on the sorts $\overline{r} = r_1, \ldots, r_n$, while the choice of D depends both on the contexts $\overline{C} = C_1, \ldots, C_k$ and the sorts $\overline{r}$.

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

Definition 5 (reducible) Let f be a valve of arity $s_1 \times \ldots \times s_k \to s$. An equational theory E is *reducible* for f iff for every $n \geq 0$ and sorts $r_1, \ldots, r_n \in \{s_1, \ldots, s_k\}$ there exist m public contexts $T_1[x_1, \ldots, x_n], \ldots, T_m[x_1, \ldots, x_n]$ of arity $r_1 \times \ldots \times r_n \to s$ such that for all k public contexts $C_i[x_1, \ldots, x_n]$ of arity $r_1 \times \cdots \times r_n \to s_i$ with $1 \leq i \leq k$ there exists a public context $D[y_1, \ldots, y_m]$ of arity $s \times \cdots \times s \to s$ such that for any ground terms $t_1, \ldots, t_n$ of sort $r_1, \ldots, r_n$ respectively we have that

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

Intuitively, reducibility for a valve f means that given a vector $(r_1, \ldots, r_n)$ of sorts that are all argument sorts of f, there are finitely many maps T_i from $r_1 \times \ldots \times r_n$ to s such that any computation of the form $f(C_1, \ldots, C_k)$ can be simulated by some D entirely inside the sort s by making use of the maps T_i. The crucial point is that the contexts T_i depend only on the sorts $r_1, \ldots, r_n$ but *not* on the contexts C_i. A pictorial view of this definition is given in Figure 2. We illustrate this notion by showing in Proposition 2 the reducibility for e of the theory of our running example E_{BP} in case $\mathcal{N}_{G_1} = \emptyset$.

Proposition 1 *Let f be a valve from $s_1, \ldots, s_k$ to s, and E an equational theory. If for any $r_1, \ldots, r_n \in \{s_1, \ldots, s_k\}$ and for any i $(1 \leq i \leq k)$ the set of public contexts $C_i[x_1, \ldots, x_n]$ of arity $r_1 \times \ldots \times r_n \to s_i$ is finite then E is reducible for f.*

Proof Let $r_1, \ldots, r_n \in \{s_1, \ldots, s_k\}$, and let n_i be the number of public contexts $C_i[x_1, \ldots, x_n]$ of arity $r_1 \times \ldots \times r_n \to s_i$. We define $m = n_1 * \cdots * n_k$ contexts T of arity $r_1 \times \ldots \times r_n \to s$ as follows, where $1 \leq i_j \leq n_i$ for $1 \leq j \leq k$:

$$T_{i_1,\ldots i_k}[x_1, \ldots, x_n] = f(C_{i_1}, \ldots, C_{i_k})[x_1, \ldots, x_n]$$

Consider k public contexts $C_{j_1}[x_1, \ldots, x_n]$, $\ldots$, $C_{j_k}[x_1, \ldots, x_n]$. We define the context D as follows:

$$\lambda y_{1,\ldots,1}. \ldots . \lambda y_{n_C,\ldots,n_C}. y_{j_1,\ldots,j_n}$$

Obviously we have that for all ground terms $t_1, \ldots, t_n$ of sort r that

$$f(C_{j_1}, \ldots, C_{j_k})[t_1, \ldots, t_n] =_E D[T_{1,\ldots,1}, \ldots, T_{n_C,\ldots n_C}][t_1, \ldots, t_n]$$

□

Proposition 2 *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

$$\begin{array}{ll} T_i = \lambda x_1. \ldots . \lambda x_n. e(x_i, exp_1(1_R)) & \text{for } 1 \leq i \leq n \\ T_{ij} = \lambda x_1. \ldots . \lambda x_n. e(x_i, x_j) & \text{for } 1 \leq i \leq j \leq n \end{array}$$

Every public context $C_i[x_1, \ldots, x_n]$ of arity $G_1 \times \cdots \times G_1 \to G_1$ is of the form $\lambda x_1. \ldots . \lambda x_n. x_1^{e_{i1}} * \cdots * x_n^{e_{in}} * exp_1(p_i)$ where $p_i =_{E_{\mathsf{BP}}} 1_R + \cdots + 1_R$ (l_i times). Hence $exp_1(p_i) =_{E_{\mathsf{BP}}} exp_1(1_R)^{l_i}$.

