Combining algorithms for deciding knowledge in security protocols

Mathilde Arnaud, Véronique Cortier, Stéphanie Delaune

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Combining algorithms for deciding knowledge in security protocols

Mathilde Arnaud — Véronique Cortier — Stéphanie Delaune

N° 6118

Février 2007

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--6118--FR+ENG

Combining algorithms for deciding knowledge in security protocols

Mathilde Arnaud*, Véronique Cortier†, Stéphanie Delaune†

Thème SYM — Systèmes symboliques
Projets Cassis

Rapport de recherche n° 6118 — Février 2007 — 28 pages

Abstract: In formal approaches, messages sent over a network are usually modeled by terms together with an equational theory, axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). The analysis of cryptographic protocols requires a precise understanding of the attacker knowledge. Two standard notions are usually used: deducibility and indistinguishability. Those notions are well-studied and a lot of decidability results already exist to deal with a variety of equational theories.

We show that decidability results can be easily combined for any disjoint equational theories: if the deducibility and indistinguishability relations are decidable for two disjoint theories, they are also decidable for their union. As an application, new decidability results can be obtained using this combination theorem.

Key-words: equational theories, security protocols, deduction, static equivalence, combination of decision procedures

* École Normale Supérieure de Cachan, Computer Science department, France
† LORIA, CNRS & INRIA project Cassis, Nancy, France. This work has been partly supported by the RNTL project PROUVÉ and the RNTL project POSE

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,
615, rue du Jardin Botanique, BP 101, 54602 Villers-Lès-Nancy (France)
Téléphone : +33 3 83 59 30 00 —Télécopie : +33 3 83 27 83 19

Algorithmes de combinaison pour décider la déduction et l'équivalence statique

Résumé : En méthodes formelles, les messages sont représentés par des termes accompagnés d'une théorie équationelle permettant de prendre en compte les propriétés algébriques des opérateurs considérés (chiffrement, ou exclusif, ...). L'analyse des protocoles de sécurité demande de raisonner sur la connaissance de l'intrus. Deux notions standards sont utilisées: la déduction et l'indistinguabilité. Ces notions ont été bien étudiées et de nombreux résultats de décidabilité existent. Ils permettent de traiter une grande variété de théories équationnelles.

Nous montrons que ces résultats de décidabilité peuvent se combiner dès lors que les théories équationnelles ne partagent pas de symboles: si la déduction et l'indistinguabilité sont décidables pour deux théories disjointes, ces deux notions sont également décidables pour leur union. De nouveaux résultats peuvent être ainsi obtenus en utilisant la procédure de combinaison proposée.

Mots-clés : théories équationnelles, protocoles de sécurité, déduction, équivalence statique, combinaison de procédures de décision

Contents

1 Introduction

Security protocols are paramount in today's secure transactions through public channels. It is therefore essential to obtain as much confidence as possible in their correctness. Formal methods have proved their usefulness for precisely analyzing the security of protocols. Understanding security protocols often requires reasoning about knowledge of the attacker. In formal approaches, two main kind of definitions have been given in the literature for this knowledge. They are known as message deducibility and indistinguishability relations.

Most often, the knowledge of the attacker is described in terms of message deducibility [17, 19, 18]. Given some set of messages ϕ representing the knowledge of the attacker and another message M, intuitively the secret, one can ask whether an attacker is able to compute M from ϕ. To obtain such a message he uses his deduction capabilities. For instance, he may encrypt and decrypt using keys that he knows.

This concept of deducibility does not always suffice for expressing the knowledge of an attacker. For example, if we consider a protocol that transmits an encrypted Boolean value, we may ask whether an attacker can learn this value by eavesdropping the protocol. Of course, it seems to be completely unrealistic to say that the Boolean true and false are not deducible. We need to express the fact that the two transcripts of the protocol, one running with the Boolean value true and the other one with false are *indistinguishable*. Besides allowing more careful formalization of secrecy properties, indistinguishability can also be used for proving the more involved notion of cryptographic indistinguishability [7, 1, 16]: two sequences of messages are cryptographically indistinguishable if their distributions is indistinguishable to any attacker, that it to any probabilistic polynomial Turing machine.

In both cases, deduction and indistinguishability apply to observations on messages at a particular point in time. They do not take into account the dynamic behavior of the protocol. For this reason the indistinguishability relation is called *static equivalence*. Nevertheless those relations are quite useful to reason about the dynamic behavior of a protocol. For instance, the deducibility relation is often used as a subroutine of many decision procedures [20, 8, 12]. In the applied-pi calculus framework [5], it has been shown that observational equivalence (relation which takes into account the dynamic behavior) coincides with labeled bisimulation which corresponds to checking static equivalences and some standard bisimulation conditions.

Both of these relations rely on an underlying equational theory axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). A lot of decision procedures have been provided to decide these relations under a variety of equational theories. For instance algorithms for deduction are provided for exclusive or [12], homomorphic operators [13], Abelian groups with distributive encryption [15] and subterm theories [2]. These theories allow basic equations for functions such as encryption, decryption and digital signature. Static equivalence is also well-studied. For instance, a general decidability result to handle the class of subterm convergent equational theories is given in [2]. In [3] some abstract conditions on the underlying equational theory are proposed to ensure decidability of deduction and static equivalence. Note that the use of this result requires checking some assumptions, which might be difficult to prove. This result has been applied to several in-

teresting equational theories such as exclusive or, blind signature and other associative and commutative functions.

For all the previous results, decidability is provided for particular fixed theories or for particular classes of theories. In this paper, we provide a general combination result for both deduction and static equivalence: if the deducibility and indistinguishability relations are decidable for two disjoint theories E_1 and E_2 (that is, the equations of E_1 and E_2 do not share any symbol), they are also decidable for their union $\mathsf{E}_1 \cup \mathsf{E}_2$. Our algorithm for combining theories is polynomial (in the DAG-size of the inputs). It ensures in particular that if the deducibility and indistinguishability relations are decidable for two disjoint theories in polynomial time, they are decidable in polynomial time for their union.

The interest of our result is twofold: first, it allows to obtain new decidability results from any combination of the existing ones: for example, we obtain that static equivalence is decidable for the theory of encryption combined with exclusive or (and also for example with blind signature), which was not known before. Second, our result allows a modular approach. Deciding interesting equational theories that could not be considered before can be done simply by reducing to the decision of simpler and independent theories.

Our combination result relies on combination algorithms for solving unification problem modulo an equational theory [21, 6]. It is closed to the result of Chevalier and Rusinowitch [9], who show how to combine decision algorithms for the deducibility problem in presence of an active attacker. Their result takes into account the dynamic behavior of the protocol. Although our combination result for deduction is clearly related to their main result, how deduction can be combined for disjoint equational theories is not stated in their paper. Moreover they do not deal at all with static equivalence.

Outline of the paper. In Section 2 we introduce notation and definitions as well as the two notions of knowledge. Section 3 provides some material for our combination algorithms. Then Sections 4 and 5 are devoted to the study of deduction and static equivalence respectively. In Section 6, we sum up our results and provide new results obtained as a consequence of our main theorems. Omitted proofs can be found in the appendices.

2 Preliminaries

2.1 Basic definitions

A *signature* Σ consists of a finite set of function symbols, such as enc and pair, each with an arity. A function symbol with arity 0 is a constant symbol. Given a signature Σ, an infinite set of names $\mathcal{N}$, and an infinite set of variables $\mathcal{X}$, we denote by $\mathcal{T}(\Sigma)$ (resp. $\mathcal{T}(\Sigma, \mathcal{X})$) the set of *terms* over $\Sigma \cup \mathcal{N}$ (resp. $\Sigma \cup \mathcal{N} \cup \mathcal{X}$). The former is called the set of ground terms over Σ, while the later is simply called the set of terms over Σ. We write $fn(M)$ (resp. $fv(M)$) for the set of names (resp. variables) that occur in the term M. A context C is a term with holes, or (more formally) a linear term. When C is a context with n distinguished variables $x_1, \ldots, x_n$, we may write $C[x_1, \ldots, x_n]$ instead of C in order to show the variables, and when $T_1, \ldots, T_n$ are terms we may also write $C[T_1, \ldots, T_n]$ for the result of replacing

each variable x_i with the corresponding term T_i. A *substitution* σ is a mapping from a finite subset of $\mathcal{X}$ called its domain and written $dom(\sigma)$ to $\mathcal{T}(\Sigma, \mathcal{X})$. Substitutions are extended to endomorphisms of $\mathcal{T}(\Sigma, \mathcal{X})$ as usual. We use a postfix notation for their application.

We equip the signature Σ with an equational theory E, that is, an equivalence relation on terms that is closed under application of contexts and under substitutions of terms for both names and variables. We write $M =_{\mathsf{E}} N$ when M and N are terms and the equation $M = N$ is in E. A theory E is *consistent* if there does not exist two distinct names n_1 and n_2 such that $n_1 =_{\mathsf{E}} n_2$. Note that, in an inconsistent theory, the problem we are interested in, *i.e.* deduction (defined in 2.3) and static equivalence (defined in 2.4) are trivial.

Example 1 *Let Σ_{xor} be the signature made up of the constant symbol 0 and the binary function $\oplus$ and $\mathsf{E}_{\mathsf{xor}}$ induced by the following set of equations:*

$$\begin{array}{rcll} x \oplus (y \oplus z) & = & (x \oplus y) \oplus z & x \oplus 0 = x \\ x \oplus y & = & y \oplus x & x \oplus x = 0 \end{array}$$

We have that $a \oplus (b \oplus a) =_{\mathsf{E}_{\mathsf{xor}}} b$.

Definition 1 (syntactic subterm) *The set $St_s(M)$ of* syntactic subterms *of a term M is defined recursively as follows:*

$$St_s(M) = \begin{cases} \{M\} & \text{if } M \text{ is a variable or a name} \\ \{M\} \cup \bigcup_{i=1}^{\ell} St_s(M_i) & \text{if } M = f(M_1, \ldots, M_\ell) \end{cases}$$

The positions in a term M are defined recursively as usual (*i.e.* sequences of integers). We denote by $M|_p$ the syntactic subterm of M at position p. The term obtained by replacing $M|_p$ by N is denoted $M[N]_p$.

2.2 Assembling terms into frames

At a particular point in time, while engaging in one or more sessions of one or more protocols, an attacker may know a sequence of messages $M_1, \ldots, M_\ell$. This means that he knows each message but he also knows in which order he obtained the messages. So it is not enough for us to say that the attacker knows the set of terms $\{M_1, \ldots, M_\ell\}$. Furthermore, we should distinguish those names that the attacker knows from those that were freshly generated by others and which remain secret from the attacker; both kinds of names may appear in the terms.

In the applied pi calculus [5], such a sequence of messages is organized into a *frame* $\phi = \nu\tilde{n}.\sigma$, where $\tilde{n}$ is a finite set of names (intuitively the fresh ones), and σ is a substitution of the form:

$$\{{}^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}\} \quad \text{with} \quad dom(\sigma) = \{x_1, \ldots, x_\ell\}$$

The variables enable us to refer to each M_i and we always assume that the terms M_i are ground. The free names of ϕ, denoted $fn(\phi)$, are those which appear in ϕ and not in $\tilde{n}$, *i.e.* $(\bigcup_{i=1}^{\ell} fn(M_i)) \setminus \tilde{n}$. The names $\tilde{n}$ are bound and can be renamed. Moreover names that do not appear in the free names of ϕ can be added or removed from $\tilde{n}$.

2.3 Deduction

Given a frame ϕ that represents the information available to an attacker, we may ask whether a given ground term M may be deduced from ϕ. Given an equational theory E on Σ, this relation is written $\phi \vdash M$ and is axiomatized by the following rules:

$$\frac{}{\nu\tilde{n}.\sigma \vdash M} \text{ if } \exists x \in dom(\sigma) \text{ s.t. } x\sigma = M \qquad \frac{}{\nu\tilde{n}.\sigma \vdash s} \; s \notin \tilde{n}$$

$$\frac{\phi \vdash M_1 \quad \ldots \quad \phi \vdash M_\ell}{\phi \vdash f(M_1, \ldots, M_\ell)} \; f \in \Sigma \qquad \frac{\phi \vdash M}{\phi \vdash M'} \; M =_{\mathsf{E}} M'$$

Intuitively, the deducible messages are the messages of ϕ and the names that are not protected in ϕ, closed by equality in E and closed by application of function symbols. Note that that ϕ and M might be built on a signature Σ', possibly larger that Σ. Since the deducible messages depend on the underlying equational theory, we write $\vdash_{\mathsf{E}}$ when E is not clear from the context. When $\nu\tilde{n}.\sigma \vdash M$, any occurrence of names from $\tilde{n}$ in M is bound by $\nu\tilde{n}$. So $\nu\tilde{n}.\sigma \vdash M$ could be formally written $\nu\tilde{n}.(\sigma \vdash M)$. It is easy to prove by induction the following characterization of deduction.

