Decidability and combination results for two notions of knowledge in security protocols *

Véronique Cortier (cortier@loria.fr)
LORIA, CNRS & INRIA

Stéphanie Delaune† (stephanie.delaune@lsv.ens-cachan.fr)
LSV, ENS de Cachan & CNRS & INRIA

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 considered: deducibility and indistinguishability. Those notions are well-studied and several decidability results already exist to deal with a variety of equational theories. Most of the existing results are dedicated to specific equational theories and only few results, especially in the case of indistinguishability, have been obtained for equational theories with associative and commutative properties (AC).

In this paper, we show that existing 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. We also propose a general setting for solving deducibility and indistinguishability for an important class (called *monoidal*) of equational theories involving AC operators.

As a consequence of these two results, new decidability and complexity results can be obtained for many relevant equational theories.

Keywords: Formal methods, Security protocols, Equational theories.

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 definitions have been proposed in the literature to express knowledge. They are known as message deducibility and indistinguishability relations.

* This work has been partly supported by the ANR-07-SESU-002 project AVOTÉ.

† Corresponding author: Stéphanie Delaune, LSV, ENS de Cachan & CNRS, 61 avenue du Président Wilson, 94235 Cachan Cedex - France *tel:* +33 1 47 40 75 63 *fax:* +33 1 47 40 75 21 (delaune@lsv.ens-cachan.fr)

Most often, the knowledge of the attacker is described in terms of message deducibility [29, 32, 30]. 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 (*e.g.* the value of a vote), we may ask whether an attacker can learn this value by eavesdropping on the protocol. Of course, it is completely unrealistic to require 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 [11, 1, 28]: two sequences of messages are cryptographically indistinguishable if their distributions are indistinguishable to any attacker, that is 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 [33, 13, 19]. In the applied pi calculus framework [3], 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, ...). Many decision procedures have been provided to decide these relations under a variety of equational theories. For instance algorithms for deduction have been provided for exclusive or [19], homomorphic operators [21], Abelian groups with distributive encryption [27] and subterm theories [2]. These theories allow basic equations for functions such as encryption, decryption and digital signature. There are also results for static equivalence. For instance, a general decidability result for the class of subterm convergent equational theories is given in [2]. Also in [2] 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. Regarding theories with associative and commutative properties (AC), they only obtain decidability for pure AC and exclusive or. The goal of this paper is to go further and to develop decision methods for deduction and static equivalence under an even larger class of equational theories.

Firstly, 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 signature symbol), they are also decidable for their union $\mathsf{E}_1 \cup \mathsf{E}_2$, provided that the word problem is decidable. 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.

This result, described in Part I, allows us 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. This result allows a modular approach. Deciding interesting equational theories can be done simply by reducing to the decision of simpler and independent theories. Our combination result relies on combination algorithms for solving unification problems modulo an equational theory [34, 7]. It follows the approach of Chevalier and Rusinowitch [14], who show how to combine decision algorithms for the deducibility problem in the presence of an active attacker. However, they do not consider static equivalence at all, which is needed to express larger classes of security properties. Considering static equivalence notoriously involves more difficulties since static equivalence is defined through universal quantification. In particular, proving static equivalence requires a careful understanding of the (infinite) set of equalities satisfied by a sequence of terms. Although our combination result for deduction is clearly related to the results by Chevalier and Rusinowitch, how deduction can be combined for disjoint equational theories is not stated in their papers [14, 17].

Secondly, we provide new decidability and complexity results for an important class of equational theories. We consider the axioms of Associativity-Commutativity (AC), Unit element (U), Nilpotency (N), Idempotency (I), homomorphism (h), and more especially the combinations of these axioms that constitute monoidal theories. We propose a general approach (see Part II) to handle *monoidal* theories that

covers several cases already studied, and furthermore includes some new decidability and complexity results on homomorphic operators. Monoidal theories have been extensively studied by F. Baader and W. Nutt [31, 5, 6] who have provided a complete survey of unification in these theories. More recently, these theories have been studied in the context of security protocols. S. Delaune *et al.* have shown that deduction is decidable for a subclass of monoidal equational theories, also considering active attacks [22]. However, they do not address static equivalence.

In Part III, we give a list of relevant equational theories for which deduction and static equivalence have been studied by us or others. This gives a (hopefully) complete picture of existing results in this area.

This paper represents a synthesis of the work published at FROCOS 2007 and LPAR 2007 with improvements in presentation and additional technical material throughout.

2. Preliminaries

We first start by introducing some common material for the next sections. In Section 2.1 we recall some basic definitions. Then, in Section 2.2, we explain our representation for the information available to an intruder who has seen messages exchanged in the course of a protocol execution. In the applied pi calculus framework [3], such a representation is known as a frame. Lastly we describe our two notions of knowledge for an intruder.

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. We assume given a signature Σ, an infinite set of names $\mathcal{N}$, and an infinite set of variables $\mathcal{X}$. Let $\mathcal{M}$ be a set of names and variables. We denote by $\mathcal{T}(\Sigma, \mathcal{M})$ the set of *terms* over $\Sigma \cup \mathcal{M}$. The concept of names is borrowed from the applied pi calculus [3] and corresponds to the notion of free constant used for instance in [14]. We write $fn(M)$ (resp. $fv(M)$) for the set of names (resp. variables) that occur in the term M. A term M is *ground* when it does not have variables, *i.e.* $fv(M) = \emptyset$. A *context* C is a term with holes, or (more formally) a term with distinguished variables that occur only once. 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 $\mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$. Substitutions are extended to endomorphisms of $\mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$ as usual. We use a postfix notation for their application.

An *equational presentation* $\mathcal{H} = (\Sigma, \mathsf{E})$ is defined by a set E of equations over $\mathcal{T}(\Sigma, \mathcal{X})$, *i.e.* a set of unordered pairs of terms without names. For any equational presentation $\mathcal{H}$, the relation $=_{\mathcal{H}}$ denotes the equational theory generated by E on $\mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$, that is the smallest congruence containing all instances of axioms of E. Abusively, we shall not distinguish between an equational presentation $\mathcal{H}$ over a signature Σ and a set E of equations presenting it. Hence, we write $M =_{\mathsf{E}} N$ instead of $M =_{\mathcal{H}} N$ when the signature is clear from the context. Since the equations in E do not contain any names, we have that $=_{\mathsf{E}}$ is closed by substitutions of terms for names. A theory E is *consistent* if there do 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 Section 2.3) and static equivalence (defined in Section 2.4) are trivial.

Given two sets of terms S_1 and S_2, we say that S_1 *is a subset of* S_2 *modulo* E, denoted $S_1 \subseteq_{\mathsf{E}} S_2$, if for any $T_1 \in S_1$, there exists $T_2 \in S_2$ such that $T_1 =_{\mathsf{E}} T_2$. When $S_1 \subseteq_{\mathsf{E}} S_2$ and $S_2 \subseteq_{\mathsf{E}} S_1$, we also write $S_1 =_{\mathsf{E}} S_2$.

Example 1. *Let* Σ_+ *be the signature made up of the constant symbol* 0 *and the binary function* $+$ *and* E_+ *be the following set of equations:*

$$\begin{array}{rcll} x + (y + z) & = & (x + y) + z & (\mathsf{A}) \\ x + y & = & y + x & (\mathsf{C}) \end{array} \qquad \begin{array}{ll} x + 0 = x & (\mathsf{U}) \\ x + x = 0 & (\mathsf{N}) \end{array}$$

We have that $n_1 + (n_2 + n_1) =_{\mathsf{E}_+} n_2$. *Let* t_1 *and* t_2 *be two terms. Since* E_+ *is closed by substitutions of terms for names, we have that* $t_1 + (t_2 + t_1) =_{\mathsf{E}_+} t_2$. *Note that this equality still holds when* $t_1 = t_2$.

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:*

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

Definition 3. (syntactic subterm). *The set* $St_s(M)$ *of* syntactic subterms *of a term* M *is defined recursively as follows:*

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

The positions in a term M are defined recursively as usual (*i.e.* sequences of integers with ϵ being the empty sequence). 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 [3], such a sequence of messages is organized into a *frame* $\phi = \nu\tilde{n}.\sigma$, where $\tilde{n}$ is a finite set of *restricted* 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. For notational convenience, we will write $\nu n_1, \ldots, n_k$ instead of $\nu\{n_1, \ldots, n_k\}$.

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 $\phi \vdash_{\mathsf{E}} M$ and is axiomatized by the following rules:

$$\frac{}{\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M} \text{ if } \exists x \in dom(\sigma) \text{ s.t. } x\sigma = M \qquad \frac{}{\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} s} \; s \in \mathcal{N} \setminus \tilde{n}$$

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

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 under application of function symbols. Note that ϕ, M, M', $M_1, \ldots, M_\ell$ might be built on a signature Σ' that possibly contains some additional function symbol not in Σ, i.e. such that $\Sigma \subseteq \Sigma'$. Hence the relation $=_{\mathsf{E}}$ means $=_{\mathcal{H}'}$ where $\mathcal{H}' = (\Sigma', \mathsf{E})$. When $\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M$, any occurrence of names from $\tilde{n}$ in M is bound by $\nu\tilde{n}$. So $\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M$ could be formally written $\nu\tilde{n}.(\sigma \vdash_{\mathsf{E}} M)$.

Definition 4. (recipe). *Let M be a ground term and $\nu\tilde{n}.\sigma$ be a frame built on $\Sigma' \supseteq \Sigma$. A* recipe of M in ϕ modulo E *is a term $\zeta \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$ such that $fn(\zeta) \cap \tilde{n} = \emptyset$ and $\zeta\sigma =_{\mathsf{E}} M$.*

It is easy to prove (see [2]) by induction the following characterization of deduction.

Lemma 5. (characterization of deduction). *Let M be a ground term and $\nu\tilde{n}.\sigma$ be a frame built on Σ' (possibly larger than Σ). Then $\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M$ if, and only if, there exists a recipe of M in ϕ modulo E.*

Example 6. *Consider the equational theory $(\Sigma_{\mathsf{enc}}, \mathsf{E}_{\mathsf{enc}})$ given in Example 2. Let $\phi = \nu k, s_1.\{^{\mathsf{enc}(\langle s_1, s_2\rangle, k)}/_{x_1}, {}^{k}/_{x_2}\}$ where k, s_1, and s_2 are names (only k and s_1 are restricted). We have that $\phi \vdash_{\mathsf{E}_{\mathsf{enc}}} k$, $\phi \vdash_{\mathsf{E}_{\mathsf{enc}}} s_1$ and also that $\phi \vdash_{\mathsf{E}_{\mathsf{enc}}} s_2$. 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.*

Example 7. *Consider the equational theory (Σ_+, E_+) given in Example 1. Let $\phi = \nu n_1, n_2, n_3.\{^{n_1+n_2+n_3}/_{x_1}, {}^{n_1+n_2}/_{x_2}, {}^{n_2+n_3}/_{x_3}\}$. We have that $\phi \vdash_{\mathsf{E}_+} n_2 + n_4$. Indeed the term $x_1 + x_2 + x_3 + n_4$ is a recipe of the term $n_2 + n_4$.*

Definition 8. (Deduction problem). *The* deduction problem *for the equational theory E built over Σ is as follows:*

Entries: *A frame ϕ and a ground term M (both built over Σ)*

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

Note that the deduction relation $\vdash_{\mathsf{E}}$ for the equational theory (Σ, E) is defined for frames and terms built over a signature Σ' which is possibly larger than Σ. However, what we call the deduction problem for the equational theory (Σ, E) contains only the instances where $\Sigma' = \Sigma$.

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. Static equivalence, also called the indistinguishability relation, is particularly important when defining for example the confidentiality of a vote or anonymity-like properties.

In the frame $\phi = \nu\tilde{n}.\sigma$, the names $\tilde{n}$ are bound in σ and can be renamed. Moreover names that do not appear in ϕ can be added or removed from $\tilde{n}$. In particular, we can always assume that two frames share the same set of restricted names. Thus, in the definition below, we will assume w.l.o.g. that the two frames ϕ and ϕ' have the same set of restricted names.