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 $t_1, \ldots, t_n$

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

Base case. We distinguish four cases:

1. $C_1 = \lambda x_1. \ldots . \lambda x_n. x_i$ and $C_2 = \lambda x_1. \ldots . \lambda x_n. x_j$
   For any sequence of terms $t_1, \ldots, t_n$ we have that
   $$e(C_1, C_2)[t_1, \ldots, t_n] = e(t_i, t_j)$$
   Let $D = \lambda y_1. \ldots . \lambda y_n. \lambda y_{11}. \ldots . \lambda y_{nn}. y_{ij}$. We have that $e(C_i, C_j)[t_1, \ldots, t_n] =_{E_{\mathsf{BP}}} D[T_1, \ldots, T_n, T_{11}, \ldots, T_{nn}][t_1, \ldots, t_n]$.
2. $C_1 = \lambda x_1. \ldots . \lambda x_n. x_i$ and $C_2 = exp_1(1_R)^l$
   For any sequence of terms $t_1, \ldots, t_n$ we have that
   $$e(C_1, C_2)[t_1, \ldots, t_n] = e(t_i, exp(1_R)^l)$$
   Let $D = \lambda y_1. \ldots . \lambda y_n. \lambda y_{11}. \ldots . \lambda y_{nn}. y_i^l$. We have that $e(C_i, C_j)[t_1, \ldots, t_n] =_{E_{\mathsf{BP}}} D[T_1, \ldots, T_n, T_{11}, \ldots, T_{nn}][t_1, \ldots, t_n]$.
3. $C_1 = exp_1(1_R)^l$ and $C_2 = \lambda x_1. \ldots . \lambda x_n. x_i$
   As $C_1 * C_2 =_{E_{\mathsf{BP}}} C_2 * C_1$ this case is similar to case 2.
4. $C_1 = exp_1(1_R)^{l_1}$ and $C_2 = exp_1(1_R)^{l_2}$
   We immediately conclude by defining
   $$D = \lambda y_1. \ldots . \lambda y_n. \lambda y_{11}. \ldots . \lambda y_{nn}. exp_2(1_R)^{l_1 \cdot l_2}$$

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 $C_{11}[x_1, \ldots, x_n]$, $C_{12}[x_1, \ldots, x_n]$, $C_2[x_1, \ldots, x_n]$, for any terms $t_1, \ldots t_n$ we have that $C_{11}[t_1, \ldots t_n] = exp_1(p_{11})$, $C_{12}[t_1, \ldots t_n] = exp_1(p_{12})$ and $C_2[t_1, \ldots t_n] = exp_1(p_2)$, 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

$$e(C_{11} * C_2)[t_1, \ldots, t_n] =_E D_1[T_1, \ldots, T_m][t_1, \ldots, t_n]$$
$$e(C_{12} * C_2)[t_1, \ldots, t_n] =_E D_2[T_1, \ldots, T_m][t_1, \ldots, t_n]$$

We conclude by defining D as $D_1 * D_2$. □

Example 4 For $n = 2$ we have that

$$T_1 = e(x_1, exp_1(1)) \qquad T_2 = e(x_2, exp_1(1))$$
$$T_{1,1} = e(x_1, x_1) \quad T_{1,2} = e(x_1, x_2) \quad T_{2,2} = e(x_2, x_2)$$

Let $C_1 = \lambda x_1 \lambda x_2 . x_1$ and $C_2 = \lambda x_1 \lambda x_2 . x_2 * x_2 * exp_1(1 + 1)$. 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 $e(t_1, t_2 * t_2 * exp_1(1 + 1)) = e(t_1, t_2) * e(t_1, t_2) * e(t_1, exp_1(1)) * e(t_1, exp_1(1))$ for any *ground* terms t_1, t_2.

Remark 1 Proposition 2 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 $exp_1(r)$ 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 [11].

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 $\mathsf{arity}(f) = r \to s$, and $E = \emptyset$. We show that E is reducible for f but not sufficiently complete w.r.t. f.

For any $n \geq 0$ there exist only finitely many public contexts $C_i[x_1, \ldots, x_n]$ of arity $r \times \ldots \times r \to r$, namely the n different contexts of the form $\lambda x_1 \ldots \lambda x_n . x_i$. Hence, E is reducible for f by Proposition 1.

To show that E is not sufficiently complete w.r.t. f we note that f is free in E. Hence, for any name n of sort r the term $f(n)$ is not equivalent to some term without f. □

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 function and constant symbols like this:

$$\begin{array}{lll} 0_r : r & & 0_s : s \\ s_r : r \to r & f : r \times r \to s & s_s : s \to s \end{array}$$

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

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

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 w.r.t. f since there are no names of sort r. Now let us assume that E is reducible for f. We choose $n = 1$. According to Definition 5 there exist contexts $T_1[x], \ldots, T_m[x]$ of arity $r \to s$ such that for all contexts $C_1[x], C_2[x]$ of arity $r \to r$ there exists a context $D[y_1, \ldots, y_m]$ of arity $s \times \ldots \times s \to s$ such that for all ground terms t of sort r:

$$LHS = f(C_1[t], C_2[t]) = D[T_1[t], \ldots, T_m[t]] = RHS \tag{1}$$

Due to our choice of the signature the following holds where we write $x/0_r$ for any of the terms x or 0_r:

- Any context $C[x]$ of arity $r \to r$ is of the form $s_r^c(x/0_r)$ for some constant c. According to our notation we write this as $c + x$, resp. c.
- Any context $T_i[x]$ of arity $r \to s$ is of the form $s_s^{n_i}(f(s_r^{m_i}(x/0_r), s_r^{k_i}(x/0_r)))$.
- Any context $D[y_1, \ldots, y_m]$ of arity $s \times \ldots \times s \to s$ is of the form $\lambda y_1, \ldots, y_m.s_s^d(y_i)$, which we now write as $d + y_i$, or of the form $\lambda y_1, \ldots, y_m.s_s^d(0)$, which we simply write as d.

Assume given the contexts $T_i[x] = s_s^{n_i}(f(s_r^{m_i}(x/0_r), s_r^{k_i}(x/0_r)))$. We choose $C_1[x] = x$, and $C_2[x] = s_r^c(x)$ for some $c > k_i + 1$ for all $1 \leq i \leq m$. The left-hand side of Equation (1) evaluates to

$$\begin{aligned} LHS &= f(C_1[t], C_2[t]) \\ &= f(t, c + t) \\ &= t + \frac{(c + t) * (c + t + 1)}{2} \\ &= \frac{c^2}{2} + \frac{t^2}{2} + ct + \frac{c}{2} + \frac{3}{2}t \end{aligned}$$

If the context $D[y_1, \ldots, y_m]$ is d for some constant d then Equation (1) reduces to

$$\frac{c^2}{2} + \frac{t^2}{2} + ct + \frac{c}{2} + \frac{3}{2}t = d$$

which clearly cannot hold for all values t. If the context $D[y_1, \ldots, y_m]$ is of the form $\lambda y_1, \ldots, y_m.s_s^d(y_i)$ then we obtain for the right-hand side of Equation (1)

$$\begin{aligned} RHS &= D[T_1[t], \ldots, T_m[t]] \\ &= d + T_i[t] \\ &\leq d + n_i + f(m_i + t, k_i + t) \\ &= d + n_i + m_i + t + \frac{(k_i + t) * (k_i + t + 1)}{2} \\ &= d + n_i + m_i + \frac{k_i^2}{2} + \frac{t^2}{2} + k_i t + \frac{k_i}{2} + \frac{3}{2}t \end{aligned}$$

We choose $t > d + n_i + m_i$ and obtain, since $c > k_i + 1$:

$$\begin{aligned} LHS &= \frac{c^2}{2} + \frac{t^2}{2} + ct + \frac{c}{2} + \frac{3}{2}t \\ &> \frac{k_i^2}{2} + \frac{t^2}{2} + (k_i t + t) + \frac{k_i}{2} + \frac{3}{2}t \\ &> \frac{k_i^2}{2} + \frac{t^2}{2} + k_i t + (d + n_i + m_i) + \frac{k_i}{2} + \frac{3}{2}t \\ &\geq RHS \end{aligned}$$

which is in contradiction to Equation (1). □

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. In the remainder of this paper we only consider signatures $(\mathcal{S}, \mathcal{F})$ where $f \in \mathcal{F}$ is a valve from $\{s_1, \ldots, s_n\}$ to s such that in $\mathcal{G}(\mathcal{S}, \mathcal{F})$ the only sorts accessible from $\{s_1, \ldots, s_n\}$ are $\{s_1, \ldots, s_n, s\}$. Consequently, the only sort accessible from s is s. This is sufficient to cover our running example and simplifies the proofs and the presentation of our results. Furthermore we will denote by $A = \{s_1, \ldots, s_n\}$ the set of argument sorts of the valve symbol. We will also write $\{A, s\}$ for the set $A \cup \{s\}$.

The valve symbol f may occur at three different places:

1. in the frames,
2. in the "observations", that is the terms M and N,
3. and in the equational theory E.

We hence proceed in three stages: First, in Subsection 5.1, we show that deciding static equivalence on $\{A, s\}$-sorted frames in the presence of a valve from A to s can be reduced to deciding two equivalences, one on A-sorted frames and one on $\{s\}$-sorted frames (Lemma 4). Then, in Subsection 5.2, we show that we may suppose that M and N are of sort A. Finally, we conclude in Subsection 5.3 that one may even assume that f is eliminated from the equational theory (Theorem 1). For this last step we will require an additional property of the equational theory. As a corollary we get the possibility of splitting the equational theory into simpler equational theories.