Lemma 1 (characterization of deduction) *Let M be a ground term and $\nu\tilde{n}.\sigma$ be a frame. Then $\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M$ if and only if there exists a term ζ such that $fn(\zeta) \cap \tilde{n} = \emptyset$ and $\zeta\sigma =_{\mathsf{E}} M$. Such a term ζ is a* recipe *of the term M.*

Example 2 *Consider the signature $\Sigma_{\mathsf{enc}} = \{\mathsf{dec}, \mathsf{enc}, \mathsf{pair}, \mathsf{proj}_1, \mathsf{proj}_2\}$. The symbols $\mathsf{dec}, \mathsf{enc}$ and pair are functional symbols of arity 2 that represent respectively the decryption, encryption and pairing functions whereas proj_1 and proj_2 are functional symbols of arity 1 that represent the projection function on respectively the first and the second component of a pair. As usual, we may write $\langle x, y\rangle$ instead of $\mathsf{pair}(x, y)$. The equational theory of pairing and symmetric encryption, denoted by $\mathsf{E}_{\mathsf{enc}}$, is defined by the following equations:*

$$\mathsf{dec}(\mathsf{enc}(x, y), y) = x, \; \mathsf{proj}_1(\langle x, y\rangle) = x \quad \text{and} \quad \mathsf{proj}_2(\langle x, y\rangle) = y.$$

Let $\phi = \nu k, s_1.\{^{\mathsf{enc}(\langle s_1, s_2\rangle, k)}/_{x_1}, {}^{k}/_{x_2}\}$. We have $\phi \vdash k$, $\phi \vdash s_1$ and $\phi \vdash s_2$. Indeed x_2, $\mathsf{proj}_1(\mathsf{dec}(x_1, x_2))$ and s_2 are recipes of the terms k, s_1 and s_2 respectively.

We say that the deduction is decidable for the equational theory (Σ, E) if the following problem is decidable.

Entries A frame ϕ and a term M built on Σ

Question $\phi \vdash_{\mathsf{E}} M$?

2.4 Static equivalence

Deduction does not always suffice for expressing the knowledge of an attacker, as discussed in the introduction. Sometimes, the attacker can deduce exactly the same set of terms from two different frames but he could still be able to tell the difference between these two frames.

Definition 2 (static equivalence) *Let ϕ be a frame and M and N be two terms. We say that M and N are* equal in the frame φ *under the theory* E*, and write $(M =_{\mathsf{E}} N)\varphi$, if there exists $\tilde{n}$ such that $\phi = \nu\tilde{n}.\sigma$, $(fn(M) \cup fn(N)) \cap \tilde{n} = \emptyset$ and $M\sigma =_{\mathsf{E}} N\sigma$. We say that two frames $\varphi = \nu\tilde{n}.\sigma$ and $\varphi' = \nu\tilde{n}.\sigma'$ are* statically equivalent *w.r.t. (Σ, E), and write $\varphi \approx_{\mathsf{E}} \varphi'$ (or shortly $\varphi_1 \approx \varphi_2$) when $dom(\varphi) = dom(\varphi')$, and*

$$\forall M, N \in \mathcal{T}(\Sigma, \mathcal{X}) \text{ we have that } (M =_{\mathsf{E}} N)\varphi \Leftrightarrow (M =_{\mathsf{E}} N)\varphi'.$$

Example 3 *Consider the equational theory $(\Sigma_{\mathsf{enc}}, \mathsf{E}_{\mathsf{enc}})$ provided in Example 2. Let $\varphi = \nu k.\sigma$, $\varphi' = \nu k.\sigma'$ where $\sigma = \{^{\mathsf{enc}(s_0,k)}/_{x_1}, {}^{k}/_{x_2}\}$, $\sigma' = \{^{\mathsf{enc}(s_1,k)}/_{x_1}, {}^{k}/_{x_2}\}$. Intuitively, s_0 and s_1 could be the two possible (public) values of a vote. We have $\mathsf{dec}(x_1, x_2)\sigma =_{\mathsf{E}_{\mathsf{enc}}} s_0$ whereas $\mathsf{dec}(x_1, x_2)\sigma' \neq_{\mathsf{E}_{\mathsf{enc}}} s_0$. Therefore we have $\varphi \not\approx \varphi'$. However, note that $\nu k.\{^{\mathsf{enc}(s_0,k)}/_{x_1}\} \approx \nu k.\{^{\mathsf{enc}(s_1,k)}/_{x_1}\}$.*

Let (Σ, E) be an equational theory. We define $\mathsf{Eq}_{\mathsf{E}}(\phi)$ to be the set of equations satisfied by the frame $\phi = \nu\tilde{n}.\sigma$ in the equational theory E:

$$\mathsf{Eq}_{\mathsf{E}}(\phi) = \{(M, N) \in \mathcal{T}(\Sigma, \mathcal{X})^2 \mid (M =_{\mathsf{E}} N)\phi\}.$$

We write $\psi \models \mathsf{Eq}_{\mathsf{E}}(\phi)$ if $(M =_{\mathsf{E}} N)\psi$ for any $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$.

Checking for static equivalence is clearly equivalent to checking whether the frames satisfy each other equalities.

Lemma 2 (characterization of static equivalence) *Let $\phi_1 = \nu\tilde{n}.\sigma_1$ and $\phi_2 = \nu\tilde{n}.\sigma_2$ be two frames. We have*

$$\phi_1 \approx_{\mathsf{E}} \phi_2 \quad \Leftrightarrow \quad \phi_2 \models \mathsf{Eq}_{\mathsf{E}}(\phi_1) \text{ and } \phi_1 \models \mathsf{Eq}_{\mathsf{E}}(\phi_2).$$

We say that the static equivalence is decidable for the equational theory (Σ, E) if the following problem is decidable.

Entries Two frames ϕ_1 and ϕ_2 built on Σ

Question $\phi_1 \approx_{\mathsf{E}} \phi_2$?

3 Material for combination algorithms

We consider two equational theories (Σ_1, E_1) and (Σ_2, E_2) that are disjoint $(\Sigma_1 \cap \Sigma_2 = \emptyset)$ and consistent. We denote by Σ the union of the signatures Σ_1 and Σ_2 and by E the union of the equations E_1 and E_2.

3.1 Factors, Subterms

We denote by $\mathsf{sign}(\cdot)$ the function that associates to each term M, the signature (Σ_1 or Σ_2) of its root symbol. For $M \in \mathcal{N} \cup \mathcal{X}$, we define $\mathsf{sign}(M) = \bot$, where $\bot$ is a new symbol. The term N is *alien* to M if $\mathsf{sign}(N) \neq \mathsf{sign}(M)$. We now introduce our notion of *subterms*. This notion is also used in [9].

Definition 3 (factors, subterms) *Let $M \in \mathcal{T}(\Sigma, \mathcal{X})$. The* factors *of M are the maximal syntactic subterms of M that are alien to M. This set is denoted $Fct(M)$. The set of its* subterms*, denoted $St(M)$, is defined recursively by*

$$St(M) = \{M\} \cup \bigcup_{N \in Fct(M)} St(N)$$

These notations are extended as expected to sets of terms and frames.

Let $M \in \mathcal{T}(\Sigma, \mathcal{X})$. The size $|M|$ of a term M is defined $|M| = 0$ if M is a name or a variable and by $1 + \sum_{i=1}^{n} |N_i|$ if $M = C[N_1, \ldots, N_n]$ where C is a context built on Σ_1 (or Σ_2) and $N_1, \ldots N_n$ are the factors of M.

Example 4 *Consider the equational theories $\mathsf{E}_{\mathsf{enc}}$ and $\mathsf{E}_{\mathsf{xor}}$. Let M be the term $\mathsf{dec}(\langle n_1 \oplus \langle n_2, n_3\rangle, \mathsf{proj}_1(n_1 \oplus n_2)\rangle, n_3)$. The term $n_1 \oplus \langle n_2, n_3\rangle$ is a syntactic subterm of M alien to M since $\mathsf{sign}(n_1 \oplus \langle n_2, n_3\rangle) = \Sigma_{\mathsf{xor}}$ and $\mathsf{sign}(M) = \Sigma_{\mathsf{enc}}$. We have that $Fct(M) = \{n_1 \oplus \langle n_2, n_3\rangle,\ n_1 \oplus n_2,\ n_3\}$, $St(M) = Fct(M) \cup \{M,\ n_1,\ n_2,\ \langle n_2, n_3\rangle\}$ and $|M| = 4$.*

3.2 Ordered rewriting

Most of the definitions and results in this subsection are borrowed from [10] since we use similar techniques. We consider the notion of *ordered rewriting* defined in [14], which is a useful tool that has been used (*e.g.* [6]) for proving correctness of combination of unification algorithms. Let $<$ be a simplification ordering[1] on ground terms assumed to be total and such that the minimum for $<$ is a name n_{min} and the constant in Σ are smaller than any non-constant ground term. We define Σ_0 to be the set of the constant symbols of Σ_1 and Σ_2 plus the name n_{min}.

Given a possibly infinite set of equations $\mathcal{O}$ we define the ordered rewriting relation $\rightarrow_{\mathcal{O}}$ by $M \rightarrow_{\mathcal{O}} M'$ if and only if there exists an equation $N_1 = N_2 \in \mathcal{O}$, a position p in M and a substitution τ such that:

$$M = M[N_1\tau]_p, \quad M' = M[N_2\tau]_p \text{ and } N_1\tau > N_2\tau.$$

It has been shown (see [14]) that by applying the *unfailing completion procedure* to a set of equations E we can derive a (possibly infinite) set of equations $\mathcal{O}$ such that on ground terms:

1. the relations $=_{\mathcal{O}}$ and $=_{\mathsf{E}}$ are equal on $\mathcal{T}(\Sigma)$,
2. the rewriting system $\rightarrow_{\mathcal{O}}$ is convergent on $\mathcal{T}(\Sigma)$.

Applying unfailing completion to $\mathsf{E} = \mathsf{E}_1 \cup \mathsf{E}_2$, it is easy to notice [6] that the set of generated equations $\mathcal{O}$ is the disjoint union of the two systems $\mathcal{O}_1$ and $\mathcal{O}_2$ obtained by applying unfailing completion procedures to E_1 and to E_2 respectively. The relation $\rightarrow_{\mathcal{O}}$ being convergent on ground terms we can define $M{\downarrow_{\mathcal{O}}}$ (or shortly $M{\downarrow}$) as the unique normal form of

[1] By definition $<$ satisfies that for all ground terms M, N_1, N_2 such that $N_1 < M[N_1]$ and $N_1 < N_2$, we have $M[N_1] < M[N_2]$.

the ground term M for $\rightarrow_{\mathcal{O}}$. We denote by $M{\downarrow}_{\mathsf{E}_1}$ (resp. $M{\downarrow}_{\mathsf{E}_2}$) the unique normal form of the ground term M for $\rightarrow_{\mathcal{O}_1}$ (resp. $\rightarrow_{\mathcal{O}_2}$).

We have the following lemmas which are classical results (see [10]).

Lemma 3 *Let M be a non-constant ground term such that all its factors are in normal form. Then*

- *either $M{\downarrow} \in \Sigma_0 \cup Fct(M)$,*
- *or $\mathsf{sign}(M) = \mathsf{sign}(M{\downarrow})$ and $Fct(M{\downarrow}) \subseteq \Sigma_0 \cup Fct(M)$.*

Looking more carefully at the proof of Lemma 3 given in [10], we easily deduce the following lemma.

Lemma 4 *Let M be a non-constant ground term such that $\mathsf{sign}(M) = \Sigma_i$ $(i = 1, 2)$ and all its factors are in normal form. Then $M{\downarrow} = M{\downarrow}_{\mathsf{E}_i}$.*

3.3 Normalization and replacements

If Π is a set of positions in a term M, we denote by $M[\Pi \leftarrow N]$ the term obtained by replacing any term at some position in Π by N. We denote by $\delta_{N,N'}$ the replacement of the occurrences of N which appears at a subterm position by N'. It is easy to establish the following lemma (see [10]).

Lemma 5 *Let M be a term such that its factors are in normal form. Let $N \in Fct(M)$ and N' be a term alien to M. We have that $(M\delta_{N,N'}){\downarrow} = ((M{\downarrow})\delta_{N,N'}){\downarrow}$.*

Example 5 *Consider the equational theories $\mathsf{E}_{\mathsf{enc}}$ and $\mathsf{E}_{\mathsf{xor}}$.*
Let $M = \mathsf{dec}(\mathsf{enc}(\langle n_1 \oplus n_2, n_1 \oplus n_2 \oplus n_3\rangle, n_1 \oplus n_2), n_1 \oplus n_2)$, $N = n_1 \oplus n_2$ and $N' = n$. We have that

- *$M\delta_{N,N'} = \mathsf{dec}(\mathsf{enc}(\langle n, n_1 \oplus n_2 \oplus n_3\rangle, n), n)$,*
- *$M{\downarrow}\delta_{N,N'} = \langle n, n_1 \oplus n_2 \oplus n_3\rangle$.*

Hence, we have that $M\delta_{N,N'}{\downarrow} = M{\downarrow}\delta_{N,N'}{\downarrow}$.