Definition 9. (static equivalence). *Let (Σ, E) be an equational theory. Let ϕ be a frame built on $\Sigma' \supseteq \Sigma$ and $M, N \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$. We say that M and N are* equal in the frame ϕ*, and write $(M =_{\mathsf{E}} N)\phi$, 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 $\phi = \nu\tilde{n}.\sigma$ and $\phi' = \nu\tilde{n}.\sigma'$ built on Σ' are statically equivalent*, and write $\phi \approx_{\mathsf{E}} \phi'$ (or shortly $\phi \approx \phi'$) when:*

- *$dom(\phi) = dom(\phi')$, and*
- *for all $M, N \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$ we have $(M =_{\mathsf{E}} N)\phi \Leftrightarrow (M =_{\mathsf{E}} N)\phi'$.*

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

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

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 each of the two frames under consideration satisfies the equalities of the other frame.

Lemma 10. (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*

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

Example 11. *Consider the equational theory $(\Sigma_{\mathsf{enc}}, \mathsf{E}_{\mathsf{enc}})$ (see Example 2). Let $\phi = \nu k.\sigma$, $\phi' = \nu k.\sigma'$ where $\sigma = \{{}^{\mathsf{enc}(s_0,k)}/_{x_1}, {}^{k}/_{x_2}\}$ and*

$\sigma' = \{^{\mathsf{enc}(s_1,k)}/_{x_1}, {}^{k}/_{x_2}\}$. *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 that* $\phi \not\approx_{\mathsf{E}_{\mathsf{enc}}} \phi'$. *However, note that* $\nu k.\{^{\mathsf{enc}(s_0,k)}/_{x_1}\} \approx_{\mathsf{E}_{\mathsf{enc}}} \nu k.\{^{\mathsf{enc}(s_1,k)}/_{x_1}\}$.

Example 12. *Consider the equational theory* ACUN *(also called* E_+*) given in Example 1 and let* $\phi = \nu n_1, n_2, n_3.\{^{n_1+n_2+n_3}/_{x_1}, {}^{n_2+n_3}/_{x_2}, {}^{n_1}/_{x_3}\}$. *Let* $M = x_1 + x_2$ *and* $N = x_3$. *We have that* $(M =_{\mathsf{E}} N)\phi$, *thus* $(M, N) \in \mathsf{Eq}(\phi)$.

Definition 13. (static equivalence problem). *The* static equivalence problem *for the equational theory* E *built over* Σ *is as follows:*

Entries: *Two frames* ϕ_1 *and* ϕ_2 *(both built over* Σ*)*

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

Again, the static equivalence relation $\approx_{\mathsf{E}}$ for the equational theory (Σ, E) is defined for frames built over a signature Σ' which is possibly larger than Σ. However, what we call the static equivalence problem for the equational theory (Σ, E) contains only the instances where $\Sigma' = \Sigma$.

— PART I: Combination algorithms —

In this part of the 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 signature symbol), they are also decidable for their union $\mathsf{E}_1 \cup \mathsf{E}_2$. Our result assumes the word problem to be decidable. Our combination results follow the approach of Chevalier and Rusinowitch [14, 17], who show how to combine decision algorithms for the deducibility problem in presence of an active attacker. Our procedures also rely on combination algorithms for solving unification problems modulo E [34, 7], and we partly reuse the techniques introduced by Baader and Schulz to combine constraint solvers [8].

3. Material for combination algorithms

We consider two equational presentations $\mathcal{H}_1 = (\Sigma_1, \mathsf{E}_1)$ and $\mathcal{H}_2 = (\Sigma_2, \mathsf{E}_2)$ that are disjoint (in the sense that $\Sigma_1 \cap \Sigma_2 = \emptyset$) and consistent. Note that $\mathcal{T}(\Sigma_1, \mathcal{N} \cup \mathcal{X})$ and $\mathcal{T}(\Sigma_2, \mathcal{N} \cup \mathcal{X})$ share symbols, namely names and variables. Names are used to represent agent identities, keys or nonces. We denote by Σ the union of the signatures Σ_1 and Σ_2 and by E the union of the sets of equations E_1 and E_2. The *union* of the two equational presentations $\mathcal{H}_1$ and $\mathcal{H}_2$ is the equational presentation defined by (Σ, E).

3.1. Factors, Subterms

We denote by $\mathsf{sign}(\cdot)$ the function that associates to each term $M \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$, the signature ($\Sigma_1$ or Σ_2) of the function symbol at position ϵ (root position) in M. 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*. A similar notion is also used in [14].

Definition 14. (factors, subterms). *Let $M \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$. 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. By abuse of notation, we may write $St(\Phi \cup \{M\})$ *instead of* $St(\Phi) \cup St(\{M\})$*, where* Φ *is a frame and* M *a term.*

Note that the names and the variables that occur in a term M are in $St(M)$. In the rest of this part, the notion of subterm will refer to the notion introduced in Definition 14. When we want to refer to the notion of syntactic subterm (Definition 3), we will mention this explicitly.

Let $M \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$. 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 15. *Consider the theories* $(\Sigma_{\mathsf{enc}}, \mathsf{E}_{\mathsf{enc}})$ *and* (Σ_+, E_+)*. Let* M *be the term* $\mathsf{dec}(\langle n_1 + \langle n_2, n_3\rangle, \mathsf{proj}_1(n_1 + n_2)\rangle, n_3)$*. The term* $n_1 + \langle n_2, n_3\rangle$ *is a syntactic subterm of* M *alien to* M *since* $\mathsf{sign}(n_1 + \langle n_2, n_3\rangle) = \Sigma_+$ *and* $\mathsf{sign}(M) = \Sigma_{\mathsf{enc}}$*. We have that*

- $Fct(M) = \{n_1 + \langle n_2, n_3\rangle,\ n_1 + n_2,\ n_3\}$*, and*
- $St(M) = Fct(M) \cup \{M,\ n_1,\ n_2,\ \langle n_2, n_3\rangle\}$.

Moreover, we have that $|M| = 4$*. Indeed, we have that*

$$|M| = 1 + |n_1 + \langle n_2, n_3\rangle| + |n_1 + n_2| + |n_3| = 1 + 2 + 1 + 0 = 4.$$

This notion of size of terms is quite non-standard and does not correspond to the actual size of a term. It is only used for proving our lemmas by induction. Our complexity results stated later on in the paper rely on the more usual notion of DAG-size.

3.2. Ordered rewriting

Most of the definitions and results in this subsection are borrowed from [15] since we use similar techniques. We consider the notion of *ordered rewriting* defined in [23], which is a useful tool that has been used (*e.g.* [7]) for proving correctness of combination of unification algorithms. Let $\prec$ be a simplification ordering[1] on ground terms assumed to be total and such that the minimum for $\prec$ is a name n_{min} and the constants in Σ are smaller that any ground term that is neither a constant nor a name. We define Σ_0 to be the set of the constant symbols of Σ_1 and Σ_2 plus the name n_{min}, i.e. $\Sigma_0 = \Sigma_1 \cup \Sigma_2 \cup \{n_{min}\}$.

[1] By definition $\prec$ satisfies that for all ground terms M, N_1, N_2, and for any position $p \neq \epsilon$ in M, we have $N_1 \prec M[N_1]_p$ and $N_1 \prec N_2$ implies $M[N_1]_p \prec M[N_2]_p$.

In what follows, we furthermore assume that n_{min} is never used under restriction in frames.

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:

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

It has been shown (see [23]) 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,
2. the rewriting system $\rightarrow_{\mathcal{O}}$ is convergent.

Applying unfailing completion to $\mathsf{E} = \mathsf{E}_1 \cup \mathsf{E}_2$, it is easy to notice [7] 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. Since the relation $\rightarrow_{\mathcal{O}}$ is convergent on ground terms, we define $M{\downarrow_{\mathsf{E}}}$ (or briefly $M{\downarrow}$) as the unique normal form of 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. $\rightarrow_{\mathcal{O}_2}$). These notations are extended as expected to sets of terms.

We can easily prove (see Appendix B) the following results.

Lemma 16. *Let M be a ground term such that all its factors are in normal form. Then*

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

By relying on Lemma 16, we can show the following result whose proof is given in Appendix B.

Corollary 17. *Let M be a ground term: $St(M{\downarrow}) \subseteq St(M){\downarrow} \cup \{n_{min}\}$.*

Example 18. *Consider the equational theory (Σ_+, E_+) described in Example 1. Let $\Sigma_0 = \{\mathsf{f}\}$ and $\mathsf{E}_0 = \{\mathsf{f}(x) = \mathsf{f}(y)\}$. We have that the theories E_+, E_0 and $\mathsf{E}_+ \cup \mathsf{E}_0$ are consistent. Let $M = \mathsf{f}(n_1 + n_2)$. We have that $M{\downarrow} = \mathsf{f}(n_{min})$. Hence $Fct(M{\downarrow})$ (resp. $St(M{\downarrow})$) contains n_{min} whereas $Fct(M)$ (resp. $St(M)$) does not contain this term.*

Lemma 19. *Let M be a 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 and N is a term, we denote by $M[\Pi \leftarrow N]$ the term obtained by replacing all terms at a position in Π by N. We denote by $\delta_{N,N'}$ the replacement by N' of all the occurrences of N that appear at a subterm position. It is easy to establish the following lemma (see Appendix B).

Lemma 20. *Let M be a ground term such that all 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 21. *Consider the equational theories $(\Sigma_{\mathsf{enc}}, \mathsf{E}_{\mathsf{enc}})$ and (Σ_+, E_+). Let $M = \mathsf{dec}(\mathsf{enc}(\langle n_1+n_2, n_1+n_2+n_3\rangle, n_1+n_2), n_1+n_2)$, $N = n_1+n_2$ and $N' = n$. We have that M, N and N' satisfy the conditions given in Lemma 20. Moreover, we have that*

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

Hence, we have that $M\delta_{N,N'}{\downarrow} = M{\downarrow}\delta_{N,N'}{\downarrow} = \langle n, n_1 + n_2 + n_3\rangle$.

Let $\rho : F \to \tilde{n}_F$ be a replacement (that is a function) from a finite set of terms F to names $\tilde{n}_F$. Let $F = \{N_1, \ldots, N_k\}$ be a set such that whenever N_i is a syntactic subterm of N_j then $i > j$. For any term M, we denote by M^ρ the term obtained by replacing in M (in an order that is consistent with the syntactic subterm relation) any subterm $N \in F$ by $\rho(N)$. Formally, we have that $M^\rho = (M\delta_{N_1,\rho(N_1)}) \cdots \delta_{N_k,\rho(N_k)}$. This extends in a natural way to sets of terms, substitutions, frames ...

Example 22. *Consider the equational theories $(\Sigma_{\mathsf{enc}}, \mathsf{E}_{\mathsf{enc}})$ and (Σ_+, E_+) and the term $M = \mathsf{dec}(\langle n_1 + \langle n_1 + n_2, n_3\rangle, \mathsf{proj}_1(n_1 + n_2)\rangle, n_1 + n_2)$. Let ρ be the replacement $\{n_1 + \langle n_1 + n_2, n_3\rangle \to k_1,\ n_1 + n_2 \to k_2\}$. $M^\rho = \mathsf{dec}(\langle k_1, \mathsf{proj}_1(k_2)\rangle, k_2)$.*

3.4. Word problem and weak normalization

Since the underlying rewriting system may be infinite, we can not compute the normal form of a term in an effective way. Instead, we will use weak normal form (see Definition 24) and we will assume that the well-known word problem modulo E is decidable, allowing us to decide whether two terms are equal or not (without putting those terms in normal form).

Definition 23. (word problem). *The* word problem *for the equational theory* E *built over* Σ *is as follows:*

Entries: *Two terms* M_1 *and* M_2 *(both built over* Σ*)*

Question: $M_1 =_{\mathsf{E}} M_2$*?*

The decidability of the word problem modulo E is a direct consequence of the decidability of the static equivalence problem modulo E. However, it is not a consequence of the decidability of the deduction problem modulo E[2]. Thus, in our combination result for deduction, we will assume the decidability of the word problem modulo E. It is interesting to note that, for disjoint theories, decidability (in PTIME) of the word problem modulo E is a consequence of its decidability (in PTIME) in E_1 and E_2 [9].