5.1 Splitting frames along valves

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

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

Definition 8 (restriction of a frame) Let $\phi = \nu\tilde{n}.\sigma_\phi$ be a frame, and $B \subseteq \mathcal{S}$ a set of sort symbols. The *B-restriction* of ϕ, denoted $\phi_{|B}$ is the frame $\nu\tilde{n}.\sigma_{\phi_{|B}}$ where $\sigma_{\phi_{|B}}$ is the substitution σ_ϕ restricted to the variables whose sort is in B.

We write shortly $\phi_{|s}$ for $\phi_{|\{s\}}$ for a single sort symbol $s \in \mathcal{S}$.

Example 5 Let ϕ_{BDH} be the G_1-restriction of the frames presented in Example 2: $\phi_{BDH} = \nu a, b, c, r.\{x_1 \mapsto exp_1(a), x_2 \mapsto exp_1(b), x_3 \mapsto exp_1(c)\}$. Using the set of terms T_i and T_{ij} defined in the proof of Proposition 2, we get

$$\begin{aligned}\overline{\phi}_{BDH} = \nu a, b, c, r.\{\ & y_1 \mapsto e(exp_1(a), exp_1(1)),\ \ y_2 \mapsto e(exp_1(b), exp_1(1)),\\ & y_3 \mapsto e(exp_1(c), exp_1(1)),\ \ y_{11} \mapsto e(exp_1(a), exp_1(a)),\\ & y_{12} \mapsto e(exp_1(a), exp_1(b)),\ y_{13} \mapsto e(exp_1(a), exp_1(c)),\\ & y_{22} \mapsto e(exp_1(b), exp_1(b)),\ y_{23} \mapsto e(exp_1(b), exp_1(c)),\\ & y_{33} \mapsto e(exp_1(c), exp_1(c)) \qquad\qquad \}\end{aligned}$$

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 A 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 $\{A, s\}$-sorted frame ϕ of size n, $M\phi =_E M'\overline{\phi_{|A}}\phi_{|s}$.*

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

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

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

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

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

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

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

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

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

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

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

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

Let us suppose that $\phi_1 \not\approx_E \phi_2$. Hence there exist two terms $M[\overrightarrow{x}, \overrightarrow{y}]$ and $N[\overrightarrow{x}, \overrightarrow{y}]$ 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 $\mathsf{sort}(M) \in A$, as the only sort transition possibility is directed from A to s (by the second item of the lemma), all variables of M are of sort A. Hence, M and N distinguish $\phi_{1|A}$ and $\phi_{2|A}$.

If $\mathsf{sort}(M) = s$, as $\mathrm{dom}(\phi_{1|A}) = \mathrm{dom}(\phi_{2|A})$ by Lemma 3 there exists terms M' and N' such that $M\phi_i =_E M'\overline{\phi_{i|A}}\phi_{i|s}$ and $N\phi_i =_E N'\overline{\phi_{i|A}}\phi_{i|s}$, 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, $(M =_E N)\overline{\phi_{1|A}}\phi_{1|s}$ and $(M \neq_E N)\overline{\phi_{2|A}}\phi_{2|s}$. □

5.2 Getting rid of the valve in obervations

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.

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

Before proving this lemma we will

- introduce some useful notations borrowed from [7],
- recall Lemma 6 from [7],
- state and prove Lemma 7.

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

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

Thus, the effect of the function $\mathsf{cut}_{u,a}(t)$ is to substitute in a top down way subterms of t equal to u modulo E with a. In the case where f is a valve, the effect of $\mathsf{cut}_{u,a}(t)$ is to substitute every subterm of t equal to u modulo E with a.

Lemma 6 ([7]) *Let E be an equational theory where f is free. Let $u = f(u_1, \ldots, u_n)$ 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,*

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

Lemma 7 *Let ϕ_1 and ϕ_2 be two A-sorted frames, f a valve from A to s and E an equational theory where f is free. If for any two terms M' and N' of some sort in A we have that $M'\phi_1 =_E N'\phi_1$ iff $M'\phi_2 =_E N'\phi_2$, then for any two terms M and N of sort s headed by f, $M\phi_1 =_E N\phi_1$ iff $M\phi_2 =_E N\phi_2$.*

Proof Let $M = f(C_1^M, \ldots, C_k^M)$ and $N = f(C_1^N, \ldots, C_k^N)$. 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 some sort in A we have that $(M' =_E N')\phi_1$ 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 $M\phi_2 =_E N\phi_2$. □

We are now able to give the proof of Lemma 5.

