Reducing Equational Theories for the Decision of Static Equivalence (Preliminary Version) *

Steve Kremer[1], Antoine Mercier[1], and Ralf Treinen[2]

[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

For almost thirty years, many formal models for analyzing cryptographic protocols have been developed. Among them we find logical or symbolic models, based on the seminal ideas of Dolev and Yao [11], that 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.

Messages of the protocol are represented by terms in an abstract algebra. The motivation of such abstractions was the simplification and even automation of the analyzes and the proofs 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 pi calculus [2]. 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

* A final version has been submitted to a conference.

active attackers, static equivalence has also been used to characterize process equivalences [2] and off-line guessing attacks [9, 4]. There now exist exact [1], and approximate [6] 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 algorithmetically 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. This kind of signatures 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 [3], 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 given in [15].

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* $\mathcal{N} = \mathcal{N}_s$ 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
$\mid\ x$	variable x of sort s
$\mid\ n$	name n of sort s
$\mid\ f(t_1, \dots, t_k)$	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 denote $|t|$ 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 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 $Pos(f(t_1, \dots, t_n)) = \{\Lambda\} \cup \{i \cdot \pi \mid 1 \leq i \leq n, \pi \in Pos(t_i)\}$. 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 $=_E$ 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 *rewriting 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 $t_1 \to_{\mathcal{R}/E} t_2 \to_{\mathcal{R}/E} \dots$. $\mathcal{R}$ 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, we write that s is a normal form of t. When this normal form is unique (up to E) we write $s = t\downarrow_{\mathcal{R}/E}$. We say that $(\mathcal{R}, E)$ is a *decomposition* of E' when $\mathcal{R}$ is E-convergent, and $u =_{E'} v$ iff $u\downarrow_{\mathcal{R}/E} = v\downarrow_{\mathcal{R}/E}$ for all ground terms u, v.

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 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 $S = \{\mathsf{sort}(x) | x \in \mathrm{dom}(\phi)\}$, and we say that ϕ is *S-sorted*.

For simplicity, we only consider frames $\phi = \nu\tilde{n}\{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ which restricts every name in use, that is, for which $\tilde{n} = \mathsf{names}(t_1, \dots, t_n)$. A name a my 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 [1]). *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 $\{\tilde{n}\} \cap (\mathsf{names}(M) \cup \mathsf{names}(N)) = \emptyset$.*

Definition 2 (static equivalence [1]). *Two frames ϕ and ψ are* statically equivalent *for the equational theory E, written $\phi \approx_E \psi$, iff $dom(\phi) = dom(\psi)$, 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, we call *distiguishers* of ϕ and ψ the terms M and N such that $(M =_E N)\phi$ and $(M \neq_E N)\psi$.

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.

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

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

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

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

We will write $*$ instead of $*_i$, the type of $*$ being always clear from the context. As a convenient shortcut we sometimes write t^i for $\underbrace{t * \ldots * t}_{i\times}$. The properties of these function symbols are defined by the following equational theory E_{BP}.

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

$$\begin{array}{rcll} exp_i(x) *_i exp_i(y) & = & exp_i(x+y) & i \in \{1,2\} \\ e(exp_1(x), exp_1(y)) & = & exp_2(x \cdot y) & \end{array}$$

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:

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

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 choice of 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 oriented labelled graph (V, E) where $V = \mathcal{S}$, $E \subseteq V \times V \times \mathcal{F}$ and $(r, s, f) \in E$ iff $\mathsf{sort}(f) = s_1 \times \cdots \times s_n \to s$ 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, s, f) and (r', s', f') we have $s = r'$.

Definition 4 (valve). *A symbol f of arity $\cdots \times r \times \cdots \to s$ 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 $(\mathcal{S}_{\mathsf{BP}}, \mathcal{F}_{\mathsf{BP}})$ introduced in our running example in Section 3. $\mathcal{G}(\mathcal{S}_{\mathsf{BP}}, \mathcal{F}_{\mathsf{BP}})$ is given in Figure 1.