Definition 24. (weak normal form). *The term* n_{min} *is in* weak normal form*. A term* M *(that is not syntactically equal to* n_{min}*) is in* weak normal form *if for any* $M' \in Fct(M) \cup \{n_{min}\}$ *we have that* M' *is in weak normal form and* $M \neq_{\mathsf{E}} M'$*.*

Given a term M, we say that M' *is in weak normal form of* M *modulo* E if M is in weak normal form and $M =_{\mathsf{E}} M'$. Provided that the word problem modulo E is decidable, we can compute a weak normal form of a term M modulo E as follows:

- Either $Fct(M) = \emptyset$. In such a case, if $M =_{\mathsf{E}} n_{min}$ then return n_{min}. Otherwise return M.
- Otherwise, we have that $M = C[M_1, \ldots, M_k]$ where $M_1, \ldots, M_k$ are the factors of M. Compute a weak normal form M_i' for each factor M_i. If $M =_{\mathsf{E}} M_i'$ for some $i \in \{1, \ldots, k\}$ then retrun M_i'. Otherwise return $C[M_1', \ldots, M_k']$.

[2] We give in Appendix A an example of a theory for which the deduction problem is - trivially - decidable, while the word problem is not.

Note that the weak normal form of a term is not necessarily unique.

The following lemma will be used later on to avoid computing normal form of terms.

Lemma 25. *Let M be a ground term and M' be a weak normal form of M modulo E that is also ground. We have that:*

- *Either M' is a name, say n, and we have that $M{\downarrow} = n$;*
- *Or $M' = C[M'_1, \ldots, M'_k]$ where $M'_1, \ldots, M'_k$ are the factors of M' and C is built on Σ_i ($i = \{1, 2\}$), and $M{\downarrow} =_{\mathsf{E}_i} C[M_1, \ldots, M_k]$ for some $M_1, \ldots, M_k$ that are the factors of $M{\downarrow}$. Moreover, we have that $M_1 =_{\mathsf{E}} M'_1$, $\ldots$, $M_k =_{\mathsf{E}} M'_k$.*

In both cases, we have that $\mathsf{sign}(M') = \mathsf{sign}(M{\downarrow})$.

Proof. Let M be a ground term and M' be a weak normal form of M modulo E that is also ground. We show this result by induction on $|M'|$.

Base case: $|M'| = 0$. In such a case, M' is a name, say n, we have that $M'{\downarrow} = n$. Hence, we have that $M{\downarrow} = M'{\downarrow} = n$ (see Remark at the beginning of Appendix B).

Induction step: $|M'| > 0$. In such a case, $M' = C[M'_1, \ldots, M'_k]$ where $M'_1, \ldots, M'_k$ are the factors of M' and we can assume w.l.o.g. that C is built on Σ_1. We apply Lemma 16 on $C[M'_1{\downarrow}, \ldots, M'_k{\downarrow}]$. Note that $M'_1{\downarrow}, \ldots, M'_k{\downarrow}$ are inded the factors of $C[M'_1{\downarrow}, \ldots, M'_k{\downarrow}]$ since thanks to our induction hypothesis we know that $\mathsf{sign}(M'_i) = \mathsf{sign}(M'_i{\downarrow})$ for each $i \in \{1, \ldots, k\}$. Since M' is in weak normal form, we know that $M'{\downarrow} \notin \{M'_1{\downarrow}, \ldots, M'_k{\downarrow}, n_{min}\}$. Thus, we have that $\mathsf{sign}(M') = \mathsf{sign}(M'{\downarrow})$ and $Fct(M'{\downarrow}) \subseteq \{M'_1{\downarrow}, \ldots, M'_k{\downarrow}, n_{min}\}$. Hence, thanks to Lemma 19, we know that:

$$C[M'_1{\downarrow}, \ldots, M'_k{\downarrow}]{\downarrow} = C[M'_1{\downarrow}, \ldots, M'_k{\downarrow}]{\downarrow}_{\mathsf{E}_1}.$$

Hence, we have that $M{\downarrow} = M'{\downarrow} =_{\mathsf{E}_1} C[M'_1{\downarrow}, \ldots, M'_k{\downarrow}]$. □

4. Combining algorithms for deduction

Our first combination result is devoted to deduction: it is possible to combine decision procedures of deduction for any two disjoint theories.

Theorem 26. *Let* (Σ_1, E_1) *and* (Σ_2, E_2) *be two consistent equational theories such that* $\Sigma_1 \cap \Sigma_2 = \emptyset$ *and for which the word problem is decidable. If deduction is decidable for* (Σ_1, E_1) *and* (Σ_2, E_2) *then deduction is decidable for* $(\Sigma_1 \cup \Sigma_2, \mathsf{E}_1 \cup \mathsf{E}_2)$.

The rest of this section is devoted to the proof of this theorem. First (see Section 4.1), we establish a *locality* lemma. If $\phi \vdash_{\mathsf{E}} M$, then by definition we know that there exists a proof tree witnessing this fact. Actually, the locality lemma states that there exists a proof tree such that the interface terms (i.e. those obtained by applying a function symbol in Σ_1 and used as a premise for an application of a symbol in Σ_2, or the converse) are in $St(\phi \cup \{M\})$. Hence, we reduce the deduction problem $\phi \vdash_{\mathsf{E}} M$ where $\mathsf{E} = \mathsf{E}_1 \cup \mathsf{E}_2$ to several other deduction problems. Each of them will be solved either in the equational theory E_1 or in the theory E_2. In order to obtain deduction problems where terms are built over Σ_1 (or Σ_2) only, we abstract alien subterms by fresh names (see Section 4.2). Our algorithm, described in Section 4.3, proceeds by saturation of ϕ by the terms in $St(\phi \cup \{M\})$ which are deducible either in (Σ_1, E_1) or in (Σ_2, E_2).

4.1. Locality

Our procedure first relies on the existence of a *local proof* of $\phi \vdash_{\mathsf{E}} M$ which involves only terms in $St(\phi \cup \{M\})$.

Lemma 27. (locality lemma). *Let* $\phi = \nu\tilde{n}.\sigma$ *be a frame and* M *be a ground term built on* Σ *such that terms in* ϕ *and* M *are in normal form. If* $\phi \vdash_{\mathsf{E}} M$ *then there exists a term* ζ *built on* Σ *such that* $fn(\zeta) \cap \tilde{n} = \emptyset$ *and* $\zeta\sigma =_{\mathsf{E}} M$*, and for all* $\zeta' \in St(\zeta)$*, we have that*

1. $\zeta'\sigma{\downarrow} \in St(\phi \cup \{M\}) \cup \{n_{min}\}$*, and*
2. $\zeta'\sigma{\downarrow} \in St(\phi) \cup \{n_{min}\}$ *when* $\mathsf{sign}(\zeta') \neq \mathsf{sign}(\zeta'\sigma{\downarrow})$.

Proof. By Lemma 5, we know that there exists a recipe built on Σ such that $fn(\zeta) \cap \tilde{n} = \emptyset$ and $\zeta\sigma =_{\mathsf{E}} M$. We choose one, say that ζ''_M, whose size $|\zeta''_M|$ is minimal. Let ζ_M be the term obtained from ζ''_M after replacing every occurrence of a name $n \notin St(\phi \cup \{M\})$ by n_{min}. Since E is closed by substitutions of terms for 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 conditions 1 and 2.

Base case: ζ_M is a name, a variable or a ground term built over Σ_1 (resp. Σ_2) only. In such a case, we easily conclude since $St(\zeta_M) = \{\zeta_M\}$. Note that $\mathsf{sign}(\zeta_M) \neq \mathsf{sign}(\zeta_M\sigma{\downarrow})$ implies that ζ_M is a variable. In such a case, condition 2 trivially holds.

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

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

First, we prove that condition 1 is satisfied. By induction hypothesis, we know that for all $i \leq \ell$, for all $\zeta' \in St(\zeta_i)$, we have $\zeta'\sigma{\downarrow} \in St(\phi \cup \{\zeta_i\sigma{\downarrow}\}) \cup \{n_{min}\}$. To conclude that $\zeta'\sigma{\downarrow} \in St(\phi \cup \{M\}) \cup \{n_{min}\}$ for any $\zeta' \in St(\zeta)$, it is sufficient to show that for all $i \leq \ell$ we have $\zeta_i\sigma{\downarrow} \in St(\phi \cup \{M\}) \cup \{n_{min}\}$.

- If $\mathsf{sign}(\zeta_i) = \bot$, then we have $\zeta_i\sigma{\downarrow} \in St(\phi \cup \{M\}) \cup \{n_{min}\}$.
- If $\mathsf{sign}(\zeta_i) = \Sigma_2$ and $\mathsf{sign}(\zeta_i\sigma{\downarrow}) \neq \Sigma_2$, then we conclude that $\zeta_i\sigma{\downarrow} \in St(\phi) \cup \{n_{min}\}$ 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. $\zeta_i\sigma{\downarrow} \in St(M) \cup \{n_{min}\}$. 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 $\mathsf{sign}(\zeta_j) \neq \Sigma_1$ and $\mathsf{sign}(\zeta_j\sigma{\downarrow}) = \Sigma_1$, we have $\zeta_j\sigma{\downarrow} \in St(\phi) \cup \{n_{min}\}$. Thus $\zeta_i\sigma{\downarrow} \in St(\phi) \cup \{n_{min}\}$.
  3. Otherwise, we consider among the ζ_i such that $\zeta_i\sigma{\downarrow} \notin St(\phi \cup \{M\}) \cup \{n_{min}\}$ a maximal one (w.r.t. the subterm ordering). Let ζ be such a term. Now, we show that we can build a recipe ζ'_M of M smaller than ζ_M. Let $\Delta = \{j \in \{1, \ldots, \ell\} \mid \zeta_j\sigma{\downarrow} = \zeta\sigma{\downarrow}\}$. Note that $\Delta \neq \emptyset$. 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

$$
\begin{array}{lll}
 & \zeta'_M\sigma{\downarrow} & \\
= & \zeta^0[\zeta'_1\sigma{\downarrow}, \ldots, \zeta'_\ell\sigma{\downarrow}]{\downarrow} & \\
= & ((\zeta^0[\zeta_1\sigma{\downarrow}, \ldots, \zeta_\ell\sigma{\downarrow}])\delta_{(\zeta\sigma){\downarrow}, n_{min}}){\downarrow} & \text{since } \zeta\sigma{\downarrow} \notin St(\zeta_j\sigma{\downarrow}) \text{ for } j \notin \Delta \\
= & ((\zeta^0[\zeta_1\sigma{\downarrow}, \ldots, \zeta_\ell\sigma{\downarrow}]){\downarrow}\delta_{(\zeta\sigma){\downarrow}, n_{min}}){\downarrow} & \text{thanks to Lemma 20} \\
= & (M\delta_{(\zeta\sigma){\downarrow}, n_{min}}){\downarrow} & \text{since } M = \zeta^0[\zeta_1\sigma{\downarrow}, \ldots, \zeta_\ell\sigma{\downarrow}]{\downarrow} \\
= & M & \text{since } \zeta\sigma \notin St(M)
\end{array}
$$

Now, it remains to prove that condition 2 is satisfied. By induction hypothesis, we know that for all $i \leq \ell$, for all $\zeta' \in St(\zeta_i)$ such that $\mathsf{sign}(\zeta') \neq \mathsf{sign}(\zeta'\sigma{\downarrow})$, we have that $\zeta'\sigma{\downarrow} \in St(\phi) \cup \{n_{min}\}$. It remains to show that this condition holds for ζ_M.