Proof The proof will be done in 3 steps:

1. We first define two replacement 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).
2. Given that for all terms M, N of some sort in A we have that $M\phi_1 =_E N\phi_1$ iff $M\phi_2 =_E N\phi_2$ we show that $M\phi_1\sigma_1 =_E N\phi_1\sigma_1$ iff $M\phi_2\sigma_2 =_E N\phi_2\sigma_2$. More precisely we show that $M\phi_1\sigma_1 =_E M\phi_2\sigma_2$ and $N\phi_1\sigma_1 =_E N\phi_2\sigma_2$ which direclty implies the previous statement.
3. Then 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 6 and the fact that σ_1 and σ_2 are bijective.

The conjunction of the assertions of step 2 and 3 implies that for any two terms M, N of sort s, $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$.

Step 1. 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 $f(C_1,\ldots,C_k)$ by a same fresh name $a_{\alpha,\beta}$. Here α,β identifies the first occurence of $f(C_1,\ldots,C_k)$ 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 be 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 $C_{\mathcal{M}}[f(C^1_{\mathcal{M}1},\ldots,C^1_{\mathcal{M}k}),\ldots,f(C^m_{\mathcal{M}1},\ldots,C^m_{\mathcal{M}k})]$ (resp. $C_{\mathcal{N}}[f(C^1_{\mathcal{N}1},\ldots,C^1_{\mathcal{N}k}),\ldots,f(C^l_{\mathcal{N}1},\ldots,C^l_{\mathcal{N}k})]$) where all variables of M (resp. N) are in the $f(C^i_{\mathcal{M}1},\ldots,C^i_{\mathcal{M}k})$ (resp. $f(C^i_{\mathcal{N}1},\ldots,C^i_{\mathcal{N}k})$) and contexts $C_{\mathcal{M}}, C_{\mathcal{N}}, C^i_{\mathcal{M}j}, C^i_{\mathcal{N}j}$ do not contain f. We then have that

$$M\phi_i = C_{\mathcal{M}}[f(C^1_{\mathcal{M}1},\ldots,C^1_{\mathcal{M}k})\phi_i,\ldots,f(C^m_{\mathcal{M}1},\ldots,C^m_{\mathcal{M}k})\phi_i]$$
$$N\phi_i = C_{\mathcal{N}}[f(C^1_{\mathcal{N}1},\ldots,C^1_{\mathcal{N}k})\phi_i,\ldots,f(C^l_{\mathcal{N}1},\ldots,C^l_{\mathcal{N}k})\phi_i]$$

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 We have that for each position $p \in Pos(M)_{|f}$ there exists i such that $M\phi_1|_p = f(C^i_{\mathcal{M}1},\ldots,C^i_{\mathcal{M}k})\phi_1$ and $M\phi_2|_p = f(C^i_{\mathcal{M}1},\ldots,C^i_{\mathcal{M}k})\phi_2$ and for each position $p \in Pos(M)_{|f}$ there exists i such that $N\phi_1|_p = f(C^i_{\mathcal{N}1},\ldots,C^i_{\mathcal{N}k})\phi_1$ and $N\phi_2|_p = f(C^i_{\mathcal{N}1},\ldots,C^i_{\mathcal{M}k})\phi_2$.

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 $(\alpha,p) \in \mathrm{dom}(\sigma_i)$ and (α',p') be the minimal element such that $\tau(\alpha')\phi_i|_{p'} =_E \tau(\alpha)\phi_i|_p$. Then we have that $\sigma_i((\alpha,p)) = a_{\alpha',p'}$.

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

Step 2. We now show that for any prefix p of an element of $Pos(\tau(\alpha))_{|f}$ we have that $\tau(\alpha)_{|p}\phi_1\sigma_1 = \tau(\alpha)_{|p}\phi_2\sigma_2$. In the particular case where $p = \Lambda$ we immediately have that $\tau(\alpha)\phi_1\sigma_1 = \tau(\alpha)\phi_2\sigma_2$. We show this by a decreasing induction on the length of p.

Base case : p is maximal. As in this case $p \in Pos(\tau(\alpha))_{|f}$, we have that $C_{\alpha|p}$ is a variable. Let (α',p') be the minimal pair such that $\tau(\alpha')\phi_{1|p'} =_E \tau(\alpha)\phi_{1|p}$. Then, by definition of σ_1 we have that $\tau(\alpha)_{|p}\phi_1\sigma_1 = a_{\alpha',p'}$.

By remark 3, there exist i,i' such that $\tau(\alpha)\phi_{1|p} = f(C^i_{\alpha 1},...,C^i_{\alpha k})\phi_1$, $\tau(\alpha)\phi_{2|p} = f(C^i_{\alpha 1},...,C^i_{\alpha k})\phi_2$, $\tau(\alpha')\phi_{1|p'} = f(C^{i'}_{\alpha' 1},...,C^{i'}_{\alpha' k})\phi_1$ and $\tau(\alpha')\phi_{2|p'} = f(C^{i'}_{\alpha' 1},...,C^{i'}_{\alpha' k})\phi_2$.