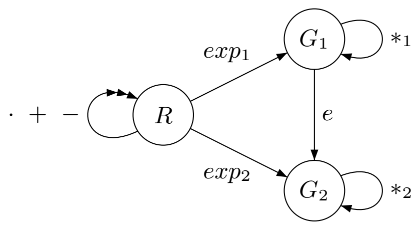

Fig. 1. $\mathcal{G}(\mathcal{S}_{\mathsf{BP}}, \mathcal{F}_{\mathsf{BP}})$

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 $T_1[x_1, \ldots, x_n], \ldots, T_m[x_1, \ldots, x_n]$ of arity $r \times \cdots \times r \to s$ such that for all public contexts $C_1[x_1, \ldots, x_n], \ldots, C_k[x_1, \ldots, x_n]$ of arity $r \times \cdots \times r \to r$ 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*

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

Intuitively, reducibility for a valve 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

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

Every public context $C_i[x_1, \ldots x_n]$ of arity $G_1 \times \cdots \times G_1 \to G_1$ has 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 is term over the set of constants of sort R. Note that p_i is E_{BP}-equivalent to some term $1_R +_R \cdots +_R 1_R$ (l times), hence $exp_1(p_i)$ is E_{BP}-equivalent to $exp_1(1_R)^{l_i}$.

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 $t_1, \ldots, t_n$

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

Base case. We distinguish three cases:

1. $C_1 = \lambda x_1.\ldots.\lambda x_n.x_i * exp_1(1_R)^{l_1}$ and $C_2 = \lambda x_1.\ldots.\lambda x_n.x_j * exp_1(1_R)^{l_2}$,
2. or w.l.o.g. $C_1 = \lambda x_1.\ldots.\lambda x_n.x_i * exp_1(1_R)^{l_1}$ and $C_2 = exp_1(1_R)^{l_2}$,
3. or $C_1 = exp_1(1_R)^{l_1}$ and $C_2 = exp_1(1_R)^{l_2}$.

In the first case we have $e(C_1[t_1, \ldots, t_n], C_2[t_1, \ldots, t_n]) = e(t_i, t_j) * exp_2(1_R)^{l_1+l_2}$ for any sequence of terms $t_1, \ldots, t_n$. With $D = \lambda\overline{y}.y_{ij} * exp_2(1_R)^{l_1+l_2}$ we obtain that $D[T_1, \ldots, T_n, T_{11}, \ldots, T_{nn}][t_1, \ldots, t_n] = e(t_i, t_j) * exp_2(1_R)^{l_1+l_2}$.

We do a similar reasoning in the second case and put $D = \lambda\overline{y}.y_i * exp_2(1_R)^{l_1+l_2}$.

In the last case we simply have that $D = exp_2(1_R)^{l_1+l_2}$.

Inductive case : $C_i = C_{i1} * C_{i2}[x_1, \ldots, x_n]$. 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 term $t_1, \ldots t_n$ 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 $e(C_{11} * C_2)[t_1, \ldots, t_n] =_E D_1[t_1, \ldots, t_n]$ and $e(C_{12} * C_2)[t_1, \ldots, t_n] =_E D_2[t_1, \ldots, t_n]$. Hence defining D as $D_1 * D_2$ we obtain our result. $\square$

Example 3. For $n = 2$ we obtain

$$\begin{array}{ll} T_1 = e(x_1, exp_1(1)) & T_{1,1} = e(x_1, x_1) \\ T_2 = e(x_2, exp_1(1)) & T_{1,2} = e(x_1, x_2) \\ & T_{2,2} = e(x_2, x_2) \end{array}$$

and we have for $C_1 = \lambda x_1, x_2.x_1$ and $C_2 = \lambda x1, x_2.x_2 * x_2 * exp_1(1 + 1)$ that

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

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 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 $exp_1(r)$ for some element of R.

One might have have expected reducibility for a symbol f to be equivalent 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 $\mathsf{sort}(f) = r \to s$, 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 $T_1 = \lambda x_1. \ldots \lambda x_n.f(x_1), \ldots, T_n = \lambda x_1. \ldots \lambda x_n.f(x_n)$. 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 $t_1, \ldots, t_n$ is equal to $n_1, \ldots, n_n$, and as the only possible contexts C of sort r are of the form $\lambda x_1. \ldots \lambda x_n.x_i$, we have $f(C[t_1, \ldots, t_n]) = f(n_i)$. Hence we only have to verify that for any i there exists a context D such that $f(n_i) =_E D[T_1[n_1, \ldots, n_n], \ldots, T_n[n_1, \ldots, n_n]]$. We choose $D = \lambda y_1. \ldots \lambda y_n.y_i$.