Assume that $\mathsf{sign}(\zeta_M) \neq \mathsf{sign}(\zeta_M\sigma\downarrow)$. Applying Lemma 16 on the term $\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow]$ whose normal form is equal to $\zeta_M\sigma\downarrow$, we obtain that $\zeta_M\sigma\downarrow \in Fct(\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow]) \cup \{n_{min}\}$. For each $1 \leq i \leq \ell$, if $\mathsf{sign}(\zeta_i) \neq \mathsf{sign}(\zeta_i\sigma\downarrow)$, we have seen that $\zeta_i\sigma\downarrow \in St(\phi) \cup \{n_{min}\}$. Hence, we deduce that $\zeta_M\sigma\downarrow \in St(\phi) \cup \{\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow, n_{min}\}$. By minimality of ζ_M, there exists no ζ_i such that $\zeta_M\sigma\downarrow = \zeta_i\sigma\downarrow$. Then we conclude that $\zeta_M\sigma\downarrow \in St(\phi) \cup \{n_{min}\}$ □

Example 28. *Consider the theory* $(\Sigma, \mathsf{E}) = (\Sigma_{\mathsf{enc}} \cup \Sigma_+, \mathsf{E}_{\mathsf{enc}} \cup \mathsf{E}_+)$*, the term* $M = n_2 + n_3$ *and the frame* $\phi = \nu n_2, n_3.\{^{\mathsf{enc}(\langle n_1+n_2, n_3\rangle, n_4)}/_{x_1}\}$*. We have that* $\phi \vdash_{\mathsf{E}} M$*. The recipe* $\zeta = \mathsf{proj}_1(\mathsf{dec}(x_1, n_4)) + \mathsf{proj}_2(\mathsf{dec}(x_1, n_4)) + n_1$ *satisfies the conditions given in Lemma 27.*

4.2. Abstraction of alien subterms

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 29. *Let* ϕ *be a frame and* M *be a ground term built on* Σ*. Let* $F_2 = \{N \mid N \in St(\phi \cup \{M\})$ *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 the same cardinality as* F_2 *and* $\rho_2 : F_2 \to \tilde{n}_{F_2}$ *be a replacement.*
Assume that terms in ϕ *and* M *are in normal form. 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.

Proof. ($\Rightarrow$) Let $\phi = \nu\tilde{n}.\sigma$. By Lemma 5, we know that there exists a term $\zeta \in \mathcal{T}(\Sigma_1, \mathcal{N} \cup \mathcal{X})$ 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 $\zeta' \in \mathcal{T}(\Sigma_1, \mathcal{N} \cup \mathcal{X})$ 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 19, 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, i.e. $\mathsf{sign}(U) \neq \Sigma_2$ for every $U \in St((\zeta\sigma)^{\rho_2})$, we deduce that all the factors of $(\zeta\sigma)^{\rho_2}$ are in normal form. Thus we can apply again Lemma 19, 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 20

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

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 $\zeta \in \mathcal{T}(\Sigma_1, \mathcal{N} \cup \mathcal{X})$, we have that $(\zeta\sigma)^{\rho_2} = \zeta(\sigma^{\rho_2})$ (syntactically). This allows us to conclude.

($\Leftarrow$) By Lemma 5, 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 by substitutions of terms for 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 $\tilde{n}_{F_2} \notin fn(\zeta)$. Hence, we conclude that $\zeta\sigma =_{\mathsf{E}_1} M$. □

4.3. Combination algorithm for deduction

Our algorithm proceeds by saturation of ϕ by the subterms in $St(\phi \cup \{M\})$ which are deducible either in (Σ_1, E_1) or in (Σ_2, E_2).

To ease the presentation, we will consider $\phi = \nu\tilde{n}.\{{}^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}\}$ as the set $\{M_1, \ldots, M_\ell\}$. When we write $\phi \cup \{T\}$, we mean the frame $\nu\tilde{n}.\{{}^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}, {}^{T}/_{x_{\ell+1}}\}$ where $x_{\ell+1}$ is a fresh variable that does not already occur in $dom(\phi)$.

We first show that $\phi\downarrow \vdash_{\mathsf{E}_i} M\downarrow$ is decidable. This is used as a sub-task in our combination algorithm for deduction.

Lemma 30. *The following problem is decidable.*

Entries: *A frame ϕ, a term M, $i \in \{1, 2\}$ and F_1, F_2, ρ_1, ρ_2 defined like in Lemma 29.*

Question: *$\phi\downarrow \vdash_{\mathsf{E}_i} M\downarrow$?*

Proof. Let us show that $\phi\downarrow \vdash_{\mathsf{E}_1} M\downarrow$ is decidable. The case $\phi\downarrow \vdash_{\mathsf{E}_2} M\downarrow$ is similar. Thanks to Lemma 29, it suffices to check whether $\nu\tilde{n}_{F_2}.(\phi\downarrow \vdash_{\mathsf{E}_1} M\downarrow)^{\rho_2}$. Since normalization is not effective, we can not compute $\nu\tilde{n}_{F_1}.(\phi\downarrow \vdash_{\mathsf{E}_1} M\downarrow)^{\rho_1}$ by simply mormalizing the terms and performing replacements. However, thanks to Lemma 25, it is sufficient to compute weak normal forms of the terms that occur in the problem and then to replace modulo E alien factors by names. This means that two factors that are equal modulo E are replaced by the same name. This is effective by relying on the fact that the word problem modulo E is decidable. □

Algorithm. Given a frame ϕ and a term M (not necessarily in normal form), we saturate ϕ as follows.

– we start with $\phi_0 = \phi \cup \{n_{min}\}$,

– for any term $T \in St(\phi \cup \{M\})$, if we have $\phi_k\downarrow \vdash_{\mathsf{E}_1} T\downarrow$ or $\phi_k\downarrow \vdash_{\mathsf{E}_2} T\downarrow$ (which is decidable thanks to Lemma 42) we add T to the set of deducible subterms: $\phi_{k+1} = \phi_k \cup \{T\}$.

We make a fixpoint iteration until no more terms are added in ϕ_k. Let ϕ^* be the saturated set. Using Lemma 27, we can show (Claim 1) that ϕ^* contains (modulo E) the set of all deducible subterms of $St(\phi \cup \{M\})$. We deduce that $\phi \vdash_{\mathsf{E}} M$ if and only if there exists $M' \in \phi^*$ such that $M =_{\mathsf{E}} M'$.

The following claim shows the correctness of the saturation algorithm.

Claim 1. *We have* $\phi^* =_{\mathsf{E}} \{T \mid \phi \vdash_{\mathsf{E}} T \text{ and } T \in St(\phi \cup \{M\})\} \cup \{n_{min}\}$.

Proof. Let $d(\phi, M) = \{T \mid \phi \vdash_{\mathsf{E}} T \text{ and } T \in St(\phi \cup \{M\})\}$. We show both inclusions separately.

• $\phi^* \subseteq d(\phi, M) \cup \{n_{min}\}$.

We show by induction on k that $\phi_k \subseteq d(\phi, M) \cup \{n_{min}\}$. The base case, that is $\phi_0 \subseteq d(\phi, M) \cup \{n_{min}\}$, is obvious. Assume now that for every $U \in \phi_k$, U is deducible, that is $\phi \vdash_{\mathsf{E}} U$. We have $\phi_{k+1} = \phi_k \cup \{T\}$ with $T \in St(\phi \cup \{M\})$ such that $\phi_k\downarrow \vdash_{\mathsf{E}_1} T\downarrow$, thus $\phi \vdash_{\mathsf{E}} T$ and thus we have that $\phi_{k+1} \subseteq d(\phi, M) \cup \{n_{min}\}$.

• $d(\phi, M) \cup \{n_{min}\} \subseteq_{\mathsf{E}} \phi^*$.

Clearly, we have that $n_{min} \in \phi^*$. Let $T \in St(\phi \cup \{M\})\downarrow$ be some deducible term, that is $\phi \vdash_{\mathsf{E}} T$. Thus $\phi\downarrow \vdash_{\mathsf{E}} T$ with T already in normal form. Lemma 27 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

$$\zeta'\sigma\downarrow \in St(\phi\downarrow \cup \{\zeta\sigma\downarrow\}) \cup \{n_{min}\} \qquad (*)$$

We show by induction on $|\zeta|$ that, whenever $\zeta\sigma\downarrow \in St(\phi \cup \{M\})\downarrow$ and for all $\zeta' \in St(\zeta)$, the property (*) holds, then $\zeta\sigma\downarrow \in \phi^*\downarrow$.

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. Thanks to Lemma 19, we have that $\zeta\sigma\downarrow = \zeta(\sigma\downarrow)\downarrow_{\mathsf{E}_1}$. Hence, we deduce that $\zeta(\sigma\downarrow) =_{\mathsf{E}_1} \zeta\sigma\downarrow$, i.e. $\phi\downarrow \vdash_{\mathsf{E}_1} \zeta\sigma\downarrow$. Thus we have that $\zeta\sigma\downarrow \in \phi^*\downarrow$.

Induction step. Assume that $\zeta = \zeta_0[\zeta_1, \ldots, \zeta_k]$. We have that $\zeta_i\sigma\downarrow \in St(\phi\downarrow \cup \{\zeta\sigma\downarrow\}) \cup \{n_{min}\}$ for $1 \leq i \leq k$. Actually, thanks to Corollary 17, we have that $\zeta_i\sigma\downarrow \in St(\phi \cup \{\zeta\sigma\downarrow\})\downarrow \cup \{n_{min}\}$. Since $\zeta\sigma\downarrow \in St(\phi \cup \{M\})\downarrow$, we deduce that $\zeta_i\sigma\downarrow \in St(\phi \cup \{M\})\downarrow \cup \{n_{min}\}$. Since $|\zeta_i| < |\zeta|$, applying the induction hypothesis, we deduce that $\zeta_i\sigma\downarrow \in \phi^*\downarrow$. W.l.o.g. we assume that $\mathsf{sign}(\zeta_0) = \Sigma_1$. Thus, we have that $\phi^*\downarrow \vdash_{\mathsf{E}_1} \zeta_0[\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow]$.

Thanks to Lemma 19, we deduce that $\phi^*\downarrow \vdash_{\mathsf{E}_1} \zeta_0[\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow]\downarrow$, i.e. $\phi^*\downarrow \vdash_{\mathsf{E}_1} \zeta\sigma\downarrow$. Thus we have that $\zeta\sigma\downarrow \in \phi^*\downarrow$. □

Example 31. *Consider Example 28, we successively add in the frame the terms n_{min}, n_1, n_4, $n_1 + n_2$, n_3, n_2 and $n_2 + n_3$.*

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 functions 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. Similarly, the DAG-size of a set S is the number of distinct syntactic subterms of terms in S. The DAG-size of a frame ϕ is defined to be the number of distinct syntactic subterms of terms in ϕ *plus* the size of $dom(\phi)$, to take into account the variables of $dom(\phi)$.

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 $f_i : \mathbb{N} \to \mathbb{R}$, $i \in \{1, 2\}$, and we assume that $M =_{\mathsf{E}} N$ can be decided in time $f_0(t_{\mathsf{dag}}(N) + t_{\mathsf{dag}}(M))$ where $f_0 : \mathbb{N} \to \mathbb{R}$. We also assume that the f_i are non-decreasing functions.

Saturating ϕ requires at most $|St(\phi \cup \{M\})| \leq t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)$ steps. Let $A_0 = t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)$.

At each step, we check whether $\nu\tilde{n}_{F_2}.(\phi_k\downarrow \vdash_{\mathsf{E}_1} T\downarrow)^{\rho_2}$ and $\nu\tilde{n}_{F_1}.(\phi_k\downarrow \vdash_{\mathsf{E}_2} T\downarrow)^{\rho_1}$ for each $T \in St(\phi \cup \{M\})$. $(\phi_k\downarrow)^{\rho_i}$ and $(T\downarrow)^{\rho_i}$ can be computed in polynomial time. Indeed, we first have to put term in weak normal forms. A weak normal form of a term T can be computed in $t_{\mathsf{dag}}(T)$. Moreover, the resulting term T' will be such that $T' \in St(T)$ and thus $t_{\mathsf{dag}}(T') \leq t_{\mathsf{dag}}(T)$. In the same way, a weak normal form of the frame ϕ_k can be computed in $t_{\mathsf{dag}}(\phi_k) \cdot dom(\phi_k) \leq t_{\mathsf{dag}}(\phi_k)^2$. Moreover, the resulting frame ϕ'_k is such that $t_{\mathsf{dag}}(\phi'_k) \leq t_{\mathsf{dag}}(\phi_k)$. Then, we have to duplicate some nodes of the DAG representation of ϕ'_k and T' such that the fathers of a node are all from the same signature (either Σ_1 or Σ_2). It is then sufficient to check for equality in E for each factor of ϕ'_k and T' and replace equal alien subterms by equal fresh names. There are at most $t_{\mathsf{dag}}(\phi'_k) + t_{\mathsf{dag}}(T')$ equality tests, each of the form $N_1 = N_2$, with $N_1, N_2 \in St(\phi'_k \cup \{T'\})$. Each equality test is performed in at most $f_0(t_{\mathsf{dag}}(N_1) + t_{\mathsf{dag}}(N_2))$. Thus, this can be done in at most

$$(t_{\mathsf{dag}}(\phi'_k) + t_{\mathsf{dag}}(T'))(f_0(2(t_{\mathsf{dag}}(\phi'_k) + t_{\mathsf{dag}}(T'))))$$