By Lemma 7, as $\tau(\alpha')\phi_{1|p'} =_E \tau(\alpha)\phi_{1|p}$, we have that $\tau(\alpha')\phi_{2|p'} =_E \tau(\alpha)\phi_{2|p}$.

Suppose there exists a pair $(\alpha'',p'') < (\alpha',p')$ such that $\tau(\alpha'')\phi_{2|p''} =_E \tau(\alpha)\phi_{2|p}$. By a similar reasoning as above he have that $\tau(\alpha'')\phi_{1|p''} =_E \tau(\alpha)\phi_{1|p}$ contradicting the fact that (α',p') is the minimal pair such that $\tau(\alpha')\phi_{1|p'} =_E \tau(\alpha)\phi_{1|p}$. Hence, $\tau(\alpha)_{|p}\phi_2\sigma_2 = a_{\alpha',p'}$ and $\tau(\alpha)_{|p}\phi_1\sigma_1 = \tau(\alpha)_{|p}\phi_2\sigma_2$.

Inductive case. We suppose that the property holds for all positions $p_1, \ldots, p_n \in Pos(\tau(\alpha))_{|f}$ of which p is a prefix. It is immediate that the property also holds for p.

Step 3. We show by induction on the number of names in the co-domain of σ_i that there is a sequence $\mathsf{cut}_{u_1,a_1}, \ldots, \mathsf{cut}_{u_n.a_n}$ with $M\phi_i\sigma_i = \mathsf{cut}_{u_n,a_n}(\ldots(\mathsf{cut}_{u_1.a_1}(M\phi_i))\ldots)$ and $N\phi_i\sigma_i = \mathsf{cut}_{u_n,a_n}(\ldots(\mathsf{cut}_{u_1.a_1}(N\phi_i))\ldots)$.

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 $\mathsf{cut}_{u_1,a_1}, \ldots, \mathsf{cut}_{u_n.a_n}$ such that $M\phi_i\sigma_i \setminus a_{\alpha,p} = \mathsf{cut}_{u_n,a_n}(\ldots(\mathsf{cut}_{u_1.a_1}(M\phi_i))\ldots)$ and $N\phi_i\sigma_i \setminus a_{\alpha,p} = \mathsf{cut}_{u_n,a_n}(\ldots(\mathsf{cut}_{u_1.a_1}(N\phi_i))\ldots)$. By definition of σ_i if there are several pairs $(\alpha_1, p_1), \ldots, (\alpha_n, p_n)$ mapped to $a_{\alpha,p}$, it means that $\tau(\alpha_1)\phi_i|_{p_1} = \cdots = \tau(\alpha_n)\phi_i|_{p_n} = \tau(\alpha_1)\phi_i|_p$ and we also have that $\tau(\alpha_1)\phi_i|_{p_1}$ is headed by f by definition of σ_i. Hence applying $\sigma_i|_{\alpha,p}$ is identical to applying $cut_{\tau(\alpha)\phi_i|_p, a_{\alpha,p}}$. As $M\phi_i\sigma_i = M\phi_i\sigma_i \setminus a_{\alpha,p}\sigma_i|_{\alpha,p}$. As $M\phi\sigma_i \setminus a_{\alpha,p} = \mathsf{cut}_{u_n,a_n}(\ldots(\mathsf{cut}_{u_1.a_1}(M\phi_i))\ldots)$, we have that $M\phi_i\sigma_i = \mathsf{cut}_{\tau(\alpha)\phi_i|_p, a_{\alpha,p}}(\mathsf{cut}_{u_n,a_n}(\ldots(\mathsf{cut}_{u_1.a_1}(M\phi_i))\ldots))$. We do the same for N.

By iterating Lemma 6 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 $M\phi_2 =_E N\phi_2$. □

5.3 Getting completely rid of the valve

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 from A to s,*
- *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 $\{A, s\}$-sorted frames ϕ_1 and ϕ_2, we have that $\phi_1 \approx_E \phi_2$ iff $\phi_{1|A} \approx_{E'} \phi_{2|A}$ and $\overline{\phi_{1|A}}\phi_{1|s} \approx_{E'} \overline{\phi_{2|A}}\phi_{2|s}$.