Let $\rho : F \rightarrow \tilde{n}_F$ is a replacement (that is a function) from a finite set of terms F to names $\tilde{n}_F$. Let $F = \{t_1, \ldots, t_k\}$ such that whenever t_i is a syntactic subterm of t_j implies $i > j$. For any term M, we denote by M^ρ the term obtained by replacing in M (in an order that is consistent with the subterm relation) any subterm N that is equal to some $N' \in F$ by $\rho(N')$. Formally, $M^\rho = (M\delta_{t_1,\rho(t_1)}) \cdots \delta_{t_k,\rho(t_k)}$. This extends in a natural way to set of terms, substitutions, frames ...

Example 6 *Consider the equational theories $\mathsf{E}_{\mathsf{enc}}$ and $\mathsf{E}_{\mathsf{xor}}$ and the term $t = \mathsf{dec}(\langle n_1 \oplus \langle n_1 \oplus n_2, n_3\rangle, \mathsf{proj}_1(n_1 \oplus n_2)\rangle, n_1 \oplus n_2)$. Let ρ_2 be the replacement $\{n_1 \oplus \langle n_1 \oplus n_2, n_3\rangle \rightarrow k_1,\ n_1 \oplus n_2 \rightarrow k_2\}$. $t^{\rho_2} = \mathsf{dec}(\langle k_1, \mathsf{proj}_1(k_2)\rangle, k_2)$.*

4 Combining algorithms for deduction

This section is devoted to the (sketch of) proof of the following theorem.

Theorem 1 *Let* (Σ_1, E_1) *and* (Σ_2, E_2) *be two consistent equational theories such that* $\Sigma_1 \cap \Sigma_2 = \emptyset$. *If deduction is decidable for* (Σ_1, E_1) *and* (Σ_2, E_2) *then deduction is decidable for* $(\Sigma_1 \cup \Sigma_2, \mathsf{E}_1 \cup \mathsf{E}_2)$.

Our algorithm consists in reducing the problem to decide whether $\phi \vdash_{\mathsf{E}} M$ ($\mathsf{E} = \mathsf{E}_1 \cup \mathsf{E}_2$) to several deduction problems. Each of them will be solved either in the equational theory E_1 or in the theory E_2. Our procedure first relies on the existence of a *local proof* of $\phi \vdash M$ which involves only terms in $St(\phi, M)$.

Lemma 6 (locality lemma) *Let* $\phi = \nu\tilde{n}.\sigma$ *be a frame and* M *be a ground term built on* Σ *and in normal form. If* $\phi \vdash_{\mathsf{E}} M$ *then there exists a term* ζ *on* Σ *such that*

- $fn(\zeta) \cap \tilde{n} = \emptyset$ *and* $\zeta\sigma =_{\mathsf{E}} M$,
- *for all* $\zeta' \in St(\zeta)$, *we have* $\zeta'\sigma\downarrow \in St(\phi, M) \cup \Sigma_0$.
  Moreover, if $\mathsf{sign}(\zeta') \neq \mathsf{sign}(\zeta'\sigma\downarrow)$, *we have* $\zeta'\sigma\downarrow \in St(\phi) \cup \Sigma_0$.

Example 7 *Consider again the equational theories* $\mathsf{E}_{\mathsf{enc}}$ *and* $\mathsf{E}_{\mathsf{xor}}$, *the frame* $\phi = \nu n_2, n_3.\{^{\mathsf{enc}(\langle n_1 \oplus n_2, n_3\rangle, n_4)}/_{x_1}\}$ *and* $M = n_2 \oplus n_3$. *We have that* $\phi \vdash M$. *The recipe* $\zeta = \mathsf{proj}_1(\mathsf{dec}(x_1, n_4)) \oplus \mathsf{proj}_2(\mathsf{dec}(x_1, n_4)) \oplus n_1$ *satisfies the conditions given in Lemma 6.*

We also need to decide deducibility in the theory E_1 (resp. E_2) for terms built on $\Sigma_1 \cup \Sigma_2$. Therefore, we show that we can abstract the alien factors by new names.

Lemma 7 *Let* ϕ *be a frame and* M *be a ground term built on* Σ *and in normal form. Let* $F_2 = \{N \mid N \in St(\phi, M)$ *and* $\mathsf{sign}(N) = \Sigma_2\}$, $\tilde{n}_{F_2}$ *be a set of names, distinct from the names occurring in* ϕ *and* M, *of same cardinality as* F_2 *and* $\rho_2 : F_2 \to \tilde{n}_{F_2}$ *be a bijection. We have that*

$$\phi \vdash_{\mathsf{E}_1} M \text{ if and only if } \nu\tilde{n}_{F_2}.(\phi \vdash_{\mathsf{E}_1} M)^{\rho_2}.$$

A similar result holds by inverting the indices 1 and 2.

We show the lemmas above (see Appendix) by using Lemmas 3, 4 and 5 stated in Section 3. Then, we proceed by saturation of ϕ by the subterms in $St(\phi, M)$ which are deducible either in (Σ_1, E_1) or in (Σ_2, E_2).

Algorithm. Given a frame ϕ and a term M, we saturate ϕ as follows.

- We start with $\phi_0 = \phi \cup \Sigma_0$.

- For any term $T \in St(\phi, M)$, if $\nu\tilde{n}_{F_2}.(\phi_k \vdash_{\mathsf{E}_1} T)^{\rho_2}$ or $\nu\tilde{n}_{F_1}.(\phi_k \vdash_{\mathsf{E}_2} T)^{\rho_1}$ where F_1, F_2, ρ_1, ρ_2 are defined like in Lemma 7, we add T in the set of deducible subterms: $\phi_{k+1} = \phi_k \cup \{T\}$.

We start over the procedure until there is no more $T \in St(\phi, M)$ such that $\nu\tilde{n}_{F_2}.(\phi_k \vdash_{\mathsf{E}_1} M)^{\rho_2}$ or $\nu\tilde{n}_{F_1}.(\phi_k \vdash_{\mathsf{E}_1} M)^{\rho_1}$. Let ϕ^* be the saturated set. Using Lemma 6, we can show that ϕ^* contains exactly the set of all deducible subterms of $St(\phi, M)$. We deduce that $\phi \vdash_{\mathsf{E}_1 \cup \mathsf{E}_2} M$ if and only if $M \in \phi^*$.

Example 8 *Consider again Example 7, we successively add in the frame the terms $n_1 \oplus n_2$, n_3 and $n_2 \oplus n_3$.*

Complexity. Our reduction is polynomial. Our notion of size for terms was introduced for proving our lemmas by induction. It does not correspond to the actual size of a term since our notion of subterms does not take into account intermediate syntactic subterms. In addition, complexity results for deduction and static equivalence are usually given as function of the DAG-size of the terms. Thus we express the complexity of our procedure as function of the DAG-size. The DAG-size of a term T, denoted $t_{\mathsf{dag}}(t)$, is the number of distinct syntactic subterms. We assume that $\phi \vdash_{\mathsf{E}_i} M$ can be decided in time $f_i(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$ where $f_i : \mathbb{N} \to \mathbb{R}$, $i \in \{1, 2\}$. Saturating ϕ requires at most $|St(\phi, M)| \leq t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)$ steps. At each step, we check whether $\nu\tilde{n}_{F_2}.(\phi_k \vdash_{\mathsf{E}_1} T)^{\rho_2}$ or $\nu\tilde{n}_{F_1}.(\phi_k \vdash_{\mathsf{E}_2} T)^{\rho_1}$ for each $T \in St(\phi, M)$. We deduce that ϕ^* can be computed in time $\mathcal{O}((t_{\mathsf{dag}}(\phi)+t_{\mathsf{dag}}(M))^2[f_1(2(t_{\mathsf{dag}}(\phi)+t_{\mathsf{dag}}(M)))+ f_2(2(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)))])$. In particular, if deciding $\vdash_{\mathsf{E}_i}$ can be done in polynomial time for $i \in \{1, 2\}$ then deciding $\vdash_{\mathsf{E}_1 \cup \mathsf{E}_2}$ is also polynomial.

5 Combination algorithm for static equivalence

This section is devoted to the (sketch of) proof of the following theorem.

Theorem 2 *Let (Σ_1, E_1) and (Σ_2, E_2) be two equational theories such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. If deduction and static equivalence are decidable for (Σ_1, E_1) and (Σ_2, E_2) then static equivalence is decidable for $(\Sigma_1 \cup \Sigma_2, \mathsf{E}_1 \cup \mathsf{E}_2)$.*

We more precisely show that whenever static equivalence is decidable for (Σ_1, E_1) and (Σ_2, E_2) and deduction is decidable for (Σ, E), then static equivalence is decidable for (Σ, E) where $\Sigma = \Sigma_1 \cup \Sigma_2$ and $\mathsf{E} = \mathsf{E}_1 \cup \mathsf{E}_2$. Thanks to our combination result for deduction (Theorem 1), we know it is sufficient for deduction to be decidable for (Σ_1, E_1) and (Σ_2, E_2). Note that the decidability of $\vdash_{\mathsf{E}_i}$ is not necessarily a consequence of the decidability of $\approx_{\mathsf{E}_i}$. The encoding proposed in [3] works only when there exists a free function symbol in Σ_1.

Our decision procedure works as follows. We first add to the frames all their deducible subterms. This is the reason why we require the decidability of $\vdash_{\mathsf{E}}$. Then, we show that to decide whether $\phi_1 \models \mathsf{Eq}_{\mathsf{E}}(\phi_2)$, it is sufficient to check whether $\phi_1 \models \mathsf{Eq}_{\mathsf{E}_1}(\phi_2)$ and $\phi_1 \models \mathsf{Eq}_{\mathsf{E}_2}(\phi_2)$. Lastly, we abstract alien subterms by fresh names in order to reduce the signature.

5.1 Step 1: adding deducible subterms to the frames

Given $\phi_1 = \nu\tilde{n}.\sigma_1$ and $\phi_2 = \nu\tilde{n}.\sigma_2$ such that $dom(\phi_1) = dom(\phi_2)$, we define the frame $\overline{\phi_2}^{\phi_1}$ by extending ϕ_2 with deducible terms.

$$\overline{\phi_2}^{\phi_1} \stackrel{\text{def}}{=} \phi_2 \cup \{^{\zeta_1\sigma_2\downarrow}/_{x_1}, \ldots, ^{\zeta_n\sigma_2\downarrow}/_{x_n}\}$$

where ζ_i is a recipe of t_i, *i.e.* $\zeta_i\sigma_1\downarrow = t_i$ and $fn(\zeta_i) \cap (\tilde{n_1} \cup \tilde{n_2})$ such that:

- $t_i \in St(\phi_1) \cup \Sigma_0$, and
- t_i is not in the image of ϕ_1, that is $t_i \neq x\sigma$ for any $x \in dom(\phi_1)$.

In particular, we have that $\overline{\phi}^{\phi} = \phi \cup \{^{t_1}/_{x_1}, \ldots, ^{t_n}/_{x_n}\}$ where t_i are the deducible subterms of ϕ. When $\overline{\phi}^{\phi} = \phi$, we say that a frame ϕ contains all its deducible subterms.

Example 9 *Consider the frame* $\phi = \nu n_2, n_3.\{^{\mathsf{enc}(\langle n_1 \oplus n_2, n_3\rangle, n_4)}/_{x_1}\}$ *given in Example 7. We have that*

$$\overline{\phi}^{\phi} = \nu n_2, n_3.\{^{\mathsf{enc}(\langle n_1 \oplus n_2, n_3\rangle, n_4)}/_{x_1}, ^{n_1 \oplus n_2}/_{x_2}, ^{n_2}/_{x_3}, ^{n_3}/_{x_4}, ^{n_1}/_{x_5}, ^{n_4}/_{x_6}, ^{0}/_{x_7}\}.$$

The following lemma ensures that extending frames preserves static equivalence.

Lemma 8 *Let* ϕ_1 *and* ϕ_2 *be two frames such that* $dom(\phi_1) = dom(\phi_2)$*. For any frame* ψ *such that* $dom(\psi) = dom(\phi_1)$*, we have that*

$$\overline{\phi_2}^{\psi} \models \mathsf{Eq}_{\mathsf{E}}(\overline{\phi_1}^{\psi}) \text{ if and only if } \phi_2 \models \mathsf{Eq}_{\mathsf{E}}(\phi_1).$$

In particular, we deduce that $\phi_1 \approx_{\mathsf{E}} \phi_2$ if and only if $\overline{\phi_1}^{\phi_2} \approx_{\mathsf{E}} \overline{\phi_2}^{\phi_2}$. Since $\overline{\phi_1}^{\phi_2}$ may not contain all its deducible subterms, we need to extend again the frames with the deducible subterms of $\overline{\phi_1}^{\phi_2}$. However, $\overline{(\overline{\phi_2}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})}$ might not contains its deducible subterms anymore. Lemma 9 states that actually, extending a frame preserves the property of containing all its deducible subterms. The proof of this lemma relies on the locality lemma (Lemma 6) stated in Section 4.

Lemma 9 *Let* ϕ *be a frame such that* $\overline{\phi}^{\phi} = \phi$ *and* ψ *be any frame such that* $dom(\psi) = dom(\phi)$*. Let* $\phi' = \overline{\phi}^{\psi}$*. We have that* ϕ' *contains all its deducible subterms, i.e.* $\overline{\phi'}^{\phi'} = \phi'$*.*

Thanks to Lemma 8, we deduce that deciding whether $\phi_1 \approx_{\mathsf{E}} \phi_2$ is thus equivalent to deciding whether $\overline{(\overline{\phi_1}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})} \approx_{\mathsf{E}} \overline{(\overline{\phi_2}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})}$ where $\overline{(\overline{\phi_1}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})}$ and $\overline{(\overline{\phi_2}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})}$ contain all their deducible subterms.