Note that at each step, the frame ϕ_k is of the same DAG-size than $\phi \cup \{M\}$ plus the number of added terms, that is at most the cardinality of $St(\phi \cup \{M\})$. We thus have that

$$t_{\mathsf{dag}}(\phi'_k) \leq t_{\mathsf{dag}}(\phi_k) \leq (t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)) + (t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)) \leq 2A_0.$$

Moreover, since $T' \in St(T)$ and $T \in St(\phi \cup \{M\})$, we have that

$$t_{\mathsf{dag}}(T') \leq t_{\mathsf{dag}}(T) \leq t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M) = A_0.$$

Thus computing $(\phi_k\downarrow)^{\rho_i}$ and $(T\downarrow)^{\rho_i}$ can be done in at most

$$4{A_0}^2 + A_0 + 3A_0 f_0(6A_0) \leq 4{A_0}^2 + A_0 + 3A_0 f_0(6A_0).$$

It then remains to check whether $\nu\tilde{n}_{F_2}.(\phi_k\downarrow \vdash_{\mathsf{E}_1} T\downarrow)^{\rho_2}$ or $\nu\tilde{n}_{F_1}.(\phi_k\downarrow \vdash_{\mathsf{E}_2} T\downarrow)^{\rho_1}$. We have just seen that computing $(\phi_k\downarrow)^{\rho_i}$ and $(T\downarrow)^{\rho_i}$ requires to at most duplicate all nodes thus

$$t_{\mathsf{dag}}((\phi_k\downarrow)^{\rho_i}) \leq 2t_{\mathsf{dag}}(\phi_k) \leq 4A_0$$

and

$$t_{\mathsf{dag}}((T\downarrow)^{\rho_i}) \leq 2t_{\mathsf{dag}}(T) \leq 2(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)) = 2A_0.$$

Hence, we deduce that ϕ^* can be computed in time

$$\mathcal{O}(A_0[f_1(6A_0) + f_2(6A_0) + 2(4{A_0}^2 + A_0 + 3A_0 f_0(6A_0))]$$

where $A_0 = t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(M)$. In particular, if deciding $\vdash_{\mathsf{E}_i}$ and $=_{\mathsf{E}_i}$ 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. Combining algorithms for static equivalence

Our second combination result regards static equivalence.

Theorem 32. *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 the equational theory $(\Sigma_1 \cup \Sigma_2, \mathsf{E}_1 \cup \mathsf{E}_2)$.*

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 26), 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 [2] works only when there exists a free function symbol in Σ_1.

Our decision procedure works as follows:

- *Step 1*: We first add to the frames all their deducible subterms. This is the reason why we require the decidability of $\vdash_{\mathsf{E}}$. We show that we can perform such a transformation preserving static equivalence (Lemma 38).
- *Step 2*: 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 $\phi_1 \models \mathsf{Eq}_{\mathsf{E}_2}(\phi_2)$ (Proposition 39).
- *Step 3*: Lastly, we abstract alien subterms by fresh names in order to reduce the signature (Lemma 41).

The rest of the section is devoted to the (sketch of the) proof of the following theorem. Omitted proofs and a detailed analysis of the complexity of our combination algorithm can be found in Appendix C.

5.1. Step 1: adding deducible terms to the frames

Let $\phi = \nu\tilde{n}.\sigma$ be a frame. A recipe ζ is *compatible* with ϕ if $fn(\zeta) \cap \tilde{n} = \emptyset$ and $fv(\zeta) \subseteq dom(\phi)$.

Definition 33. ($\overline{\phi}^{\Pi}$). *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and $\Pi = \zeta_1, \ldots, \zeta_\ell$ be a sequence of recipes compatible with ϕ. We define $\overline{\phi}^{\Pi}$ to be:*

$$\overline{\phi}^{\Pi} = \nu\tilde{n}.\sigma \cup \{{}^{\zeta_1\sigma}/_{y_1}, \ldots, {}^{\zeta_\ell\sigma}/_{y_\ell}\}$$

where for $i \in \{1, \ldots, \ell\}$, y_i is a fresh variable.

Example 34. *Let $\phi = \nu n_1, n_2.\{{}^{\mathsf{enc}(n_1,n_2)}/_{x_1}\}$ and Π be the sequence $\mathsf{proj}_1(x_1), \mathsf{proj}_2(x_1), n_{min}$. We have that*

$$\overline{\phi}^{\Pi} = \nu n_1, n_2.\{{}^{\mathsf{enc}(n_1,n_2)}/_{x_1}, {}^{\mathsf{proj}_1(\mathsf{enc}(n_1,n_2))}/_{y_1}, {}^{\mathsf{proj}_2(\mathsf{enc}(n_1,n_2))}/_{y_2}, {}^{n_{min}}/_{y_3}\}.$$

Let $\phi = \nu\tilde{n}.\sigma$ be a frame. We say that ϕ *contains all its deducible subterms* if $\{M \mid M \in St(\phi) \text{ and } \phi \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \phi$.

Example 35. *Consider the frame $\phi = \nu n_2, n_3.\{{}^{\mathsf{enc}(\langle n_1+n_2, n_3\rangle, n_4)}/_{x_1}\}$ given in Example 28 and let $\mathsf{E} = \mathsf{E}_{\mathsf{enc}} \cup \mathsf{E}_{\mathsf{xor}}$. Clearly, ϕ does not contain all its deducible subterms. Let Π be the sequence $\mathsf{proj}_1(\mathsf{dec}(x_1, n_4))$, $\mathsf{proj}_1(\mathsf{dec}(x_1, n_4)) + n_1$, $\mathsf{proj}_2(\mathsf{dec}(x_1, n_4))$, n_1, n_4, n_{min}. We have that:*

$$\overline{\phi}^{\Pi} =_{\mathsf{E}} \nu n_2, n_3.\{{}^{\mathsf{enc}(\langle n_1+n_2, n_3\rangle, n_4)}/_{x_1}, {}^{n_1+n_2}/_{y_1}, {}^{n_2}/_{y_2}, {}^{n_3}/_{y_3}, {}^{n_1}/_{y_4}, {}^{n_4}/_{y_5}, {}^{n_{min}}/_{y_6}\}.$$

Lemma 36. *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and Π be a sequence of recipes compatible with ϕ such that:*

1. $St(\Pi) \subseteq \Pi \cup dom(\phi)$;
2. $\{M \mid M \in St(\phi) \text{ and } \phi \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \{\zeta\sigma \mid \zeta \in \Pi\} \cup \phi$.

We have that $\overline{\phi}^{\Pi}$ contains all its deducible subterms.

Proof. We have to show that:

$$\{M \mid M \in St(\overline{\phi}^{\Pi}) \text{ and } \overline{\phi}^{\Pi} \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \overline{\phi}^{\Pi}.$$

We have that: $St(\overline{\phi}^{\Pi}) = St(\phi) \cup \bigcup_{\zeta\in\Pi} St(\zeta\sigma) = St(\phi) \cup \{\zeta\sigma \mid \zeta \in \Pi\}$. The last equality comes from our hypothesis 1. Hence, we have that:

$$\begin{array}{ll} & \{M \mid M \in St(\overline{\phi}^{\Pi}) \text{ and } \overline{\phi}^{\Pi} \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \\ = & \{M \mid M \in St(\phi) \text{ and } \phi \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \cup \{\zeta\sigma \mid \zeta \in \Pi\} \\ \subseteq_{\mathsf{E}} & \{\zeta\sigma \mid \zeta \in \Pi\} \cup \phi \qquad \text{thanks to our hypothesis 2} \\ = & \overline{\phi}^{\Pi} \end{array}$$

Hence we have that $\overline{\phi}^{\Pi}$ contains all its deducible subterms. □

Example 37. *Going back to Example 35, we have that:*

- $St(\Pi) \subseteq \Pi \cup dom(\phi)$ *since* $St(\Pi) = \Pi \cup \{x_1\}$;
- $\{M \mid M \in St(\phi) \text{ and } \phi \vdash_{\mathsf{E}} M\} = \phi \cup \{n_1, n_2, n_3, n_4, n_1 + n_2\}$;
- $\{\zeta\sigma\downarrow \mid \zeta \in \Pi\} \cup \phi = \{n_{min}, n_1, n_2, n_3, n_4, n_1 + n_2\} \cup \phi$.

Hence, according to Lemma 36, we have that $\overline{\phi}^{\Pi}$ contains all its deducible subterms. This is indeed the case.

The following lemma ensures that extending frames preserves static equivalence.

Lemma 38. *Let $\phi_1 = \nu\tilde{n}.\sigma_1$ and $\phi_2 = \nu\tilde{n}.\sigma_2$ be two frames such that $dom(\phi_1) = dom(\phi_2)$. For any sequence Π of recipes compatible with ϕ_1 (and ϕ_2), we have that:*

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

Proof. ($\Rightarrow$) Assume that $\overline{\phi_2}^{\Pi} \models \mathsf{Eq}_{\mathsf{E}}(\overline{\phi_1}^{\Pi})$ and consider $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi_1)$. As $(\overline{\phi_1}^{\Pi})|_{dom(\phi_1)} = \phi_1$ and $(\overline{\phi_2}^{\Pi})|_{dom(\phi_1)} = \phi_2$, it follows that $(M =_{\mathsf{E}} N)\overline{\phi_1}^{\Pi}$, thus $(M =_{\mathsf{E}} N)\overline{\phi_2}^{\Pi}$, that is $(M =_{\mathsf{E}} N)\phi_2$.
($\Leftarrow$) Assume that $\phi_2 \models \mathsf{Eq}_{\mathsf{E}}(\phi_1)$ and consider $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\overline{\phi_1}^{\Pi})$. Let $\Pi = \zeta_1, \ldots, \zeta_n$. We have that $\overline{\phi_1}^{\Pi} = \phi_1 \cup \{^{\zeta_1\sigma_1}/_{y_1}, \ldots, ^{\zeta_n\sigma_1}/_{y_n}\}$. Let $M' = M\theta$ and $N' = N\theta$ where $\theta = \{^{\zeta_1}/_{y_1}, \ldots, ^{\zeta_n}/_{y_n}\}$. Since $(M =_{\mathsf{E}} N)\overline{\phi_1}^{\Pi}$, we have that $(M' =_{\mathsf{E}} N')\phi_1$, i.e. $(M', N') \in \mathsf{Eq}(\phi_1)$. Since $\phi_2 \models \mathsf{Eq}_{\mathsf{E}}(\phi_1)$, we have $(M' =_{\mathsf{E}} N')\phi_2$, and thus $(M =_{\mathsf{E}} N)\overline{\phi_2}^{\Pi}$. □

Thanks to Lemma 38, we deduce that deciding whether $\phi_1 \approx_{\mathsf{E}} \phi_2$ is thus equivalent to deciding whether $\overline{\phi_1}^{\Pi} \approx_{\mathsf{E}} \overline{\phi_2}^{\Pi}$ (for any suitable sequence Π). We are looking for a sequence Π such that $\overline{\phi_1}^{\Pi}$ and $\overline{\phi_2}^{\Pi}$ contain all their deducible subterms. Thanks to Lemma 36, we know that it is sufficient to chose a set Π such that:

1. $St(\Pi) \subseteq \Pi \cup dom(\phi_i)$;
2. $\{M \mid M \in St(\phi_1) \text{ and } \phi_1 \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \{\zeta\sigma_1 \mid \zeta \in \Pi\} \cup \phi_1$;
3. $\{M \mid M \in St(\phi_2) \text{ and } \phi_2 \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \{\zeta\sigma_2 \mid \zeta \in \Pi\} \cup \phi_2$.

Computing Π. To compute such a set Π, we need to compute the set of deducible subterms of ϕ_1 (resp. ϕ_2). Moreover, for each deducible subterm T of ϕ_1 (resp. ϕ_2), we also need to compute a recipe ζ_T of T in ϕ_1 (resp. ϕ_2) modulo E. Such a recipe can usually be deduced from the decision algorithm applied to $\phi_1 \vdash_{\mathsf{E}} T$ (resp. $\phi_2 \vdash_{\mathsf{E}} T$). However, if it is not the case, once we know that $\phi_1 \vdash_{\mathsf{E}} T$ (resp. $\phi_2 \vdash_{\mathsf{E}} T$) using the decision algorithm, we can enumerate all the recipes until we find such a ζ_T. Once we have computed a recipe for each deducible subterm T of ϕ_1 (resp. ϕ_2), we obtain a set Π'. In order to obtain a set Π satisfying the three conditions stated above, it is sufficient to consider $\Pi = St(\Pi')$.