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

We will show that

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

We will prove the three following assertions separately :

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

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

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

(2) if $\phi_{1|A} \not\approx_E \phi_{2|A}$ then $\phi_{1|A} \not\approx_{E'} \phi_{2|A}$ or $\overline{\phi_{1|A}}\phi_{1|s} \not\approx_{E'} \overline{\phi_{2|A}}\phi_{2|s}$
Let M and N be two terms distinguishing $\phi_{1|A}$ and $\phi_{2|A}$.
If M is of some sort in A, as f is a valve, we can suppose w.l.o.g. that M, N, $\phi_{1|A}$ and $\phi_{2|A}$ do not involve any f. Hence $M\phi_{i|A}$ and $N\phi_{i|A}$ do not involve f. As E' is sufficient for E without f we have that $M\phi_{i|A} =_E N\phi_{i|A}$ iff $M\phi_{i|A} =_{E'} N\phi_{i|A}$. Hence $\phi_{1|A} \not\approx_{E'} \phi_{2|A}$.
If M is of sort s, by Lemma 3 there exist terms M' and N' such that $M\phi_{i|A} =_E M'\overline{\phi_{i|A}}$ and $N\phi_{i|A} =_E N'\overline{\phi_{i|A}}$. As f is a valve and E is sufficiently complete w.r.t. f, M' and N' do not involve any symbol f. By sufficient completeness of E w.r.t. $\{f\}$, we can consider frames $\overline{\phi_{1|A}}$ and $\overline{\phi_{2|A}}$ that do not involve f, $M'\overline{\phi_{i|A}}$ and $N'\overline{\phi_{i|A}}$ do not involve f either. As E' is sufficient without f we have that $M'\overline{\phi_{i|A}} =_E N'\overline{\phi_{i|A}}$ iff $M'\overline{\phi_{i|A}} =_{E'} N'\overline{\phi_{i|A}}$. Hence $\overline{\phi_{1|A}} \not\approx_{E'} \overline{\phi_{2|A}}$ and $\overline{\phi_{1|A}}\phi_{1|s} \not\approx_{E'} \overline{\phi_{2|A}}\phi_{2|s}$.

(3) if $\phi_{1|A} \not\approx_{E'} \phi_{2|A}$ then $\phi_{1|A} \not\approx_E \phi_{2|A}$
As $\phi_{1|A} \not\approx_{E'} \phi_{2|A}$ there exist terms M and N distinguishing $\phi_{1|A}$ and $\phi_{2|A}$.
If there are no terms M and N of some sort in A distinguishing $\phi_{1|A}$ and $\phi_{2|A}$, by Lemma 5 there are no terms of sort s distinguishing $\phi_{1|A}$ and $\phi_{2|A}$. Hence if $\phi_{1|A} \not\approx_{E'} \phi_{2|A}$ then there are terms M and N distinguishing $\phi_{1|A}$ and $\phi_{2|A}$ of some sort in A.
If M is of some sort in A, as f is a valve, M, N, $\phi_{1|A}$ and $\phi_{2|A}$ do not involve any f. Hence $M\phi_{i|A}$ and $N\phi_{i|A}$ do not involve f. As E' is sufficient without f we have that $M\phi_{i|A} =_{E'} N\phi_{i|A}$ iff $M\phi_{i|A} =_E N\phi_{i|A}$. Hence $\phi_{1|A} \not\approx_E \phi_{2|A}$. □

Remark 4 Let us notice that, by item (1) of the proof of Theorem 1 in case $\overline{\phi_{1|A}}\phi_{1|s} \not\approx_E \overline{\phi_{2|A}}\phi_{2|s}$, and if we do the same assumptions on equational theories and signatures as in Theorem 1, we obtain that if $\overline{\phi_{1|A}}\phi_{1|s} \not\approx_{E'} \overline{\phi_{2|A}}\phi_{2|s}$, then it is distinguishable by contexts M and N where M and N do not involve f.

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

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 $\{A, s\}$-sorted frames ϕ_1 and ϕ_2, we have that $\phi_1 \approx_E \phi_2$ iff $\phi_{1|A} \approx_{E'^{-s}} \phi_{2|A}$ and $\overline{\phi_{1|A}}\phi_{1|s} \approx_{E'^{-A}} \overline{\phi_{2|A}}\phi_{2|s}$.*

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

By Lemma 5, we have that if for any two terms M and N of some sort in A $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$, then for any two terms M and N of sort s, $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$. Hence it is sufficient to consider terms of sorts in A to decide static equivalence between $\phi_{1|A}$ and $\phi_{2|A}$. As f is a valve, for any term M no subterms of M are of sort s. We can consider only E'^{-s} to decide static equivalence between $\phi_{1|A}$ and $\phi_{2|A}$.