Computing $\overline{\phi}^{\psi}$. To compute $\overline{\phi}^{\psi}$, we not only need to compute that the set of deducible subterms of ψ but for each deducible subterm T of ψ, we need to compute a recipe ζ_T such that $(\zeta_T =_{\mathsf{E}} T)\psi$. Such a recipe can usually be deduced from the decision algorithm applied to $\psi \vdash_{\mathsf{E}} T$ [2]. However, if it is not the case, once we know that $\psi \vdash_{\mathsf{E}} T$ (using the decision algorithm), we can enumerate all the recipes until we find ζ such that $(\zeta_T =_{\mathsf{E}} T)\psi$.

5.2 Step 2: Checking for equalities in $\mathsf{Eq}_{\mathsf{E}_i}$

Checking for $\phi \approx_{\mathsf{E}} \psi$ is equivalent to checking for $\phi \models \mathsf{Eq}_{\mathsf{E}}(\psi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}}(\phi)$. We show that checking for $\psi \models \mathsf{Eq}_{\mathsf{E}}(\phi)$ can actually be done using only equalities in E_1 and E_2.

Proposition 1 *Let ϕ and ψ be two frames such that $\overline{\phi}^{\phi} = \phi$. We have that $\psi \models \mathsf{Eq}_{\mathsf{E}}(\phi)$ if and only if $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$.*

It is straightforward that $\psi \models \mathsf{Eq}_{\mathsf{E}}(\phi)$ implies $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$. The converse is more difficult. We first introduce some ordering on pair of terms. We have $(M, N) < (M', N')$ if

$$(\max(|M|, |N|), |M| + |N|) <_{lex} (\max(|M'|, |N'|), |M'| + |N'|)$$

where $<_{lex}$ is the lexicographic order. Now, assuming that $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$, we show by induction on the order on (M, N) that $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$ implies $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\psi)$. The key lemma for the induction step is as follows.

Lemma 10 *Let ϕ be a frame such that $\overline{\phi}^{\phi} = \phi$ and ψ be a frame such that $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$. Let $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$ and assume that for all terms M', N' such that $(M', N') < (M, N)$, we have that*

$$(M' =_{\mathsf{E}} N')\phi \Rightarrow (M' =_{\mathsf{E}} N')\psi.$$

Let $\phi = \nu\tilde{n}.\sigma$ such that $(fn(M) \cup fn(N)) \cap \tilde{n} = \emptyset$. If there exists $\zeta \in St(M)$ such that $\mathsf{sign}(\zeta\sigma) \neq \mathsf{sign}(\zeta\sigma\downarrow)$, then there exists M_1 such that $|M_1| < |M|$, $(M =_{\mathsf{E}} M_1)\phi$ and $(M =_{\mathsf{E}} M_1)\psi$.

5.3 Step 3: Abstraction of alien subterms

Since ψ and ϕ are built on Σ (and not on Σ_i), we cannot check whether $\psi \approx_{\mathsf{E}_i} \phi$ using the decision algorithm for $\approx_{\mathsf{E}_i}$. We show however that we can simply abstract the alien subterms by fresh names.

Lemma 11 *Let ϕ and ψ be two frames built on Σ and in normal form. Let $F_2 = \{N \in St(\phi \cup \psi) \mid \mathsf{sign}(N) = \Sigma_2\}$, $\tilde{n}_{F_2}$ be a set of names, distinct from the names occurring in ϕ and ψ, of same cardinality as F_2 and $\rho_2 : F_2 \to \tilde{n}_F$ a replacement. We have that*

$$\phi \models \mathsf{Eq}_{\mathsf{E}_1}(\psi) \text{ if and only if } \nu\tilde{n}_{F_2}.\phi^{\rho_2} \models \mathsf{Eq}_{\mathsf{E}_1}(\nu\tilde{n}_{F_2}.\psi^{\rho_2})$$

A similar result holds when inverting the indices 1 and 2.

5.4 Combination algorithm for static equivalence

To sum up, checking for $\phi_1 \approx_{\mathsf{E}} \phi_2$ is performed in two steps:

1. Computing $\phi_1' = \overline{(\overline{\phi_1}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})}$ and $\phi_2' = \overline{(\overline{\phi_2}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})}$.

2. checking for $\nu\tilde{n}_{F_2}.(\phi'_1)^{\rho_2} \approx_{\mathsf{E}_1} \nu\tilde{n}_{F_2}.(\phi'_2)^{\rho_2}$ and $\nu\tilde{n}_{F_1}.(\phi'_1)^{\rho_1} \approx_{\mathsf{E}_2} \nu\tilde{n}_{F_1}.(\phi'_2)^{\rho_1}$.

Complexity. The complexity of the procedure mostly depends on the complexity of computing ϕ'_1 and ϕ'_2 and on their size. In particular, it depends on the time for computing recipes and on their size. Assume that

- $\phi \vdash_{\mathsf{E}} M$ can be decided in $f_3(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$,
- a recipe ζ such that $(\zeta =_{\mathsf{E}} M)\phi$ can be computed in $f_4(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$ and that we control the size of the recipe $t_{\mathsf{dag}}(\zeta) \leq f_5(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$
- $\phi \approx_{\mathsf{E}_i} \psi$ can be decided in $f_i(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$ for $i \in \{1, 2\}$.

Then it is easy to check that $\phi \approx_{\mathsf{E}} \psi$ can be decided in time polynomial in the $f_i(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$ with $i \in \{1, \ldots, 5\}$. In particular, if the f_i are polynomial, $\approx_{\mathsf{E}}$ is decidable in polynomial time.

6 Application to new decidability results

Deduction and static equivalence are decidable in polynomial time (in the DAG-size of the inputs) for any convergent subterm theory [2]. A convergent subterm theory is an equational theory induced by a finite set of equations of the form $u = v$ where v is a subterm of u or v is a constant and such that the associate rewriting system is convergent. For example, $\mathsf{E}_{\mathsf{enc}}$ is a convergent subterm theory. From [4], we also know that deduction and static equivalence are decidable in polynomial time for the equational theory $\mathsf{E}_{\mathsf{xor}}$ of the exclusive or. Applying Theorems 1 and 2, we get the following new decidability result.

Proposition 2 *Let* E *be a convergent subterm theory. Deduction and static equivalence are decidable in polynomial time for* $\mathsf{E} \cup \mathsf{E}_{\mathsf{xor}}$.

Since deduction and static equivalence are also decidable for the theory of blind signature and the theory of associativity [4], we get that deduction and static equivalence are decidable for any combination of these theories.

As further work, we consider extending our combination result for non disjoint theories. This would allow us to consider challenging theories like modular exponentiation or simply Diffie-Hellman. We might use for example a notion of hierarchy between theories like in [11].

References

[1] M. Abadi, M. Baudet, and B. Warinschi. Guessing attacks and the computational soundness of static equivalence. In *Proceedings of the 9th International Conference on Foundations of Software Science and Computation Structures (FOSSACS'06)*, pages 398–412, 2006.

[2] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. In *Proceedings of the 31st International Colloquium on Automata, Languages, and Programming (ICALP'04)*, volume 3142 of *LNCS*, pages 46–58, Turku (Finland), 2004. Springer-Verlag.

[3] M. Abadi and V. Cortier. Deciding knowledge in security protocols under (many more) equational theories. In *Proceedings of the 18th IEEE Computer Security Foundations Workshop (CSFW'05)*, pages 62–76, Aix-en-Provence (France), 2005. IEEE Comp. Soc. Press.

[4] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 387(1-2):2–32, November 2006.

[5] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proceedings of the 28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115. ACM, 2001.

[6] F. Baader and K. U. Schulz. Unification in the union of disjoint equational theories: Combining decision procedures. *Journal of Symbolic Computation*, 21(2):211–243, 1996.

[7] M. Baudet, V. Cortier, and S. Kremer. Computationally sound implementations of equational theories against passive adversaries. In *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *LNCS*, pages 652–663, Lisboa (Portugal), 2005. Springer-Verlag.

[8] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with XOR. In *Proceedings of 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03)*, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.

[9] Y. Chevalier and M. Rusinowitch. Combining intruder theories. In *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *LNCS*, pages 639–651, Lisbon (Portugal), 2005. Springer.

[10] Y. Chevalier and M. Rusinowitch. Combining intruder theories. Technical Report 5495, INRIA, 2005. http://www.inria.fr/rrrt/rr-5495.html.

[11] Y. Chevalier and M. Rusinowitch. Hierarchical combination of intruder theories. In *Proceedings of the 17th International Conference on Rewriting Techniques and Applications, (RTA'06)*, volume 4098 of *LNCS*, pages 108–122, Seattle (WA), 2006. Springer.

[12] H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *Proceedings of 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03)*, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.

[13] S. Delaune. Easy intruder deduction problems with homomorphisms. *Information Processing Letters*, 97(6):213–218, Mar. 2006.

[14] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In *Handbook of Theoretical Computer Science*, volume B, chapter 6. Elsevier, 1990.

[15] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of Abelian groups with distributive encryption. *Information and Computation*, 2007. To appear.

[16] Y. Lakhnech, L. Mazaré, and B. Warinschi. Soundness of symbolic equivalence for modular exponentiation. In *Proceedings of the Second Workshop on Formal and Computational Cryptography (FCC'06)*, pages 19–23, Venice, Italy, July 2006.

[17] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *Proceedings of the 2nd International Workshop on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'96)*, volume 1055 of *LNCS*, pages 147–166, Berlin (Germany), 1996. Springer-Verlag.

[18] J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS'01)*. ACM Press, 2001.

[19] L. C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6(1-2):85–128, 1998.

[20] M. Rusinowitch and M. Turuani. Protocol insecurity with a finite number of sessions, composed keys is NP-complete. *Theoretical Computer Science*, 1-3(299):451–475, 2003.

[21] M. Schmidt-Schauß. Unification in a combination of arbitrary disjoint equational theories. *Journal of Symbolic Computation*, 8(1/2):51–99, 1989.

A Proofs of Section 4

Lemma 6 (locality lemma) *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and M be a ground term built on Σ and in normal form. If $\phi \vdash_{\mathsf{E}} M$ then there exists a term ζ on Σ such that*

- *$fn(\zeta) \cap \tilde{n} = \emptyset$ and $\zeta\sigma =_{\mathsf{E}} M$,*
- *for all $\zeta' \in St(\zeta)$, we have $\zeta'\sigma\downarrow \in St(\phi, M) \cup \Sigma_0$.*
  Moreover, if $\mathsf{sign}(\zeta') \neq \mathsf{sign}(\zeta'\sigma\downarrow)$, we have $\zeta'\sigma\downarrow \in St(\phi) \cup \Sigma_0$.

Proof. By Lemma 1, we know that there exists a term built on Σ satisfying the first condition. We choose one, say that ζ'_M, whose size is minimal. Let ζ_M be the term obtained from ζ'_M after replacing every occurrence of a name $n \notin St(\phi, M)$ by n_{min}. Since E is stable under substitution of names, from the fact that $\zeta'_M\sigma =_{\mathsf{E}} M$, we easily deduce that $\zeta_M\sigma =_{\mathsf{E}} M$. Now, we establish (by induction) that such a ζ_M satisfies the second condition.

Base case: ζ_M is a name, a variable or a term built over Σ_1 (resp. Σ_2) only. In such a case, we easily conclude since $St(\zeta_M) = \{\zeta_M\}$.

Induction step: There exist $\zeta^0, \zeta_1, \ldots, \zeta_\ell$ such that

- $\zeta = \zeta^0[\zeta_1, \ldots, \zeta_\ell]$,
- ζ^0 is built on Σ_i and in the remainder of the proof we assume w.l.o.g. that $i = 1$,
- $\zeta_1, \ldots, \zeta_\ell$ are built on Σ and $\mathsf{sign}(\zeta_i) \neq \Sigma_1$.

By induction hypothesis, we know that for all $i \leq \ell$, for all $\zeta' \in St(\zeta_i)$, we have $\zeta'\sigma\downarrow \in St(\phi, \zeta_i\sigma\downarrow) \cup \Sigma_0$. To conclude that $\zeta'\sigma\downarrow \in St(\phi, M) \cup \Sigma_0$ for any $\zeta' \in St(\zeta)$, it is sufficient to show that for all $i \leq \ell$ we have $\zeta_i\sigma\downarrow \in St(\phi, M) \cup \Sigma_0$.