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 39. *Let ϕ and ψ be two frames in normal form such that ϕ contains all its deducible subterms. 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 $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$. To prove the converse, we consider the following ordering on pairs 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 that $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$ implies $(M =_{\mathsf{E}} N)\psi$.

When $(\max(|M|, |N|), |M| + |N|) \leq (1, 1)$, we have that $(M, N) \in \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ (or $(M, N) \in \mathsf{Eq}_{\mathsf{E}_2}(\phi)$) and we easily conclude. Otherwise, we distinguish the following cases (detailed in Appendix C):

- There exists $\zeta \in Fct(M)$ (or $\zeta \in Fct(N)$) such that $\zeta\sigma\downarrow \in St(\phi)$. By relying on the fact that ϕ contains all its deducible subterms, we know that there exists a variable x in $dom(\phi)$ such that $(\zeta =_{\mathsf{E}} x)\phi$. By using our induction hypothesis, we deduce that $(\zeta =_{\mathsf{E}} x)\psi$. This will allow us to build a term M' that is smaller than M such that $(M =_{\mathsf{E}} M')\phi$ and $(M =_{\mathsf{E}} M')\psi$. Then, by relying again on our induction hypothesis, we deduce from $(M' =_{\mathsf{E}} N)\phi$ that $(M' =_{\mathsf{E}} N)\psi$, and thus $(M =_{\mathsf{E}} N)\psi$.

- The same kind of reasoning holds when there exists $\zeta \in Fct(M)$ (or $\zeta \in Fct(N)$) such that $\mathsf{sign}(\zeta\sigma) \neq \mathsf{sign}(\zeta\sigma\downarrow)$. By relying on the fact that ϕ contains all its deducible subtems, we will find M' such that $|M'| \leq |M|$, $(M =_{\mathsf{E}} M')\phi$ and $(M =_{\mathsf{E}} M')\psi$ (this is formally stated in Lemma 40). Then, using again our induction hypothesis, we deduce that $(M' =_{\mathsf{E}} N)\psi$, and thus $(M =_{\mathsf{E}} N)\psi$.

- Otherwise, we can built a smaller test (M', N') by abstracting some of the factors of M and N by fresh names. We will still have that $(M' =_{\mathsf{E}} N')\phi$. By relying on our induction hypothesis, we deduce that $(M' =_{\mathsf{E}} N')\psi$. Then, it remains to go back to the test (M, N) by replacing the fresh names by the original terms, still preserving the equality.

Lemma 40. *Let $\phi = \nu\tilde{n}.\sigma$ and $\psi = \nu\tilde{n}.\sigma'$ be two frames in normal form such that ϕ contains all its deducible subterms, $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$. Let $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$ be such that $(fn(M) \cup fn(N)) \cap \tilde{n} = \emptyset$ and assume that for all terms M', N'*

$$(M', N') < (M, N) \quad \textit{implies} \quad (M' =_{\mathsf{E}} N')\phi \Rightarrow (M' =_{\mathsf{E}} N')\psi.$$

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 $(M =_{\mathsf{E}} M_1)\psi$.

The proofs of Lemma 40 and Proposition 39 are given in Appendix C.

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 41. *Let ϕ and ψ be two frames built on Σ. 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 the same cardinality as F_2 and $\rho_2 : F_2 \to \tilde{n}_{F_2}$ a replacement. Assume that ϕ and ψ are in normal form. We have that*

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

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

Proof. ($\Rightarrow$) Let $(M, N) \in \mathsf{Eq}_{\mathsf{E}_1}(\nu\tilde{n}_{F_2}.\psi^{\rho_2})$. 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 by substitutions of terms for 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 $\tilde{n}_{F_2} \notin fn(M)$, and
- $(N\psi^{\rho_2})^{\rho_2{}^{-1}} = N(\psi^{\rho_2})^{\rho_2{}^{-1}} = N\psi$ since $\tilde{n}_{F_2} \notin fn(N)$.

This allows us to obtain that $(M =_{\mathsf{E}_1} N)\psi$. Now, since $\phi \models \mathsf{Eq}_{\mathsf{E}_1}(\psi)$, 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 19, yielding to $(M\sigma)^{\rho_2}{\downarrow} = (M\sigma)^{\rho_2}{\downarrow_{\mathsf{E}_1}}$. We deduce that

$$(M\sigma)^{\rho_2}{\downarrow} =_{\mathsf{E}_1} (M\sigma)^{\rho_2} \tag{4}$$

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 20, yielding to

$$(M\sigma)^{\rho_2}\downarrow = (M\sigma)\downarrow^{\rho_2}\downarrow \qquad (N\sigma)^{\rho_2}\downarrow = (N\sigma)\downarrow^{\rho_2}\downarrow \tag{5}$$

By the equalities (5) 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 (4), we obtain $(M\sigma)^{\rho_2} =_{\mathsf{E}_1} (N\sigma)^{\rho_2}$. 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 $(fn(M) \cup fn(N)) \cap \tilde{n}_{F_2} = \emptyset$. 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 19, yielding to $(M\sigma)^{\rho_2}\downarrow = (M\sigma)^{\rho_2}\downarrow_{\mathsf{E}_1}$. We deduce that

$$(M\sigma)^{\rho_2}\downarrow =_{\mathsf{E}_1} (M\sigma)^{\rho_2} \tag{6}$$

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 20, yielding to

$$(M\sigma)^{\rho_2}\downarrow = (M\sigma)\downarrow^{\rho_2}\downarrow \qquad (N\sigma)^{\rho_2}\downarrow = (N\sigma)\downarrow^{\rho_2}\downarrow \tag{7}$$

By the equalities (7) 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 (6), we obtain $(M\sigma)^{\rho_2} =_{\mathsf{E}_1} (N\sigma)^{\rho_2}$. 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 $\nu\tilde{n}_{F_2}.\phi^{\rho_2} \models \mathsf{Eq}_{\mathsf{E}_1}(\nu\tilde{n}_{F_2}.\psi^{\rho_2})$, we deduce that $(M =_{\mathsf{E}_1} N)\phi^{\rho_2}$. Since E_1 is closed by substitutions of terms for 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 $\tilde{n}_{F_2} \cap fn(M) = \emptyset$. For the same reason, we have that $(N\phi^{\rho_2})^{{\rho_2}^{-1}} = N\phi$. This allows us to conclude. □

5.4. Combination algorithm for static equivalence

Similarly to the deduction case, we first show that $\phi_1\downarrow \approx_{\mathsf{E}_i} \phi_2\downarrow$ is decidable. This is used as a sub-task in our combination algorithm for static equivalence.

Lemma 42. *The following problem is decidable.*

Entries: *Two frames ϕ_1 and ϕ_2, $i \in \{1, 2\}$ and F_1, F_2, ρ_1, ρ_2 defined like in Lemma 41.*

Question: $\phi_1{\downarrow} \approx_{\mathsf{E}_i} \phi_2{\downarrow}$*?*

Proof. Without loss of generality, let us show that $\phi_1{\downarrow} \approx_{\mathsf{E}_1} \phi_2{\downarrow}$ is decidable. Thanks to Lemma 41, it suffices to check whether we have that $\nu\tilde{n}_{F_2}.\phi_1{\downarrow}^{\rho_2} \approx_{\mathsf{E}_1} \nu\tilde{n}_{F_2}.\phi_2{\downarrow}^{\rho_2}$. Since normalization is not effective, we have to compute $\nu\tilde{n}_{F_2}.(\phi_1{\downarrow})^{\rho_2}$ and $\nu\tilde{n}_{F_2}.(\phi_2{\downarrow})^{\rho_2}$ without normalizing terms. For this, we rely on Lemma 25. It is actually sufficient to compute weak normal forms of the terms that occur in the problem and then to replace modulo E alien factors by names. This means that two factors that are equal modulo E are replaced by the same name. This is effective by relying on the fact that the word problem modulo E is decidable. Note that checking whether $M =_{\mathsf{E}_i} N$ amounts to check whether $\{^M/_x\} \approx_{\mathsf{E}_i} \{^N/_x\}$. Hence decidability of $=_{\mathsf{E}}$ is a consequence of the facts that $\approx_{\mathsf{E}_1}$ and $\approx_{\mathsf{E}_2}$ are decidable by relying on a well-known combination result [9]. □

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

1. computing $\phi'_1 = \overline{\phi_1}^{\Pi}$ and $\phi'_2 = \overline{\phi_2}^{\Pi}$ where Π is a set of recipes compatible with ϕ_1 (and ϕ_2) such that:

   $St(\Pi) \subseteq \Pi \cup dom(\phi_i)$;
   $\{M \mid M \in St(\phi_1) \text{ and } \phi_1 \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \{\zeta\sigma_1 \mid \zeta \in \Pi\} \cup \phi_1$;
   $\{M \mid M \in St(\phi_2) \text{ and } \phi_2 \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \{\zeta\sigma_2 \mid \zeta \in \Pi\} \cup \phi_2$.

2. checking for $\phi'_1{\downarrow} \approx_{\mathsf{E}_1} \phi'_2{\downarrow}$ and $\phi'_1{\downarrow} \approx_{\mathsf{E}_2} \phi'_2{\downarrow}$.

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 $f_i(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(\psi))$ for $i \in \{1, 2\}$.
- $M =_{\mathsf{E}} N$ can be decided in $f_0(t_{\mathsf{dag}}(M) + t_{\mathsf{dag}}(N))$. Since $M =_{\mathsf{E}_i} N$ can be decided by checking whether $\{^M/_x\} \approx_{\mathsf{E}_i} \{^N/_x\}$, we can decide $=_{\mathsf{E}_i}$ using the decidability of $\approx_{\mathsf{E}_i}$ and then combine the algorithms to get the decidability of $=_{\mathsf{E}}$ (see [9]). In particular, if f_1 and f_2 are polynomial, then f_0 is polynomial. However, it is

often the case that an easier algorithm exists for the word problem for E.

Then it is easy to check (see Appendix C) that $\phi \approx_{\mathsf{E}} \psi$ can be decided in a time that can expressed as a polynomial in $f_i(P(f_5(Q(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(\psi))), t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(\psi)))$ with $i \in \{0, \ldots, 5\}$ where P and Q are polynomials. In particular, if the f_i are polynomial, $\approx_{\mathsf{E}}$ is decidable in polynomial time.

— PART II: Monoidal theories —

In this part of the paper, we develop a general approach for deciding deduction and static equivalence for the class of monoidal theories introduced by F. Baader [4] and W. Nutt [31]. This class captures many theories with associative and commutative properties (AC), which are known to be difficult to deal with. Actually, we propose a general schema for deciding deduction and static equivalence. This schema has to be filled with procedures for linear equations in order to yield complete algorithms. Such algorithms strongly depend on the structure of the semiring associated to a monoidal theory. We will see in Part III that Algebra provides useful techniques and results to fill in this gap.

In Section 6, we define the central notion of monoidal theory. We show how monoidal theories are related to semirings and how to represent terms (resp. frames) by means of vectors (resp. matrices) over semirings. Then Section 7 and 8 are devoted to the study of deduction and static equivalence respectively.

6. Monoidal theories

Monoidal theories generalise the equational theories AC, *exclusive or*, ... In this section, we first define monoidal theories and then give examples.

Definition 43. (monoidal theory). *A theory* E *over* Σ *is called* monoidal *if it satisfies the following properties:*

1. *The signature* Σ *contains a binary function symbol* $+$ *and a constant symbol* 0*, and all other function symbols in* Σ *are unary.*
2. *The symbol* $+$ *is associative-commutative with unit* 0, i.e. *the equations* $x + (y + z) = (x + y) + z$, $x + y = y + x$ *and* $x + 0 = x$ *are in* E.
3. *Every unary function symbol* $\mathsf{h} \in \Sigma$ *is an endomorphism for* $+$ *and* 0, *i.e.* $\mathsf{h}(x + y) = \mathsf{h}(x) + \mathsf{h}(y)$ *and* $\mathsf{h}(0) = 0$ *are in* E.