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

$\overline{\phi_{1|A}}\phi_{1|s} \not\approx_{E'} \overline{\phi_{2|A}}\phi_{2|s}$ iff there are two terms M and N distinguishing $\overline{\phi_{1|A}}\phi_{1|s}$ and $\overline{\phi_{2|A}}\phi_{2|s}$. By Remark 4, 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 $\overline{\phi_{1|A}}\phi_{1|s}$ and $\overline{\phi_{2|A}}\phi_{2|s}$ do not involve f. Hence $M\overline{\phi_{i|A}}\phi_{i|s}$ and $N\overline{\phi_{i|A}}\phi_{i|s}$ do not involve f either. As f is a valve we have that $M\overline{\phi_{i|A}}\phi_{i|s}$ and $N\overline{\phi_{i|A}}\phi_{i|s}$ do not involve subterms of any sort in A. So we have that $M\overline{\phi_{i|A}}\phi_{i|s} =_{E'} N'\overline{\phi_{i|A}}\phi_{i|s}$ iff $M\overline{\phi_{i|A}}\phi_{i|s} =_{E'^{-A}} N\overline{\phi_{i|A}}\phi_{i|s}$. Hence $\overline{\phi_{1|A}}\phi_{1|s} \not\approx_{E'^{-A}} \overline{\phi_{2|A}}\phi_{2|s}$. □

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 $l \to r \in \mathcal{R}$, f appears in l.

Lemma 8 *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 $u =_{E'} v$. □

Example 6 (continued) We define $\mathcal{R}_{\mathsf{BP}}$ to be the rewriting system obtained by orienting the rule $e(exp_1(x), exp_1(y)) = exp_2(x \cdot y)$ from left to right, and E'_{BP} the equational theory E_{BP} without this rule. We remark that $(\mathcal{R}, E'_{\mathsf{BP}})$ is a decomposition of E_{BP} and it is easy to see that $\mathcal{R}$ exclusively defines e.

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

Proof As $\mathcal{R}_{\mathsf{BP}}$ exclusively defines e, by Lemma 8, we have that E'_{BP} is sufficient for E_{BP} without e. By Proposition 2 we have that E_{BP} is reducible for f. Finally, as the sets of names of sorts G_1 and G_2 is empty, E_{BP} is sufficiently complete w.r.t. e. Hence by Corollary 1, for two frames ϕ_1 and ϕ_2, $\phi_1 \approx_E \phi_2$ iff $\phi_{1|G_1} \approx_{E'^{-G_2}_{\mathsf{BP}}} \phi_{2|G_1}$ and $\overline{\phi_{1|G_1}}\phi_{1|G_2} \approx_{E'^{-G_1}_{\mathsf{BP}}} \overline{\phi_{2|G_1}}\phi_{2|G_2}$.

As $E'^{-G_2}_{\mathsf{BP}}$ and $E'^{-G_1}_{\mathsf{BP}}$ correspond both to the classical equational theory modelling Diffie-Hellman, which is known to be decidable [16] 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. □

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.

An interesting open question in the context of bilinear pairing also arises when we do not restrict frames to be $\{G_1, G_2\}$-sorted, i.e., when we allow terms of type R in the frame. To the best of our knowledge there exist no (un)decidability results for static equivalence (and even for deduction) without this restriction. Even in the case of the simpler Diffie-Hellman equational theory these questions are open.

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 *Lecture Notes in Computer Science*, 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. Delaune. YAPA: A generic tool for computing intruder knowledge. In R. Treinen, editor, *Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA'09)*, volume 5595 of *Lecture Notes in Computer Science*, pages 148–163, Brasília, Brazil, June-July 2009. Springer.
7. M. Baudet, V. Cortier, and S. Kremer. Computationally sound implementations of equational theories against passive adversaries. *Information and Computation*, 207(4):496–520, 2009.
8. 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 *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.
9. Y. Chevalier and M. Rusinowitch. Hierarchical combination of intruder theories. *Information and Computation*, 206(2-4):352–377, 2008.
10. Ş. Ciobâcă, S. Delaune, and S. Kremer. Computing knowledge in security protocols under convergent equational theories. In R. Schmidt, editor, *Proceedings of the 22nd International Conference on Automated Deduction (CADE'09)*, Lecture Notes in Computer Science, pages 355–370, Montreal, Canada, Aug. 2009. Springer.
11. H. Comon. Inductionless induction. In J. A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, pages 913–962. Elsevier, 2001.
12. 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.
13. 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.
14. D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
15. 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 *Lecture Notes in Computer Science*, pages 385–394. Springer, 2000.
16. 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 *Lecture Notes in Computer Science*, pages 610–625. Springer, 2007.
17. S. Kremer and L. Mazaré. Computationally sound analysis of protocols using bilinear pairings. *Journal of Computer Security*, 2009. To appear.
18. S. Kremer, A. Mercier, and R. Treinen. Reducing equational theories for the decision of static equivalence. In A. Datta, editor, *Proceedings of the 13th Asian Computing Science Conference (ASIAN'09)*, volume 5913 of *Lecture Notes in Computer Science*, pages 94–108, Seoul, Korea, Dec. 2009. Springer.