- If $\mathsf{sign}(\zeta_i) = \bot$, then we have $\zeta_i\sigma\downarrow \in St(\phi) \cup \Sigma_0$.
- If $\mathsf{sign}(\zeta_i) = \Sigma_2$ and $\mathsf{sign}(\zeta_i\sigma\downarrow) \neq \Sigma_2$, then we conclude that $\zeta_i\sigma\downarrow \in St(\phi) \cup \Sigma_0$ thanks to the induction hypothesis.
- Now, we assume that $\mathsf{sign}(\zeta_i) = \Sigma_2$ and $\mathsf{sign}(\zeta_i\sigma\downarrow) = \Sigma_2$. We distinguish several cases.
  1. $\zeta_i\sigma\downarrow \in St(M) \cup \Sigma_0$. In such a case, we easily conclude.
  2. $\zeta_i\sigma\downarrow \in St(\zeta_j\sigma\downarrow)$ for some j such that $\mathsf{sign}(\zeta_j\sigma\downarrow) = \Sigma_1$. By induction hypothesis, since $\mathsf{sign}(\zeta_j) = \Sigma_2 \neq \mathsf{sign}(\zeta_j\sigma\downarrow)$, we have $\zeta_j\sigma\downarrow \in St(\phi) \cup \Sigma_0$. Thus $\zeta_i\sigma\downarrow \in St(\phi) \cup \Sigma_0$.
  3. Otherwise, we show that we can build a recipe ζ'_M of M smaller than ζ_M. Let $\Delta = \{j \in \{1, \ldots, \ell\} \mid \zeta_j\sigma\downarrow = \zeta_i\sigma\downarrow\}$. Note that $\Delta \neq \emptyset$ since $i \in \Delta$. Let

$\zeta'_M = \zeta^0[\zeta'_1, \ldots, \zeta'_\ell]$ where ζ'_j is equal to n_{min} if $j \in \Delta$ and to ζ_j otherwise. Note that $|\zeta'_M| < |\zeta_M|$. Lastly, we have that ζ'_M is a recipe of M. Indeed

$$\begin{array}{lcll} \zeta'_M\sigma\downarrow & = & \zeta^0[\zeta'_1\sigma\downarrow, \ldots, \zeta'_\ell\sigma\downarrow]\downarrow & \\ & = & ((\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow])\delta_{(\zeta_i\sigma)\downarrow, n_{min}})\downarrow & \text{since } \zeta_i\sigma\downarrow \notin St(\zeta_j\sigma\downarrow) \text{ for } j \notin \Delta \\ & = & ((\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow])\downarrow\delta_{(\zeta_i\sigma)\downarrow, n_{min}})\downarrow & \text{thanks to Lemma 5} \\ & = & M\delta_{(\zeta_i\sigma)\downarrow, n_{min}}\downarrow = M & \text{since } \zeta_i\sigma \notin St(M) \end{array}$$

Moreover, assume $\mathsf{sign}(\zeta_M) \neq \mathsf{sign}(\zeta_M\sigma\downarrow)$. Since we have that $\mathsf{sign}(\zeta_M) = \mathsf{sign}(\zeta^0[\zeta'_1\sigma\downarrow, \ldots, \zeta'_\ell\sigma\downarrow])$ and $\zeta^0[\zeta'_1\sigma\downarrow, \ldots, \zeta'_\ell\sigma\downarrow]\downarrow = \zeta_M\sigma\downarrow$ then applying Lemma 3, we get $\zeta_M\sigma\downarrow \in \Sigma_0 \cup Fct(\zeta^0[\zeta'_1\sigma\downarrow, \ldots, \zeta'_\ell\sigma\downarrow])$. For each $1 \leq i \leq \ell$, if $\mathsf{sign}(\zeta_i) \neq \mathsf{sign}(\zeta_i\sigma\downarrow)$, we have seen that $\zeta_i\sigma\downarrow \in St(\phi) \cup \Sigma_0$. We deduce that $\zeta_M\sigma\downarrow \in \Sigma_0 \cup St(\phi) \cup \{\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow\}$. By minimality of ζ_M, there exists no ζ_i such that $\zeta_M\sigma\downarrow = \zeta_i\sigma\downarrow$. This allows us to conclude. □

Lemma 7 *Let ϕ be a frame and M be a ground term built on Σ and in normal form. Let $F_2 = \{N \mid N \in St(\phi, M)$ and $\mathsf{sign}(N) = \Sigma_2\}$, $\tilde{n}_{F_2}$ be a set of names, distinct from the names occurring in ϕ and M, of same cardinality as F_2 and $\rho_2 : F_2 \to \tilde{n}_{F_2}$ be a bijection. We have that*

$$\phi \vdash_{\mathsf{E}_1} M \text{ if and only if } \nu\tilde{n}_{F_2}.(\phi \vdash_{\mathsf{E}_1} M)^{\rho_2}.$$

Proof. ($\Rightarrow$) Let $\phi = \nu\tilde{n}.\sigma$. By Lemma 1, we know that there exists a term ζ on Σ_1 such that $fn(\zeta) \cap \tilde{n} = \emptyset$ and $\zeta\sigma =_{\mathsf{E}_1} M$. Hence, we know that $\zeta\sigma\downarrow = M$. We have to show that there exists a term ζ' on Σ_1 such that $fn(\zeta') \cap (\tilde{n} \cup \tilde{n}_{F_2}) = \emptyset$ and $\zeta'\sigma^{\rho_2} =_{\mathsf{E}_1} M^{\rho_2}$. W.l.o.g. we can assume that $fn(\zeta) \cap \tilde{n}_{F_2} = \emptyset$. Let us show that the term ζ satisfies the required conditions. Either $\mathsf{sign}(M^{\rho_2}) = \bot$ or $\mathsf{sign}(M^{\rho_2}) = \Sigma_1$. In this last case, since M is in normal form, applying Lemma 4, we get $M^{\rho_2}\downarrow = M^{\rho_2}\downarrow_{\mathsf{E}_1}$. In both cases, we get

$$M^{\rho_2}\downarrow =_{\mathsf{E}_1} M^{\rho_2} \tag{1}$$

Since $\mathsf{sign}((\zeta\sigma)^{\rho_2}) \neq \Sigma_2$ and $(\zeta\sigma)^{\rho_2}$ does not contain subterms of sign Σ_2 anymore, all its factor are in normal form thus we can apply again Lemma 4, yielding to $(\zeta\sigma)^{\rho_2}\downarrow = (\zeta\sigma)^{\rho_2}\downarrow_{\mathsf{E}_1}$. We deduce

$$(\zeta\sigma)^{\rho_2}\downarrow =_{\mathsf{E}_1} (\zeta\sigma)^{\rho_2} \tag{2}$$

Since all the factors of $\zeta\sigma$ are in normal form, we can apply Lemma 5

$$(\zeta\sigma)^{\rho_2}\downarrow = (\zeta\sigma)\downarrow^{\rho_2}\downarrow \tag{3}$$

By equality (3) and the fact that $(\zeta\sigma)\downarrow = M$, we get $(\zeta\sigma)^{\rho_2}\downarrow = M^{\rho_2}\downarrow$. Using equalities (1) and (2), we deduce that $(\zeta\sigma)^{\rho_2} =_{\mathsf{E}_1} M^{\rho_2}$. Now, since ζ is a term built on Σ_1, we have that $(\zeta\sigma)^{\rho_2} = \zeta(\sigma^{\rho_2})$ (syntactically). This allows us to conclude.

($\Leftarrow$) By Lemma 1, we know that there exists a term ζ on Σ_1 such that $fn(\zeta) \cap (\tilde{n} \cup \tilde{n}_{F_2}) = \emptyset$ and $\zeta\sigma^{\rho_2} =_{\mathsf{E}_1} M^{\rho_2}$. We show that $fn(\zeta) \cap \tilde{n} = \emptyset$ (obvious) and $\zeta\sigma =_{\mathsf{E}_1} M$. Since $\zeta\sigma^{\rho_2} =_{\mathsf{E}_1} M^{\rho_2}$

and since E_1 is closed under substitution of names, we deduce that $(\zeta\sigma^{\rho_2})^{\rho_2^{-1}} =_{\mathsf{E}_1} (M^{\rho_2})^{\rho_2^{-1}}$. We have $(M^{\rho_2})^{\rho_2^{-1}} = M$ and $(\zeta\sigma^{\rho_2})^{\rho_2^{-1}} = \zeta((\sigma^{\rho_2})^{\rho_2^{-1}}) = \zeta\sigma$ since $\tilde{n}_{F_2} \notin fn(\zeta)$. This allows us to conclude that $\zeta\sigma =_{\mathsf{E}_1} M$. □

We prove the following claim, that shows the correction of the saturation algorithm.

Claim: ϕ^* contains exactly the set $d(St(\phi, M))$ of all deducible subterms of $St(\phi, M)$.

$\phi^* \subseteq d(St(\phi, M))$. We show by induction on k that $\phi_k \subseteq d(St(\phi, M))$. The base case $\phi_0 \subseteq d(St(\phi, M))$ is obvious. Assume now that for every $U \in \phi_k$, U is deducible, that is $\phi \vdash_{\mathsf{E}_1 \cup \mathsf{E}_2} U$. We have $\phi_{k+1} = \phi_k \cup \{T\}$ with $T \in St(\phi, M)$ such that (w.l.o.g.) $\nu\tilde{n}_{F_2}.(\phi_k \vdash_{\mathsf{E}_1} T)^{\rho_2}$. Applying Lemma 7 we get that $\phi_k \vdash_{\mathsf{E}_1} T$ thus $\phi \vdash_{\mathsf{E}_1 \cup \mathsf{E}_2} T$ and $\phi_{k+1} \subseteq d(St(\phi, M))$.

$d(St(\phi, M)) \subseteq \phi^*$. Let $T \in St(\phi, M)$ be some deducible term, that is $\phi \vdash_{\mathsf{E}_1 \cup \mathsf{E}_2} T$. Lemma 6 ensures that there exists ζ such that $fn(\zeta) \cap \tilde{n} = \emptyset$, $(\zeta\sigma)\downarrow = T$ and for all $\zeta' \in St(\zeta)$, we have $\zeta'\sigma\downarrow \in St(\phi, M) \cup \Sigma_0$. We show by induction on $|\zeta|$ that $T \in \phi^*$.

Base case. If $|\zeta| \leq 1$ then either ζ is a name or a variable and we easily conclude, or ζ is built on Σ_1 or Σ_2. We assume w.l.o.g. that ζ is built on Σ_1. From Lemma 4 $(\zeta\sigma)\downarrow = T$ implies that $(\zeta\sigma)\downarrow_{\mathsf{E}_1} = T$ thus $\phi \vdash_{\mathsf{E}_1} T$. Applying Lemma 7, we get that $\nu\tilde{n}_{F_2}.(\phi \vdash_{\mathsf{E}_1} T)^{\rho_2}$ thus $T \in \phi^*$.

Induction step. Assume $\zeta = \zeta_0[\zeta_1, \ldots, \zeta_k]$. We have $\zeta_i\sigma\downarrow \in St(\phi, M) \cup \Sigma_0$ for $1 \leq i \leq k$. Since $|\zeta_i| \leq |\zeta|$, applying the induction hypothesis, we deduce that $\zeta_i\sigma\downarrow \in \phi^*$. W.l.o.g. we assume that $\mathsf{sign}(\zeta_0) = \Sigma_1$. Thus $\phi^* \vdash_{\mathsf{E}_1} \zeta\sigma\downarrow = T$. Applying Lemma 7, we get that $\nu\tilde{n}_{F_2}.(\phi \vdash_{\mathsf{E}_1} T)^{\rho_2}$ thus $T \in \phi^*$. □

B Proofs of Section 5

B.1 Adding deducible subterms

Lemma 8 *Let ϕ_1 and ϕ_2 be two frames such that $dom(\phi_1) = dom(\phi_2)$. For any frame ψ such that $dom(\psi) = dom(\phi_1)$, we have that*

$$\overline{\phi_2}^{\psi} \models \mathsf{Eq}_{\mathsf{E}}(\overline{\phi_1}^{\psi}) \text{ if and only if } \phi_2 \models \mathsf{Eq}_{\mathsf{E}}(\phi_1).$$

Proof. ($\Rightarrow$) Assume that $\overline{\phi_2}^{\psi} \models \mathsf{Eq}_{\mathsf{E}}(\overline{\phi_1}^{\psi})$ and consider $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi_1)$. As $(\overline{\phi_1}^{\psi})|_{dom(\phi_1)} = \phi_1$ and $(\overline{\phi_2}^{\psi})|_{dom(\phi_1)} = \phi_2$, it follows that $(M =_{\mathsf{E}} N)\overline{\phi_1}^{\psi}$, thus $(M =_{\mathsf{E}} N)\overline{\phi_2}^{\psi}$, that is $(M =_{\mathsf{E}} N)\phi_2$.