Example 44. *Suppose* $+$ *is a binary function symbol and* 0 *is nullary. Moreover assume that the others symbols,* i.e $-$, h*, are unary symbols. The equational theories below are monoidal.*

- *The theory* ACU *over* $\Sigma = \{+, 0\}$ *which consists of the axioms of associativity and commutativity with unit* 0.

– *The theory* ACUI *over* $\Sigma = \{+, 0\}$ *which consists of the axioms* (AC), (U), *and the axiom of Idempotency* (I) $x + x = x$.

– *The theory* ACUN *(*exclusive or*, previously denoted* E_+*) over* $\Sigma = \{+, 0\}$ *which consists of the axioms* (AC), (U), *and the axiom of Nilpotency* (N) $x + x = 0$.

– *The theory* AG *(*Abelian groups*) over* $\Sigma = \{+, -, 0\}$ *which is generated by the axioms* (AC), (U) *and* $x + -(x) = 0$ (Inv). *Indeed, the equations* $-(x+y) = -(x)+-(y)$ *and* $-0 = 0$ *are consequences of the others.*

– *The theories* ACUh, ACUIh, ACUNh *over* $\Sigma = \{+, \mathsf{h}, 0\}$ *and* AGh *over* $\Sigma = \{+, -, \mathsf{h}, 0\}$*: these theories correspond to the ones described above extended by the homomorphism laws* (h) *for the symbol* h, i.e. $\mathsf{h}(x + y) = \mathsf{h}(x) + \mathsf{h}(y)$ *and* $\mathsf{h}(0) = 0$ *(if it is not a consequence of the other equations).*

Note that there are two homomorphisms in the theory AGh, namely $-$ and h. These two homomorphisms commute: $\mathsf{h}(-x) = -(\mathsf{h}(x))$ is a consequence of the others. Other examples of monoidal theories can be found in [31].

It has been shown that the deduction problem for ACU amounts to solving linear equations over the semiring $\mathbb{N}$ whereas for AGh this problem amounts to solving linear equations over the ring $\mathbb{Z}[\mathsf{h}]$, the ring of polynomials in one indeterminate with coefficients over $\mathbb{Z}$ [21]. Some results of this kind also exist in the case of static equivalence. For instance, static equivalence has been shown decidable for the equational theories ACUN and AC [2]. By using an algebraic characterization of the problem, we will generalize these results by associating to every monoidal theory E a semiring $\mathcal{S}_{\mathsf{E}}$, that will be used to solve the deduction and the static equivalence problems in E.

6.1. Monoidal theories define semirings

Monoidal theories have an algebraic structure close to rings except that elements might not have an additive inverse. Such a structure is called a *semiring*.

Definition 45. (semiring). *A* semiring *is a set* $\mathcal{S}$ *(called the* universe *of the semiring) with distinct elements* 0 *and* 1 *that is equipped with two binary operations* $+$ *and* $\cdot$ *such that* $(\mathcal{S}, +, 0)$ *is a commutative monoid,* $(\mathcal{S}, \cdot, 1)$ *is a monoid, and the following identities hold for all* $\alpha, \beta, \gamma \in \mathcal{S}$*:*

$$(\alpha+\beta)\cdot\gamma = \alpha\cdot\gamma + \beta\cdot\gamma \quad \textit{(right distributivity)}$$
$$\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta + \alpha\cdot\gamma \quad \textit{(left distributivity)}$$
$$0\cdot\alpha = \alpha\cdot 0 = 0 \quad \textit{(zero laws).}$$

We call the binary operations $+$ and $\cdot$ respectively the *addition* and the *multiplication* of the semiring. The elements 0 and 1 are called respectively *zero* and *unit*. In the sequel we will often omit the $\cdot$ sign and write $\alpha\beta$ instead of $\alpha\cdot\beta$. A semiring is *commutative* if its multiplication is commutative. Semirings are different from rings in that they need not be groups with respect to addition. Every ring is a semiring. In a ring, we will denote by $-\alpha$ the additive inverse of α, and we write $\alpha-\beta$ as an abbreviation of $\alpha+(-\beta)$.

It has been shown in [31] that for any monoidal theory E there exists a corresponding semiring $\mathcal{S}_{\mathsf{E}}$. We can rephrase the definition of $\mathcal{S}_{\mathsf{E}}$ as follows. Let $\mathbf{1}$ be a free constant ($\mathbf{1}\notin\Sigma$). The universe of $\mathcal{S}_{\mathsf{E}}$ is $\mathcal{T}(\Sigma,\{\mathbf{1}\})/\mathsf{E}$, that is the set of equivalence classes of terms built over Σ and $\mathbf{1}$ under equivalence by the equational axioms E. The constant 0 and the sum $+$ of the semiring are defined as in the algebra $\mathcal{T}(\Sigma,\{\mathbf{1}\})/\mathsf{E}$. The multiplication in the semiring is defined by $s\cdot t := s[\mathbf{1}\mapsto t]$ where $M[N_1\mapsto N_2]$ denotes the *replacement* of all occurrences of N_1 in M by N_2. As a consequence, $\mathbf{1}$ acts as a neutral element of multiplication in $\mathcal{S}_{\mathsf{E}}$. This is the reason why we call this new generator $\mathbf{1}$ instead of, say, x, as it is often done in the literature. It can be shown [31] that $\mathcal{S}_{\mathsf{E}}$ is a ring if, and only if, E is a group theory, and also that $\mathcal{S}_{\mathsf{E}}$ is commutative if, and only if, E has commuting homomorphisms, *i.e.* $\mathsf{h}_1(\mathsf{h}_2(x)) =_{\mathsf{E}} \mathsf{h}_2(\mathsf{h}_1(x))$ for any two homomorphisms h_1 and h_2. For instance, we have that

1. The semiring $\mathcal{S}_{\mathsf{ACU}}$ is isomorphic to $\mathbb{N}$, the semiring of natural numbers.

2. The semiring $\mathcal{S}_{\mathsf{ACUN}}$ consists of the two elements 0 and $\mathbf{1}$ and we have $0+\mathbf{1}=\mathbf{1}+0=\mathbf{1}$, $0+0=\mathbf{1}+\mathbf{1}=0$, $0\cdot 0=\mathbf{1}\cdot 0=0\cdot\mathbf{1}=0$, and $\mathbf{1}\cdot\mathbf{1}=\mathbf{1}$. Hence, $\mathcal{S}_{\mathsf{ACUN}}$ is isomorphic to the commutative ring (field) $\mathbb{Z}/2\mathbb{Z}$.

3. The semiring $\mathcal{S}_{\mathsf{AGh}}$ is isomorphic to $\mathbb{Z}[\mathsf{h}]$ which is a commutative ring.

Let b be a free symbol (name or variable). We denote by $\psi_b\colon \mathcal{T}(\Sigma,\{b\})\to\mathcal{S}_{\mathsf{E}}$ the function which maps any term $M\in\mathcal{T}(\Sigma,\{b\})$ to $M[b\mapsto\mathbf{1}]$ considered as an element of the semiring $\mathcal{S}_{\mathsf{E}}$.

Example 46. *Let* $\mathsf{E} = \mathsf{ACUN}$ *and* $t = b + b + b$. *We have* $\psi_b(t) = \mathbf{1} + \mathbf{1} + \mathbf{1} = \mathbf{1}$.

6.2. Representation of terms and frames

In this section, we show how to represent terms and frames by means of vectors and matrices over a semiring. For this, we introduce the notion of *base* to decompose terms and frames. We also consider frames which are saturated *w.r.t.* a base (see Definition 51). This will be convenient in the next two sections and can be easily achieved.

A *base* $\mathcal{B}$ is a sequence $[b_1, \ldots, b_m]$ of free symbols (names or variables), We say that $\mathcal{B}$ is a *base of names* when $b_1, \ldots, b_m$ are names.

Definition 47. (decomposable in a base). *A term* $M \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$ *is* decomposable *in* $\mathcal{B}$ *if* $fn(M) \cup fv(M) \subseteq \mathcal{B}$.

Let $\phi = \nu\tilde{n}.\{{}^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}\}$ *be a frame. We say that* ϕ *is* decomposable *in* $\mathcal{B}$ *if each* M_i *is decomposable in* $\mathcal{B}$.

Let $\mathcal{B} = [b_1, \ldots, b_m]$. We generalize the construction of the previous section and obtain a function which assigns to any term in $\mathcal{T}(\Sigma, \mathcal{B})$ a tuple in $\mathcal{S}_{\mathsf{E}}^m$, that is a tuple of m elements over $\mathcal{S}_{\mathsf{E}}$.

The function $\psi_{\mathcal{B}} \colon \mathcal{T}(\Sigma, \{b_1, \ldots, b_m\}) \to \mathcal{S}_{\mathsf{E}}^m$ is defined as follows: Any term $M \in \mathcal{T}(\Sigma, \{b_1, \ldots, b_m\})$ has a unique decomposition $M_1, \ldots, M_m$ such that $M = M_1 + \ldots + M_m$ with $M_i \in \mathcal{T}(\Sigma, \{b_i\})$ [31]. We define $\psi_{\mathcal{B}}(M) = (\psi_{b_1}(M_1), \ldots, \psi_{b_m}(M_m))$. Given a vector $X \in \mathcal{S}_{\mathsf{E}}^m$ of size m, $\psi_{\mathcal{B}}^{-1}(X)$ is a term $M \in \mathcal{T}(\Sigma, \mathcal{B})$ such that $\psi_{\mathcal{B}}(M) = X$. This term is uniquely defined modulo E.

Example 48. *Taking into account that the semiring* $\mathcal{S}_{\mathsf{AGh}}$ *is (isomorphic to)* $\mathbb{Z}[\mathsf{h}]$, *we have that* $\psi_{[b_1,b_2,b_3]}(b_1 + b_1 + \mathsf{h}(b_3) + \mathsf{h}(\mathsf{h}(\mathsf{h}(b_3)))) = (2, 0, \mathsf{h} + \mathsf{h}^3)$. *Indeed, we have that* $\psi_{b_1}(b_1 + b_1) = 2$, $\psi_{b_2}(0) = 0$ *and* $\psi_{b_3}(\mathsf{h}(b_3) + \mathsf{h}(\mathsf{h}(\mathsf{h}(b_3)))) = \mathsf{h} + \mathsf{h}^3$.

A term can be uniquely decomposed on a base $\mathcal{B}$. This can be extended to associate a (unique) matrix to a frame. Let $\phi = \nu\tilde{n}.\sigma$ be a frame and $\mathcal{B} = [b_1, \ldots, b_m]$ be a base of names in which ϕ is decomposable. Let $\sigma = \{{}^{M_1}/_{x_1} \ldots {}^{M_\ell}/_{x_\ell}\}$. We denote by $\psi_{\mathcal{B}}(\phi)$ the matrix of size $\ell \times m$ (ℓ rows and m columns) defined by $(\psi_{\mathcal{B}}(M_1); \ldots; \psi_{\mathcal{B}}(M_\ell))$. This matrix is the decomposition of ϕ in $\mathcal{B}$.

Example 49. *Consider the equational theory* ACU *given in Example 44 and let*

$$\phi = \nu n_1, n_2, n_3.\{{}^{3n_1+2n_2+3n_3}/_{x_1}, {}^{n_2+3n_3}/_{x_2}, {}^{3n_2+n_3}/_{x_3}, {}^{3n_1+n_2+4n_3}/_{x_4}\}$$

where the notation kn with $k \in \mathbb{N}$ denotes $n + \cdots + n$ (k times). Let $\mathcal{B} = [n_1, n_2, n_3]$. We have that

$$\psi_{\mathcal{B}}(\phi) = \begin{pmatrix} 3 & 2 & 3 \\ 0 & 1 & 3 \\ 0 & 3 & 1 \\ 3 & 1 & 4 \end{pmatrix} \quad \textit{since} \quad \begin{array}{l} - \ \psi_{\mathcal{B}}(3n_1 + 2n_2 + 3n_3) = (3, 2, 3), \\ - \ \psi_{\mathcal{B}}(n_2 + 3n_3) = (0, 1, 3), \\ - \ \psi_{\mathcal{B}}(3n_2 + n_3) = (0, 3, 1), \textit{ and} \\ - \ \psi_{\mathcal{B}}(3n_1 + n_2 + 4n_3) = (3, 1, 4). \end{array}$$

Applying a recipe to a frame is equivalent to multiplying the corresponding matrices.