To show that E is not sufficiently complete w.r.t. f, we only remark that as f is free, for any i the term $f(n_i)$ are 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 $0_r : r,\ s_r : r \to r,\ f : r \to s,\ 0_s : s,\ s_s : s \to s$. The function symbol f is the valve. We have the following equational theory:

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

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 [15]. □

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 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 $\phi = \nu\tilde{n}\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ be a frame of sort r. The* reduction *of ϕ is defined as $\overline{\phi} = \{y_1 \mapsto T_1[t_1, \ldots t_n], \ldots, y_m \mapsto T_m[t_1, \ldots t_n]\}$ where the T_i are the contexts 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 (s-restriction). *Let $\phi = \nu\tilde{n}.\sigma_\phi$ be an $\{s_1, \ldots, s_n\}$-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 :

$$\phi_{BDH} = \nu a, b, c, r.\{x_1 \mapsto exp_1(a), x_2 \mapsto exp_1(b), x_3 \mapsto exp_1(c)\}$$

Using the set of terms T_i and T_{ij} defined in the proof of Proposition 1, we get

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

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

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

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

If $M = f'(C_1[x_1, \ldots, x_n, y_1, \ldots, y_m], \ldots, C_{k'}[x_1, \ldots, x_n, y_1, \ldots, y_m])$ with $f' \neq f$ then $\mathsf{sort}(C_i) = s$. By induction there exist public contexts $D_1 \ldots D_{k'}$ such that for any $\{r,s\}$-sorted frame ϕ of size n, $C_i\phi =_E D_{i'}\overline{\phi_{|r}}\phi_{|s}$. We define $M' = f'(D_1 \ldots D_{k'})$, and obtain $M\phi =_E M'\overline{\phi_{|r}}\phi_{|s}$. □

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 $\overline{\phi}_i$ 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: We assume $\phi_1 \not\approx_E \phi_2$ and consider the two possibilities for the sorts of the distinguishers M and N. If $\mathsf{sort}(M) = r$, by the fact that f is a valve, we have that M and N distinguish $\phi_{1|r}$ and $\phi_{2|r}$. If $\mathsf{sort}(M) = s$, by invoking Lemma 3, we infer the existence of distinguishers for $\overline{\phi_{1|r}}\phi_{1|s}$ and $\overline{\phi_{2|r}}\phi_{2|s}$. □

A detailed proof can be found in [15].

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 conditions which 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 type 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 invoke the condition that for any two terms M N of type r $(M =_E N)\phi_1$ iff $(M =_E N)\phi_2$ as well as the construction of σ_1 and σ_2.

To show that $M\phi_i =_E N\phi_i$ iff $M\phi_i\sigma_i =_E N\phi_i\sigma_i$ for $i \in \{1, 2\}$, we study the two directions of the equivalence independantly. To show that $M\phi_i =_E N\phi_i$ implies $M\phi_i\sigma_i =_E N\phi_i\sigma_i$, we recall a useful definition of *cutting function* already given in [5]. Then showing that σ_1 (resp. σ_2) corresponds to a sequence of cutting function applications allows us to use Lemma 15 of [5]. To show that $M\phi_i\sigma_i =_E N\phi_i\sigma_i$ implies $M\phi_i =_E N\phi_i$ we simply invoke the fact that σ_1 and σ_2 are bijective. □

A complete proof lies in [15].

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

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

We will prove the three following assertion 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) $\overline{\phi_{1|r}}\phi_{1|s} \not\approx_E \overline{\phi_{2|r}}\phi_{2|s}$ iff $\overline{\phi_{1|r}}\phi_{1|s} \not\approx_{E'} \overline{\phi_{2|r}}\phi_{2|s}$.