($\Leftarrow$) Conversely, assume that $\phi_2 \models \mathsf{Eq}_{\mathsf{E}}(\phi_1)$ and consider $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\overline{\phi_1}^{\psi})$. Let $\phi_1 = \nu\tilde{n}_1.\sigma_1$ and $\phi_2 = \nu\tilde{n}_2.\sigma_2$ such that $(fn(M) \cup fn(N)) \cap (\tilde{n}_1 \cup \tilde{n}_2) = \emptyset$. We have that $\overline{\phi_1}^{\psi} = \phi_1 \cup \{^{t_1}/_{x_1}, \ldots, ^{t_n}/_{x_n}\}$ with $\zeta_i\sigma_1\downarrow = t_i$. Let $M' = M\theta$ and $N' = N\theta$ where $\theta = \{^{\zeta_1}/_{x_1}, \ldots, ^{\zeta_n}/_{x_n}\}$. Since we have that $\zeta_i\sigma_1 =_{\mathsf{E}} x_i\overline{\sigma_1}^{\psi}$, we deduce that $M'\sigma_1 =_{\mathsf{E}} M\overline{\sigma_1}^{\psi}$ and $N'\sigma_1 =_{\mathsf{E}} N\overline{\sigma_1}^{\psi}$, that is $(M' =_{\mathsf{E}} N')\phi_1$. Since $\phi_2 \models \mathsf{Eq}_{\mathsf{E}}(\phi_1)$, we have $(M' =_{\mathsf{E}} N')\phi_2$. As we also have that $M'\sigma_2 =_{\mathsf{E}} M\overline{\sigma_2}^{\psi}$ and $N'\sigma_2 =_{\mathsf{E}} N\overline{\sigma_2}^{\psi}$ (since $\zeta_i\sigma_2 =_{\mathsf{E}} x_i\overline{\sigma_2}^{\psi}$), we conclude that $(M =_{\mathsf{E}} N)\overline{\phi_2}^{\psi}$. □

Lemma 9 *Let ϕ be a frame such that $\overline{\phi}^{\phi} = \phi$ and ψ be any frame such that $dom(\psi) = dom(\phi)$. Let $\phi' = \overline{\phi}^{\psi}$. We have that ϕ' contains all its deducible subterms, i.e. $\overline{\phi'}^{\phi'} = \phi'$.*

Proof. Let $\phi = \nu\tilde{n}.\sigma$ and $\psi = \nu\tilde{n}.\sigma'$ for some sequence of names $\tilde{n}$ and some substitutions σ and σ'. By construction, we have that $\phi' = \phi \cup \{^{\zeta_1\sigma\downarrow}/_{x_1}, \ldots, ^{\zeta_n\sigma\downarrow}/_{x_n}\}$ where ζ_i are such that $\zeta_i\sigma'\downarrow \in St(\psi)$. We assume w.l.o.g. that for every i, we have that ζ_i satisfies the hypothesis of the Lemma 6 (locality lemma), *i.e.* for all $\zeta' \in St(\zeta_i)$, we have that $\zeta'\sigma'\downarrow \in St(\psi)$. Moreover, we also assume that terms have been introduced in the frame obeying the following ordering condition: Let ζ_i and ζ_j be two terms such that $\zeta_i\sigma'\downarrow \in St(\psi)$ and $\zeta_j\sigma'\downarrow \in St(\psi)$. If $\zeta_i \in St(\zeta_j)$ then $i < j$. Now, to conclude, it remains to show that for every i $(1 \leq i \leq n)$ we have

$$St(\zeta_i\sigma\downarrow) \subseteq St(\phi) \cup \{^{\zeta_1\sigma\downarrow}/_{x_1}, \ldots, ^{\zeta_i\sigma\downarrow}/_{x_i}\}. \qquad (\star)$$

Let i_0 be the first indice for which condition $(\star)$ is violated. Hence, there exists M such that $M \in St(\zeta_{i_0}\sigma\downarrow)$ and $M \notin St(\phi) \cup \{^{\zeta_1\sigma\downarrow}/_{x_1}, \ldots, ^{\zeta_{i_0}\sigma\downarrow}/_{x_{i_0}}\}$. We have that $\zeta_{i_0} = \zeta^0[\zeta^1, \ldots, \zeta^\ell]$ where $\zeta^1, \ldots, \zeta^\ell$ are the factors of ζ_i. By construction, we know that condition $(\star)$ is satisfied for $\zeta^1, \ldots, \zeta^\ell$. Hence, we have that $St(\zeta^j\sigma\downarrow) \subseteq St(\phi) \cup \{^{\zeta_1\sigma\downarrow}/_{x_1}, \ldots, ^{\zeta_{i_0}\sigma\downarrow}/_{x_{i_0}}\}$ for any j such that $1 \leq j \leq \ell$.

We consider the term $\zeta^0[\zeta^1\sigma\downarrow, \ldots, \zeta^\ell\sigma\downarrow]$ and we have that its factors are in normal form. We can apply Lemma 3. Hence, we are in one of the two cases described below:

1. $\zeta_{i_0}\sigma\downarrow \in \Sigma_0 \cup Fct(\zeta^0[\zeta^1\sigma\downarrow, \ldots, \zeta^\ell\sigma\downarrow]) \subseteq St(\phi) \cup St(\{\zeta^1\sigma\downarrow, \ldots, \zeta^\ell\sigma\downarrow\})$.
2. $Fct(\zeta_{i_0}\sigma\downarrow) \subseteq \Sigma_0 \cup Fct(\zeta^0[\zeta^1\sigma\downarrow, \ldots, \zeta^\ell\sigma\downarrow]) \subseteq St(\phi) \cup St(\{\zeta^1\sigma\downarrow, \ldots, \zeta^\ell\sigma\downarrow\})$.

In both cases, we obtain a contradiction with the fact that i_0 is the first indice for which condition $(\star)$ is violated. □

B.2 Proof of Proposition 1

Lemma 10 *Let ϕ be a frame such that $\overline{\phi}^{\phi} = \phi$ and ψ be a frame such that $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$. Let $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$ and assume that for all terms M', N' such that $(M', N') < (M, N)$, we have that*

$$(M' =_{\mathsf{E}} N')\phi \Rightarrow (M' =_{\mathsf{E}} N')\psi.$$

Let $\phi = \nu\tilde{n}.\sigma$ such that $(fn(M) \cup fn(N)) \cap \tilde{n} = \emptyset$. If there exists $\zeta \in St(M)$ such that $\mathsf{sign}(\zeta\sigma) \neq \mathsf{sign}(\zeta\sigma\downarrow)$, then there exists M_1 such that $|M_1| < |M|$, $(M =_{\mathsf{E}} M_1)\phi$ and $(M =_{\mathsf{E}} M_1)\psi$.

Proof. Let $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$ and $\phi = \nu\tilde{n}.\sigma$ such that $(fn(M) \cup fn(N)) \cap \tilde{n} = \emptyset$. W.l.o.g. we assume $|M| \geq |N|$. We prove this result by induction on $|M|$. Note that when $|M| = 0$, *i.e.* M is a variable or a nonce, the result is obvious since $(M, N) \in \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ or $(M, N) \in \mathsf{Eq}_{\mathsf{E}_2}(\phi)$. Now, we know that that there exists $\zeta^0, \zeta_1, \ldots, \zeta_\ell$ such that:

- $M = \zeta^0[\zeta_1, \ldots, \zeta_\ell]$,
- ζ^0 is built on Σ_i and in the remainder of the proof we assume w.l.o.g. that $i = 1$. Moreover, we know that ζ^0 is not reduced to a variable or a name.
- $\zeta_1, \ldots, \zeta_\ell$ are built on Σ and $\mathsf{sign}(\zeta_i) \neq \Sigma_1$.

We distinguish three cases.

First case: There exists i $(1 \leq i \leq \ell)$ and $\zeta' \in St(\zeta_i)$ such that $\mathsf{sign}(\zeta'\sigma) \neq \mathsf{sign}(\zeta'\sigma\downarrow)$. By induction hypothesis we know that there exists ζ_i' such that $|\zeta_i'| < |\zeta_i|$, $(\zeta_i' =_{\mathsf{E}} \zeta_i)\phi$ and $(\zeta_i' =_{\mathsf{E}} \zeta_i)\psi$. Let $M_1 = \zeta^0[\zeta_1, \ldots, \zeta_i', \ldots, \zeta_\ell]$. We have that $|M_1| < |M|$, $(M_1 =_{\mathsf{E}} M)\phi$ and $(M_1 =_{\mathsf{E}} M)\psi$.

Second case: There exists ζ_i such that $\mathsf{sign}(\zeta_i) = \Sigma_2$ and $\zeta_i\sigma\downarrow \in St(\phi)$. This means that $\zeta_i\sigma\downarrow$ is a deducible subterm. Thus there exists $x \in dom(\phi)$ such that $(x =_{\mathsf{E}} \zeta_i)\phi$. Since $(\zeta_i, x) < (M, N)$, we deduce that $(\zeta_i =_{\mathsf{E}} x)\psi$. Let $M' = \zeta^0[\zeta_1, \ldots, x, \ldots, \zeta_\ell]$. We have that $|M'| < |M|$, $(M =_{\mathsf{E}} M')\phi$ and $(M =_{\mathsf{E}} M')\psi$.

Third case: We know that $\mathsf{sign}(\zeta_i\sigma) = \mathsf{sign}(\zeta_i\sigma\downarrow)$ for every i such that $1 \leq i \leq \ell$. Moreover, if $\mathsf{sign}(\zeta_i) \neq \bot$, we have that $\zeta_i\sigma\downarrow \notin St(\phi)$. In addition, since by hypothesis there exists $\zeta \in St(M)$ such that $\mathsf{sign}(\zeta\sigma) \neq \mathsf{sign}(\zeta\sigma\downarrow)$, we must have $\zeta = M$ thus $\mathsf{sign}(M\sigma) \neq \mathsf{sign}(M\sigma\downarrow)$.

Now, either (Case (a)) there is no ζ_i such that $\mathsf{sign}(\zeta_i) = \Sigma_2$ meaning that $M\sigma$ has all its factor in normal form, thus applying Lemma 3, we have $M\sigma\downarrow \in St(\phi) \cup \Sigma_0 \subseteq St(\phi)$ since $\overline{\phi}^{\phi} = \phi$.

- Either there exists $x \in dom(\phi)$ such that $(M =_{\mathsf{E}} x)\phi$. Thanks to Lemma 4, we deduce that $(M =_{\mathsf{E}_1} x)\phi$ and hence we have that $(M, x) \in \mathsf{Eq}_{\mathsf{E}_1}(\phi)$. Since $\psi \in \mathsf{Eq}_{\mathsf{E}_1}(\phi)$, we have also $(M =_{\mathsf{E}_1} x)\psi$, thus $(M =_{\mathsf{E}} x)\psi$. Let $M_1 = x$, we easily conclude.
- Or there exists $n \in \mathcal{N}$, such that $M\sigma\downarrow = n$. Thanks to Lemma 4, we have that $(M =_{\mathsf{E}_1} n)\phi$. Since $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$, we deduce that $(M =_{\mathsf{E}_1} n)\psi$ and hence $(M =_{\mathsf{E}} n)\psi$. Let $M_1 = n$, we easily conclude.

Otherwise (Case (b)), let $\Delta = \{\zeta_i\sigma\downarrow \mid \mathsf{sign}(\zeta_i) = \Sigma_2 \text{ and } 1 \leq i \leq \ell\}$. Let $t_1, \ldots, t_k$ be the elements of Δ ordered in such a way that if t_i is a syntactic subterm of t_j then $j < i$. Let $n_1, \ldots, n_k$ be some new nonces that do not appear in ϕ nor ψ. Let $\delta_i = \delta_{t_i, n_i}$ for every i such that $1 \leq i \leq k$.

By applying successively Lemma 5, we obtain

$$((\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow]\delta_1)\ldots\delta_k)\downarrow = (((M\sigma\downarrow)\delta_1\downarrow)\ldots)\delta_k\downarrow \tag{4}$$

Let $M' = \zeta^0[\zeta_1', \ldots, \zeta_\ell']$ where $\zeta_i' = \zeta_i$ if $\zeta_i\sigma\downarrow \notin \Delta$ and $\zeta_i' = n_j$ if $\zeta_i\sigma\downarrow = t_j$. We have that $((\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow]\delta_1)\ldots\delta_k) = \zeta^0[\zeta_1'\sigma\downarrow, \ldots, \zeta_\ell'\sigma\downarrow] =_{\mathsf{E}} M'\sigma$. In addition, since $\mathsf{sign}(\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow]) \neq \mathsf{sign}(M\sigma\downarrow)$ and $\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow]$ has all its factors in normal form, applying Lemma 3, we get $M\sigma\downarrow \in \Delta \cup St(\phi)$ (note that $\Sigma_0 \subseteq St(\phi)$). From the equality (4) we can deduce that

- either $M\sigma\downarrow = t_j$ for some t_j $(1 \leq j \leq k)$ and we have $(M' =_{\mathsf{E}} n_j)\phi$,
- or $M\sigma\downarrow \in St(\phi)$ and in such a case, we know that there exists $x \in dom(\phi)$ such that $M\sigma\downarrow = x\sigma$. Hence we have that $(M' =_{\mathsf{E}} x)\phi$.

In both case, we have obtain an equality in $\mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and thanks to the fact that $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$, we deduce that either $(M' =_{\mathsf{E}_1} n_j)\psi$ (Case 1) or $(M' =_{\mathsf{E}_1} x)\psi$ (Case 2). For every i such that $1 \leq i \leq k$, let $\Delta_i = \{\zeta_j \mid \zeta_j\sigma\downarrow = t_i \text{ and } 1 \leq j \leq \ell\}$ and let $\zeta^i \in \Delta_i$. We denote by δ' the following replacement:

$$\delta' = \{n_1 \mapsto \zeta^1\sigma'\downarrow, \ldots, n_k \mapsto \zeta^k\sigma'\downarrow\}.$$

Claim: For every i such that $1 \leq i \leq \ell$, we have that $(\zeta'_i\sigma'\downarrow)\delta' = \zeta_i\sigma'\downarrow$.
Indeed either $\zeta'_i = \zeta_i$ and we easily conclude. Otherwise we have that $\zeta'_i = n_p$ for some p such that $1 \leq p \leq k$ and we know that $(\zeta_i =_{\mathsf{E}} \zeta^p)\phi$. By induction hypothesis, we deduce that $(\zeta_i =_{\mathsf{E}} \zeta^p)\psi$. Hence, we have that $(\zeta'_i\sigma'\downarrow)\delta' = (n_p\sigma'\downarrow)\delta' = \zeta^p\sigma'\downarrow = \zeta_i\sigma'\downarrow$.

(Case 1) We have that $(M =_{\mathsf{E}} \zeta^j)\phi$. Note also that $|\zeta^j| < |M|$. Hence, it remains to show that $(M =_{\mathsf{E}} \zeta^j)\psi$. We have shown that $(M' =_{\mathsf{E}_1} n_j)\psi$, this means that $\zeta^0[\zeta'_1\sigma'\downarrow, \ldots, \zeta'_\ell\sigma'\downarrow] =_{\mathsf{E}} n_j$. Since E is closed under substitution of names, we have that $\zeta^0[(\zeta'_1\sigma'\downarrow)\delta', \ldots, (\zeta'_1\sigma'\downarrow)\delta'] =_{\mathsf{E}} \zeta^j\sigma'\downarrow$. Using our claim, we obtain that $\zeta^0[\zeta_1\sigma'\downarrow, \ldots, \zeta_\ell\sigma'\downarrow] =_{\mathsf{E}} \zeta^j\sigma'\downarrow$. Hence, we deduce that $(M =_{\mathsf{E}} \zeta^j)\psi$.

(Case 2) We have that $(M =_{\mathsf{E}} x)\phi$. Since $|x| < |M|$, it remains to show that $(M =_{\mathsf{E}} x)\psi$. We have shown that $(M' =_{\mathsf{E}_1} x)\psi$, this means that $\zeta^0[\zeta'_1\sigma'\downarrow, \ldots, \zeta'_\ell\sigma'\downarrow] =_{\mathsf{E}} x\sigma'$. Since E is closed under substitution of names, we have that $\zeta^0[(\zeta'_1\sigma'\downarrow)\delta', \ldots, (\zeta'_1\sigma'\downarrow)\delta'] =_{\mathsf{E}} x\sigma'\downarrow$. By using our claim, we obtain that $\zeta^0[\zeta_1\sigma'\downarrow, \ldots, \zeta_\ell\sigma'\downarrow] =_{\mathsf{E}} x\sigma'\downarrow$. Hence, we easily deduce that $(M =_{\mathsf{E}} x)\psi$. □

Proposition 1 *Let ϕ and ψ be two frames such that $\overline{\phi}^{\phi} = \phi$. We have that $\psi \models \mathsf{Eq}_{\mathsf{E}}(\phi)$ if and only if $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$.*

Proof. $(\Rightarrow)$ Since $\mathsf{Eq}_{\mathsf{E}_1}(\phi) \subseteq \mathsf{Eq}_{\mathsf{E}}(\phi)$ and $\mathsf{Eq}_{\mathsf{E}_2}(\phi) \subseteq \mathsf{Eq}_{\mathsf{E}}(\phi)$ and thanks to Lemma 4 we have that $\psi \models \mathsf{Eq}_{\mathsf{E}}(\phi)$ implies $\psi \models \mathsf{Eq}_{\mathsf{E}_i}(\phi)$ for $i \in \{1, 2\}$.

$(\Leftarrow)$ Conversely, let $\psi = \nu\tilde{n}.\sigma'$ be a frame such that $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$. Let $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$ and $\phi = \nu\tilde{n}.\sigma$ for some substitution σ. We prove, by induction on the size of (M, N), that $(M =_{\mathsf{E}} N)\psi$. We assume w.l.o.g. that M is such that $|M| \geq |N|$.

Base case: $|M|+|N| \leq 1$. This means that M and N are variables, names or terms built only on Σ_1 or Σ_2 and only M can satisfy $\mathsf{sign}(M) \neq \bot$. In such a case, either $(M, N) \in \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ or $(M, N) \in \mathsf{Eq}_{\mathsf{E}_2}(\phi)$ and we conclude by applying our hypothesis.

Induction step: We know that $|M| \geq 1$. This means that there exist $\zeta^0_M, \zeta^1_M, \ldots, \zeta^\ell_M$ such that

- $M = \zeta_M^0[\zeta_M^1, \ldots, \zeta_M^\ell]$,
- ζ_M^0 is built on Σ_i and in the remainder of the proof we will assume w.l.o.g. that $i = 1$,
- $\zeta_M^1, \ldots, \zeta_M^\ell$ are built on Σ and $\mathsf{sign}(\zeta_M^i) \neq \Sigma_1$ for $i \in \{1, \ldots, \ell\}$.

and we know also that there exist $\zeta_N^0, \zeta_N^1, \ldots, \zeta_N^p$ such that

- $N = \zeta_N^0[\zeta_N^1, \ldots, \zeta_N^p]$,
- ζ_N^0 is built on Σ_i and in the remainder of the proof we will assume that $\mathsf{sign}(\zeta_N^0) \neq 2$ since if $\mathsf{sign}(M\sigma) \neq \mathsf{sign}(N\sigma)$ we easily conclude, thanks to Lemma 10, by noticing that either $\mathsf{sign}(M\sigma) \neq \mathsf{sign}(M\sigma\downarrow)$ or $\mathsf{sign}(N\sigma) \neq \mathsf{sign}(N\sigma\downarrow)$.
- $\zeta_N^1, \ldots, \zeta_N^p$ are built on Σ and $\mathsf{sign}(\zeta_N^i) \neq \Sigma_1$ for $i \in \{1, \ldots, p\}$.

Note that the sets $\{\zeta_M^1, \ldots, \zeta_M^\ell\}$ and $\{\zeta_N^1, \ldots, \zeta_N^p\}$ might be empty.
We distinguish several cases.

Case 1: If there exists ζ_M^i (or ζ_N^i) such that $\mathsf{sign}(\zeta_M^i\sigma) \neq \mathsf{sign}(\zeta_M^i\sigma\downarrow)$. In such a case, we can apply Lemma 10 on ζ_M^i. We deduce that there exists U such that $|U| < |\zeta_M^i|$, $(U =_\mathsf{E} \zeta_M^i)\phi$ and $(U =_\mathsf{E} \zeta_M^i)\psi$. Let $M' = \zeta_M^0[\zeta_M^1, \ldots, U, \ldots, \zeta_M^\ell]$. We have that $(M =_\mathsf{E} M')\phi$ and $(M =_\mathsf{E} M')\psi$. Applying our induction hypothesis on (M', N), we obtain $(M' =_\mathsf{E} N)\psi$. Thus we deduce that $(M =_\mathsf{E} N)\psi$.

Case 2: If there exists ζ_M^i (or ζ_N^i) such that $\mathsf{sign}(\zeta_M^i) = \Sigma_2$ and $\zeta_M^i\sigma\downarrow \in St(\phi)$. This means that $\zeta_M^i\sigma\downarrow$ is a deducible subterm. Thus there exists $x \in dom(\phi)$ such that $(\zeta_M^i =_\mathsf{E} x)\phi$. Let $M' = \zeta_M^0[\zeta_M^1, \ldots, x, \ldots, \zeta_M^\ell]$. We have that $(M =_\mathsf{E} M')\phi$ and $(M =_\mathsf{E} M')\psi$. Now, we apply our induction hypothesis on (M', N). We obtain that $(M' =_\mathsf{E} N)\psi$ and we deduce that $(M =_\mathsf{E} N)\psi$.

Case 3: We have that $\mathsf{sign}(\zeta_M^i\sigma) = \mathsf{sign}(\zeta_M^i\sigma\downarrow)$ for every i such that $1 \leq i \leq \ell$ and also that $\mathsf{sign}(\zeta_N^i\sigma) = \mathsf{sign}(\zeta_N^i\sigma\downarrow)$ for every i such that $1 \leq i \leq p$. Moreover, if $\mathsf{sign}(\zeta_M^i) \neq \bot$ (resp. $\mathsf{sign}(\zeta_N^i) \neq \bot$), we have that $\zeta_M^i\sigma\downarrow \notin St(\phi)$ (resp. $\zeta_N^i\sigma\downarrow \notin St(\phi)$).

Consider among the ζ_M^i, ζ_N^j such that $\mathsf{sign}(\zeta_M^i) = \Sigma_2$, $\mathsf{sign}(\zeta_N^j) = \Sigma_2$, one such that $\zeta_M^i\sigma\downarrow$, $\zeta_N^j\sigma\downarrow$ is maximal w.r.t. the syntactic subterm ordering. Note that if such a ζ_M^i (or ζ_N^j) does not exist then we have that $(M, N) \in \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and we conclude using the fact that $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$. In that case, we obtain $(M =_{\mathsf{E}_1} N)\psi$ thus $(M =_\mathsf{E} N)\psi$. So, let ζ_X be such a term.

Let $\Delta = \{\zeta \in \{\zeta_M^1, \ldots, \zeta_M^\ell, \zeta_N^1, \ldots, \zeta_N^p\} \mid \zeta\sigma\downarrow = \zeta_X\sigma\downarrow\}$ and n be a new name. Let $M' = \zeta_M^0[\zeta_M'^1, \ldots, \zeta_M'^\ell]$ and $N' = \zeta_N^0[\zeta_N'^1, \ldots, \zeta_N'^p]$ where

- $\zeta_M'^i$ is equal to n if $\zeta_M^i \in \Delta$ and to ζ_M^i otherwise, and
- $\zeta_N'^i$ is equal to n if $\zeta_N^i \in \Delta$ and to ζ_N^i otherwise.

Let $\delta = \delta_{\zeta_X\sigma\downarrow, n}$. Since $M\sigma\downarrow = N\sigma\downarrow$, we have $(M\sigma\downarrow)\delta\downarrow = (N\sigma\downarrow)\delta\downarrow$. Moreover, thanks to Lemma 5, we have also that

- $(\zeta_M^0[\zeta_M^1\sigma\downarrow,\ldots,\zeta_M^\ell\sigma\downarrow])\delta\downarrow = (M\sigma\downarrow)\delta\downarrow$, *i.e.* $M'\sigma\downarrow = (M\sigma\downarrow)\delta\downarrow$,
- $(\zeta_N^0[\zeta_N^1\sigma\downarrow,\ldots,\zeta_N^p\sigma\downarrow])\delta\downarrow = (N\sigma\downarrow)\delta\downarrow$, *i.e.* $N'\sigma\downarrow = (N\sigma\downarrow)\delta\downarrow$.

Hence, we have that $(M',N') \in \mathsf{Eq}_{\mathsf{E}}(\phi)$. Since $(M',N') < (M,N)$, by induction hypothesis, we obtain $(M' =_{\mathsf{E}} N')\psi$.

Let $\delta' = \delta_{n,\zeta_X\sigma'\downarrow}$.

Claim: For every i such that $1 \leq i \leq \ell$ (resp. $1 \leq i \leq p$), we have that $(\zeta_M'^i\sigma'\downarrow)\delta' = \zeta_M^i\sigma'\downarrow$ (resp. $(\zeta_N'^i\sigma'\downarrow)\delta' = \zeta_N^i\sigma'\downarrow$).
Indeed either $\zeta_M'^i = \zeta_M^i$ and we easily conclude. Otherwise we have that $\zeta_M'^i = n$ and we know that $(\zeta_M^i =_{\mathsf{E}} \zeta_X)\phi$. By induction hypothesis (since $(\zeta_M^i,\zeta_X) < (M,N)$), we deduce that $(\zeta_M^i =_{\mathsf{E}} \zeta_X)\psi$. Hence we have $(\zeta_M'^i\sigma'\downarrow)\delta' = \zeta_X\sigma'\downarrow = \zeta_M^i\sigma'\downarrow$.