$\overline{\phi_{1|r}}\phi_{1|s} \not\approx_E \overline{\phi_{2|r}}\phi_{2|s}$ 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 symbols. Hence $M\overline{\phi_{i|r}}\phi_{i|s}$ and $N\overline{\phi_{i|r}}\phi_{i|s}$ do not involve f symbols also. As E' is sufficient for E without f we have that $M\overline{\phi_{i|r}} =_E N'\overline{\phi_{i|r}}$ 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 us 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 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 exists terms M' and N' such that $M\phi_i =_E M'\overline{\phi_{i|r}}$ and $N\phi_i =_E N'\overline{\phi_{i|r}}$. 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, $M\phi_{i|r}$ and $N\phi_{i|r}$ do not involve f symbols also. 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 $\phi_{1|r} \not\approx_E \phi_{2|r}$ If $\phi_{1|r} \not\approx_{E'} \phi_{2|r}$ then let us consider two 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 term 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 symbol 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 $\phi_{1|r} \not\approx_E \phi_{2|r}$. □

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*

- *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 $\phi_{1|r} \approx_{E'^{-s}} \phi_{2|r}$ 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 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 $(M =_E N)\phi_2$. 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. Let us recall that 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 symbols. Hence $M\overline{\phi_{i|r}}\phi_{i|s}$ and $N\overline{\phi_{i|r}}\phi_{i|s}$ do not involve f symbols also. 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. Hence $M\overline{\phi_{i|r}} =_{E'} N'\overline{\phi_{i|r}}$ iff $M\overline{\phi_{i|r}}\phi_{i|s} =_{E'^{-r}} N\overline{\phi_{i|r}}\phi_{i|s}$. Hence $\overline{\phi_{1|r}}\phi_{1|s} \not\approx_{E'^{-r}} \overline{\phi_{2|r}}\phi_{2|s}$. □

6 A criterion for sufficient equational theories

In this section we make a first attempt to find sufficient criteria for applying the Theorem 1. Future work includes finding broader criteria. Also, we 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 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 $u =_{E'} v$.

Example 5 (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 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 $\mathcal{R}_{\mathsf{BP}}$ exclusively defines e we have that $E^{'}_{\mathsf{BP}}$ is sufficient without e for E_{BP} by Lemma 6. Proposition 1 shows 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 $\phi_{1|G_1} \approx_{E'^{-G_2}_{\mathsf{BP}}} \phi_{2|G_1}$ 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 Diffie-Hellman equational theory, 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.

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 in order to find 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 the reducibility.

(2) In this paper we have analyzed the case where there is only one reducible valve in an equational theory. We think that extending the reduction possibilities to the case where several valves belong to the theory is possible. Nevertheless it seems that we should define 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 type to another. Yet cases where a valve takes as argument terms of distinct types 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 should state some conditions on the links between the arguments of such valves.

References

1. Martín Abadi and Véronique Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 367(1):2–32, 2006.
2. Martín Abadi and Cédric 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.
3. Mathilde Arnaud, Véronique Cortier, and Stéphanie 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.
4. Mathieu 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.
5. Mathieu Baudet, Véronique Cortier, and Steve Kremer. Computationally sound implementations of equational theories against passive adversaries. *Information and Computation*, 207(4):496–520, 2009.
6. Bruno Blanchet. Automatic proof of strong secrecy for security protocols. In *Proceedings of the 25th IEEE Symposium on Security and Privacy (SSP'04)*, pages 86–100. IEEE Computer Society, 2004.
7. Dan Boneh and Matthew 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. Hubert Common. Inductionless induction. In *Handbook of Automated Reasoning*. Elsevier, 2001.
9. Ricardo Corin, Jeroen Doumen, and Sandro 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. Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.
11. Danny Dolev and Andrew C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
12. Antoine 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. Steve Kremer and Laurent 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. Steve Kremer and Laurent Mazaré. Computationally sound analysis of protocols using bilinear pairings. *Journal of Computer Security*, 2009. To appear.
15. Steve Kremer, Antoine Mercier, and Ralf Treinen. Reducing equational theories for the decision of static equivalence. Research Report LSV, Laboratoire Spécification et Vérification, ENS Cachan, France, May 2009. http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/rapports.php?filename=lsv-2009.