We have shown that $(M' =_{\mathsf{E}} N')\psi$. Hence we have that

$$\zeta_M^0[\zeta_M'^1\sigma'\downarrow,\ldots,\zeta_M'^\ell\sigma'\downarrow] =_{\mathsf{E}} \zeta_N^0[\zeta_N'^1\sigma'\downarrow,\ldots,\zeta_N'^p\sigma'\downarrow].$$

Since E is closed under substitution of names, we deduce that

$$\zeta_M^0[(\zeta_M'^1\sigma'\downarrow)\delta',\ldots,(\zeta_M'^\ell\sigma'\downarrow)\delta'] =_{\mathsf{E}} \zeta_N^0[(\zeta_N'^1\sigma'\downarrow)\delta',\ldots,(\zeta_N'^p\sigma'\downarrow)\delta'].$$

By using our claim, we obtain that

$$\zeta_M^0[\zeta_M^1\sigma'\downarrow,\ldots,\zeta_M^\ell\sigma'\downarrow] =_{\mathsf{E}} \zeta_N^0[\zeta_N^1\sigma'\downarrow,\ldots,\zeta_N^p\sigma'\downarrow].$$

Hence we deduce that $(M =_{\mathsf{E}} N)\psi$. □

B.3 Abstracting alien subterms

Lemma 11 *Let ϕ and ψ be two frames built on Σ and in normal form. Let $F_2 = \{N \in St(\phi\cup\psi) \mid \mathsf{sign}(N) = \Sigma_2\}$, $\tilde{n}_{F_2}$ be a set of names, distinct from the names occurring in ϕ and ψ, of same cardinality as F_2 and $\rho_2 : F_2 \to \tilde{n}_F$ a replacement. We have that*

$$\phi \models \mathsf{Eq}_{\mathsf{E}_1}(\psi) \text{ if and only if } \nu\tilde{n}_{F_2}.\phi^{\rho_2} \models \mathsf{Eq}_{\mathsf{E}_1}(\nu\tilde{n}_{F_2}.\psi^{\rho_2})$$

Proof. ($\Rightarrow$) Let $(M,N) \in \mathsf{Eq}_{\mathsf{E}_1}(\nu\tilde{n}_F.\psi^{\rho_2})$. We have to show $(M =_{\mathsf{E}_1} N)\phi^{\rho_2}$. Since $(M =_{\mathsf{E}_1} N)\psi^{\rho_2}$ and since E_1 is closed under substitution of names, we deduce that $((M =_{\mathsf{E}_1} N)\psi^{\rho_2})^{\rho_2^{-1}}$. Moreover, we have that

- $(M\psi^{\rho_2})^{\rho_2^{-1}} = M(\psi^{\rho_2})^{\rho_2^{-1}} = M\psi$ since $\tilde{n}_F \notin fn(M)$, and
- $(N\psi^{\rho_2})^{\rho_2^{-1}} = N(\psi^{\rho_2})^{\rho_2^{-1}} = N\psi$ since $\tilde{n}_F \notin fn(N)$.

This allows us to obtain that $(M =_{\mathsf{E}_1} N)\psi$. Now, thanks to the fact that $\phi \models \mathsf{Eq}_{\mathsf{E}_1}(\psi)$, we deduce that $(M =_{\mathsf{E}_1} N)\phi$. Let $\phi = \nu\tilde{n}.\sigma$. We have that $M\sigma\downarrow = N\sigma\downarrow$. Since $\mathsf{sign}((M\sigma)^{\rho_2}) \neq \Sigma_2$ and $(M\sigma)^{\rho_2}$ does not contain subterms of sign Σ_2, all its factors are in normal form. Thus, we can apply Lemma 4, yielding to $(M\sigma)^{\rho_2}\downarrow = (M\sigma)^{\rho_2}\downarrow_{\mathsf{E}_1}$. We deduce that

$$(M\sigma)^{\rho_2}\downarrow =_{\mathsf{E}_1} (M\sigma)^{\rho_2} \tag{5}$$

In the same way, we can obtain $(N\sigma)^{\rho_2}\downarrow =_{\mathsf{E}_1} (N\sigma)^{\rho_2}$.

Since all the factors of $M\sigma$ and $N\sigma$ are in normal form, we can apply Lemma 5 , yielding to

$$(M\sigma)^{\rho_2}\downarrow = (M\sigma)\downarrow^{\rho_2}\downarrow \qquad\qquad (N\sigma)^{\rho_2}\downarrow = (N\sigma)\downarrow^{\rho_2}\downarrow \tag{6}$$

By the equalities (6) and the fact that $M\sigma\downarrow = N\sigma\downarrow$, we obtain that $(M\sigma)^{\rho_2}\downarrow = (N\sigma)\downarrow^{\rho_2}\downarrow = (N\sigma)^{\rho_2}\downarrow$. Now, using equalities (5), we obtain that $(M\sigma)^{\rho_2} =_{\mathsf{E}_1} (N\sigma)^{\rho_2}$. Now, since M and N are terms built on Σ_1, we have that $(M\sigma)^{\rho_2} = M(\sigma^{\rho_2})$ and $(N\sigma)^{\rho_2} = N(\sigma^{\rho_2})$ (syntactically). This allows us to conclude.

($\Leftarrow$) Let $(M, N) \in \mathsf{Eq}_{\mathsf{E}_1}(\psi)$. We have to show that $(M =_{\mathsf{E}_1} N)\phi$. Firstly, we can assume w.l.o.g. that $(fn(M) \cup fn(N)) \cap \tilde{n}_F = \emptyset$. Let $\psi = \nu\tilde{n}.\sigma$.

Since $\mathsf{sign}((M\sigma)^{\rho_2}) \neq \Sigma_2$ and $(M\sigma)^{\rho_2}$ does not contain subterms of sign Σ_2, all its factors are in normal form. Thus, we can apply Lemma 4, yielding to $(M\sigma)^{\rho_2}\downarrow = (M\sigma)^{\rho_2}\downarrow_{\mathsf{E}_1}$. We deduce that

$$(M\sigma)^{\rho_2}\downarrow =_{\mathsf{E}_1} (M\sigma)^{\rho_2} \tag{7}$$

In the same way, we obtain $(N\sigma)^{\rho_2}\downarrow =_{\mathsf{E}_1} (N\sigma)^{\rho_2}$.

Since all the factors of $M\sigma$ and $N\sigma$ are in normal form, we can apply Lemma 5 , yielding to

$$(M\sigma)^{\rho_2}\downarrow = (M\sigma)\downarrow^{\rho_2}\downarrow \qquad\qquad (N\sigma)^{\rho_2}\downarrow = (N\sigma)\downarrow^{\rho_2}\downarrow \tag{8}$$

By the equalities (8) and the fact that $M\sigma\downarrow = N\sigma\downarrow$, we obtain that $(M\sigma)^{\rho_2}\downarrow = (N\sigma)\downarrow^{\rho_2}\downarrow = (N\sigma)^{\rho_2}\downarrow$. Now, using equalities (7), we obtain that $(M\sigma)^{\rho_2} =_{\mathsf{E}_1} (N\sigma)^{\rho_2}$. Now, since M and N are terms built on Σ_1, we have that $(M\sigma)^{\rho_2} = M(\sigma^{\rho_2})$ and $(N\sigma)^{\rho_2} = N(\sigma^{\rho_2})$ (syntactically). Hence, we obtain that $(M =_{\mathsf{E}_1} N)\psi^{\rho_2}$. Since $\nu\tilde{n}_F.\phi^{\rho_2} \models \mathsf{Eq}_{\mathsf{E}_1}(\nu\tilde{n}_F.\psi^{\rho_2})$, we deduce that $(M =_{\mathsf{E}_1} N)\phi^{\rho_2}$. Since E_1 is closed under substitution of names, we deduce that $((M =_{\mathsf{E}_1} N)\phi^{\rho_2})^{{\rho_2}^{-1}}$. We have $(M\phi^{\rho_2})^{{\rho_2}^{-1}} = M(\phi^{\rho_2})^{{\rho_2}^{-1}} = M\phi$ since $\tilde{n}_F \cap fn(M) = \emptyset$. For the same reason, we have that $(N\phi^{\rho_2})^{{\rho_2}^{-1}} = N\phi$. This allows us to conclude. □

B.4 Complexity

Let ϕ_1 and ϕ_2 be two frames. Let $\phi_1' = \overline{(\overline{\phi_1}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})}$ and $\phi_2' = \overline{(\overline{\phi_2}^{\phi_2})}^{(\overline{\phi_1}^{\phi_2})}$.
Assume that

- $\phi \vdash_{\mathsf{E}} M$ can be decided in $f_3(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$,
- a recipe ζ such that $(\zeta =_{\mathsf{E}} M)\phi$ can be computed in $f_4(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$ and that we control the size of the recipe $t_{\mathsf{dag}}(\zeta) \leq f_5(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$
- $\phi \approx_{\mathsf{E}_i} \psi$ can be decided in $f_i(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M))$ for $i \in \{1, 2\}$.

We also assume that the f_i are non-decreasing functions.

Let $h : \mathbb{N} \to \mathbb{N}$ such that $h(x) = x(f_3(2x) + f_4(2x))$. Let $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that $g(x, y) = x(f_5(2y) + x)$.

Claim 1 *Let ϕ be a frame. $\overline{\phi}^{\phi}$ can be computed in time $t_{\mathsf{dag}}(\phi)f_3(2t_{\mathsf{dag}}(\phi))$. Moreover, $t_{\mathsf{dag}}(\overline{\phi}^{\phi}) \leq t_{\mathsf{dag}}(\phi)$.*

Computing $\overline{\phi}^{\phi}$ is equivalent to computing the deducible subterms of ϕ. That is, for each M in $St(\phi)$, we check whether $\phi \vdash_{\mathsf{E}} M$, which can be performed in $f_3(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)) \leq f_3(2t_{\mathsf{dag}}(\phi))$. Thus $\overline{\phi}^{\phi}$ can be computed in time $t_{\mathsf{dag}}(\phi)f_3(2t_{\mathsf{dag}}(\phi))$. Moreover, since only subterms of ϕ are added in $\overline{\phi}^{\phi}$, the DAG-size does not change thus $t_{\mathsf{dag}}(\overline{\phi}^{\phi}) \leq t_{\mathsf{dag}}(\phi)$. □

Claim 2 *Let ϕ and ψ be two frames. $\overline{\phi}^{\psi}$ can be computed in time $h(t_{\mathsf{dag}}(\psi))$. Moreover, $t_{\mathsf{dag}}(\overline{\phi}^{\psi}) \leq g(t_{\mathsf{dag}}(\phi), t_{\mathsf{dag}}(\psi))$.*

To compute $\overline{\phi}^{\psi}$ we have to check, for each M in $St(\psi)$ whether $\psi \vdash_E M$, which can be performed in $f_3(t_{\mathsf{dag}}(\psi) + t_{\mathsf{dag}}(M)) \leq f_3(2t_{\mathsf{dag}}(\psi))$. Whenever $\psi \vdash_E M$, we have to compute a recipe for M, which can be done in $f_4(t_{\mathsf{dag}}(\psi) + t_{\mathsf{dag}}(M)) \leq f_4(2t_{\mathsf{dag}}(\psi))$. Altogether we deduce that $\overline{\phi}^{\psi}$ can be computed in time $h(t_{\mathsf{dag}}(\psi))$. Moreover, $t_{\mathsf{dag}}(\overline{\phi}^{\psi}) \leq t_{\mathsf{dag}}(\phi) + |\psi|(f_5(t_{\mathsf{dag}}(\psi)) + t_{\mathsf{dag}}(\phi)) \leq g(t_{\mathsf{dag}}(\phi), t_{\mathsf{dag}}(\psi))$. □

We deduce that $\overline{\phi_1}^{\phi_2}$ can be computed in time $h(t_{\mathsf{dag}}(\phi_2))$ and ϕ_1' can be computed in time $h(t_{\mathsf{dag}}(\phi_2)) + t_{\mathsf{dag}}(\overline{\phi_1}^{\phi_2})f_3(2t_{\mathsf{dag}}(\overline{\phi_1}^{\phi_2}))$ that is ϕ_1' can be computed in time at most

$$h(t_{\mathsf{dag}}(\phi_2)) + g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2))f_3(2g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2))) \tag{9}$$

Moreover $t_{\mathsf{dag}}(\phi_1') \leq t_{\mathsf{dag}}(\overline{\phi_1}^{\phi_2}) \leq g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2))$.

Similarly, $\overline{\phi_2}^{\phi_2}$ can be computed in time $t_{\mathsf{dag}}(\phi_2)f_3(2t_{\mathsf{dag}}(\phi_2))$. Thus ϕ_2' can be computed in time $t_{\mathsf{dag}}(\phi_2)f_3(2t_{\mathsf{dag}}(\phi_2)) + h(t_{\mathsf{dag}}(\overline{\phi_1}^{\phi_2}))$ that is ϕ_2' can be computed in time at most

$$t_{\mathsf{dag}}(\phi_2)f_3(2t_{\mathsf{dag}}(\phi_2)) + h(g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2))) \tag{10}$$

Moreover $t_{\mathsf{dag}}(\phi_2') \leq g(t_{\mathsf{dag}}(\phi_2), g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)))$.

Since abstracting alien subterms make the size decrease, we get that checking whether $\tilde{n}_{F_2}.(\phi_1')^{\rho_2} \approx_{\mathsf{E}_1} \tilde{n}_{F_2}.(\phi_2')^{\rho_2}$ can be computed in time at most

$$f_1(g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)) + g(t_{\mathsf{dag}}(\phi_2), g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)))) \tag{11}$$

and whether $\tilde{n}_{F_1}.(\phi_1')^{\rho_1} \approx_{\mathsf{E}_2} \tilde{n}_{F_1}.(\phi_2')^{\rho_1}$ can be computed in time at most

$$f_2(g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)) + g(t_{\mathsf{dag}}(\phi_2), g(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)))) \tag{12}$$

Altogether, the complexity of checking whether $\phi_1 \approx_{\mathsf{E}} \phi_2$ is obtained by summing the four values (9) +(10) + (11) +(12).

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399