Lemma 50. *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and ζ be a term in $\mathcal{T}(\Sigma, dom(\phi))$. Let $\mathcal{B}$ be a base of names in which we can decompose ϕ. We have that:*

$$\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{dom(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi).$$

Proof. Let $\sigma = \{{}^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}\}$ and ζ be a term in $\mathcal{T}(\Sigma, dom(\phi))$. We have that $\zeta = \zeta_1 + \ldots + \zeta_\ell$ for some $\zeta_i \in \mathcal{T}(\Sigma, \{x_i\})$.

$$\begin{array}{rcl} \psi_{\mathcal{B}}(\zeta\sigma) & = & \psi_{\mathcal{B}}(\zeta_1\sigma + \ldots + \zeta_\ell\sigma) \\ & = & \psi_{\mathcal{B}}(\zeta_1[x_1 \mapsto M_1] + \ldots + \zeta_\ell[x_\ell \mapsto M_\ell]) \\ & = & \psi_{\mathcal{B}}(\zeta_1[x_1 \mapsto M_1]) + \ldots + \psi_{\mathcal{B}}(\zeta_\ell[x_\ell \mapsto M_\ell]) \\ & = & \psi_{x_1}(\zeta_1) \cdot \psi_{\mathcal{B}}(M_1) + \ldots + \psi_{x_\ell}(\zeta_\ell) \cdot \psi_{\mathcal{B}}(M_\ell) \\ & = & \psi_{dom(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi) \end{array}$$

□

Note that to apply the equation stated in Lemma 50, the recipe ζ has to be built without names. To ensure that such kind of recipes always exist, we will work with frames saturated w.r.t. $\mathcal{B}$ (base of names in which the frames are decomposable).

Definition 51. (frame saturated w.r.t. $\mathcal{B}$). *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and $\mathcal{B}$ be a base of names $[b_1, \ldots, b_m]$ in which ϕ is decomposable. We say that ϕ is* saturated *w.r.t. $\mathcal{B}$ if for each $b_i \in \mathcal{B}$ such that $b_i \notin \tilde{n}$ we have that $b_i = x\sigma$ for some $x \in dom(\phi)$.*

Given a frame $\phi = \nu\tilde{n}.\{{}^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}\}$ and a base of names $\mathcal{B} = [b_1, \ldots, b_k]$ in which ϕ is decomposable, we denote by $\overline{\phi}^{\mathcal{B}}$ the frame defined as follows:

$$\overline{\phi}^{\mathcal{B}} = \nu\tilde{n}.\{{}^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}, {}^{b_{i_1}}/_{y_1}, \ldots, {}^{b_{i_p}}/_{y_p}\}$$

where $b_{i_1}, \ldots, b_{i_p}$ is a subsequence of $\mathcal{B}$ such that $b_{i_j} \notin \tilde{n}$ and $b_{i_j} \neq x\sigma$ for every $x \in dom(\phi)$. The variables $y_1, \ldots y_p$ are fresh, which means that they do not appear in $dom(\phi)$. Note that the resulting frame $\overline{\phi}^{\mathcal{B}}$ is saturated w.r.t. $\mathcal{B}$.

Example 52. *Let ϕ be the frame given in Example 49. Let $\mathcal{B} = [n_1, n_2, n_3]$. We have that ϕ is decomposable on $\mathcal{B}$ and also that ϕ is saturated w.r.t. $\mathcal{B}$. However, note that ϕ is not saturated w.r.t. $\mathcal{B}' = [n_1, n_2, n_3, n_4]$. We have that*

$$\overline{\phi}^{\mathcal{B}'} = \nu n_1, n_2, n_3.\{{}^{3n_1+2n_2+3n_3}/_{x_1}, {}^{n_2+3n_3}/_{x_2}, {}^{3n_2+n_3}/_{x_3}, {}^{3n_1+n_2+4n_3}/_{x_4}, {}^{n_4}/_{y_1}\}.$$

7. Deduction

We show that solving a deduction problem can be reduced to solving a linear system of equations in the corresponding semiring.

Theorem 53. *Let E be a monoidal theory and $\mathcal{S}_{\mathsf{E}}$ be its associated semiring. Deduction in E is reducible in polynomial time to the following problem:*

Entries*: A matrix A over $\mathcal{S}_{\mathsf{E}}$ of size $\ell \times m$ and a vector b over $\mathcal{S}_{\mathsf{E}}$ of size ℓ*

Question*: Does there exist X (a vector over $\mathcal{S}_{\mathsf{E}}$ of size ℓ) such that $X \cdot A = b$?*

Note that when $\mathcal{S}_{\mathsf{E}}$ is commutative, this problem is equivalent to the problem of deciding whether $A^{\mathsf{T}} \cdot Y = b^{\mathsf{T}}$, *i.e* whether b^{T} is in the image of A^{T} where M^{T} is the transpose of M. Before proving the reduction we need to establish that we can restrict our attention to saturated frames. Moreover, for such frames, it is sufficient to consider recipes without names, *i.e.* such that $fn(\zeta) = \emptyset$.

Lemma 54. *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and M be a ground term. Let $\mathcal{B}$ be a base of names in which ϕ and M are decomposable. We have that $\phi \vdash_{\mathsf{E}} M$ if and only if $\overline{\phi}^{\mathcal{B}} \vdash_{\mathsf{E}} M$. Moreover when $\overline{\phi}^{\mathcal{B}} \vdash_{\mathsf{E}} M$ there exists a recipe ζ of M such that $fn(\zeta) = \emptyset$.*

Proof. Intuitively, the first point is due to the fact that we extend ϕ with some names which are deducible from ϕ. Hence, in term of deducible power ϕ and $\overline{\phi}^{\mathcal{B}}$ are equivalent. More formally, if $\phi \vdash_{\mathsf{E}} M$, we can assume that there exists ζ such that $fn(\zeta) \subseteq \mathcal{B} \setminus \tilde{n}$ and $fv(\zeta) \subseteq dom(\phi)$. From such a ζ it is easy to compute ζ' by replacing any occurrence of a name in $\mathcal{B} \setminus \tilde{n}$ by the corresponding variable in $dom(\overline{\phi}^{\mathcal{B}})$ which refers to this name. Since we can always assume that $fn(\zeta) \subseteq \mathcal{B} \setminus \tilde{n}$, we have that $fn(\zeta') = \emptyset$. The reverse transformation, *i.e.* the replacement of variables in $dom(\overline{\phi}^{\mathcal{B}}) \setminus dom(\phi)$ by names refered by these variables in $\overline{\phi}^{\mathcal{B}}$, allows us to conclude for the converse. □

Reduction. Let $\phi = \nu\tilde{n}.\sigma$ be a frame and M be a ground term. Let $\mathcal{B}$ be a base of names in which ϕ and M are decomposable. We will also assume w.l.o.g. that ϕ is saturated w.r.t. $\mathcal{B}$. Let $A = \psi_{\mathcal{B}}(\phi)$ be matrix of size $\ell \times m$ over $\mathcal{S}_{\mathsf{E}}$, and $b = \psi_{\mathcal{B}}(M)$ be a vector of size m over $\mathcal{S}_{\mathsf{E}}$.

Proof. (of Theorem 53) The construction described above is such that $X \cdot A = b$ has a solution over $\mathcal{S}_{\mathsf{E}}$ if and only if $\phi \vdash_{\mathsf{E}} M$.
($\Rightarrow$) We know that there exists $X \in \mathcal{S}_{\mathsf{E}}^{\ell}$ such that $X \cdot A = b$. Consider the recipe $\zeta = \psi^{-1}_{dom(\phi)}(X)$. By construction, we have that $fn(\zeta) \cap \tilde{n} = \emptyset$. It remains to show that $\zeta\sigma =_{\mathsf{E}} M$. For this, we establish that $\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{\mathcal{B}}(M)$. Thanks to Lemma 50, we have that $\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{dom(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi)$. Hence we deduce that $\psi_{\mathcal{B}}(\zeta\sigma) = X \cdot A = b = \psi_{\mathcal{B}}(M)$. Hence the result.
($\Leftarrow$) Assume that $\phi \vdash_{\mathsf{E}} M$. Thanks to Lemma 54 and by the fact that ϕ is saturated w.r.t. $\mathcal{B}$, we know that there exists $\zeta \in \mathcal{T}(\Sigma, dom(\phi))$ such that $\zeta\sigma =_{\mathsf{E}} M$. Let $Y = \psi_{dom(\phi)}(\zeta)$. It remains to establish that $Y \cdot A = b$. Since $\zeta\sigma =_{\mathsf{E}} M$, we have $\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{\mathcal{B}}(M)$. By Lemma 50, we have $\psi_{dom(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi) = \psi_{\mathcal{B}}(M)$, *i.e.* $Y \cdot A = b$ witnessing the fact that $X \cdot A = b$ has a solution over $\mathcal{S}_{\mathsf{E}}$. □

Example 55. *Consider the theory* ACUNh *and the term* $M = n_1 + \mathsf{h}(\mathsf{h}(n_1))$. *Let* $\phi = \nu n_1, n_2.\{^{n_1+\mathsf{h}(n_1)+\mathsf{h}(\mathsf{h}(n_1))}/_{x_1}, ^{n_2+\mathsf{h}(\mathsf{h}(n_1))}/_{x_2}, ^{\mathsf{h}(n_2)+\mathsf{h}(\mathsf{h}(n_1))}/_{x_3}\}$. *We have:*

$$A = \begin{pmatrix} 1+\mathsf{h}+\mathsf{h}^2 & \mathsf{h}^2 & \mathsf{h}^2 \\ 0 & 1 & \mathsf{h} \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1+\mathsf{h}^2 \\ 0 \end{pmatrix}$$

The equation $X \cdot A = b$ *has a solution over* $\mathbb{Z}/2\mathbb{Z}[\mathsf{h}]$ *:* $(1+\mathsf{h}, \mathsf{h}, 1)$. *The term* M *is deducible from* ϕ *by using the recipe* $x_1 + \mathsf{h}(x_1) + \mathsf{h}(x_2) + x_3$.

As a consequence, decidability/complexity results for deduction can be deduced from decidability/complexity results for solving linear system of equations over semirings (see Section 9).

8. Static equivalence

We show that deciding whether two frames are equivalent can be reduced to deciding whether two matrices satisfy the same set of equalities.

Theorem 56. *Let* E *be a monoidal theory and* $\mathcal{S}_{\mathsf{E}}$ *be its associated semiring. Static equivalence in* E *is reducible in polynomial time to the following problem:*

Entries*: Two matrices A_1 and A_2 over $\mathcal{S}_{\mathsf{E}}$ of size $\ell \times m$*
Question*: Does the following equality holds?*
$\{(X,Y) \in \mathcal{S}_{\mathsf{E}}^{\ell} \times \mathcal{S}_{\mathsf{E}}^{\ell} \mid X \cdot A_1 = Y \cdot A_1\} = \{(X,Y) \in \mathcal{S}_{\mathsf{E}}^{\ell} \times \mathcal{S}_{\mathsf{E}}^{\ell} \mid X \cdot A_2 = Y \cdot A_2\}$

Similarly to deduction, we first show that we can restrict our attention to saturated frames. Moreover, we show that it is sufficient to consider recipes, *i.e.* tests (M,N), without names.

Lemma 57. *Let $\phi_1 = \nu\tilde{n}.\sigma_1, \phi_2 = \nu\tilde{n}.\sigma_2$. and $\mathcal{B}$ be a base of names in which ϕ_1 and ϕ_2 are decomposable. We have that $\phi_1 \approx_{\mathsf{E}} \phi_2$ if and only if $\overline{\phi_1}^{\mathcal{B}} \approx_{\mathsf{E}} \overline{\phi_2}^{\mathcal{B}}$. Moreover, if $\overline{\phi_1}^{\mathcal{B}} \not\approx_{\mathsf{E}} \overline{\phi_2}^{\mathcal{B}}$ then there exist $M, N \in \mathcal{T}(\Sigma, dom(\overline{\phi_1}^{\mathcal{B}}))$ such that $(M =_{\mathsf{E}} N)\overline{\phi_1}^{\mathcal{B}} \not\Leftrightarrow (M =_{\mathsf{E}} N)\overline{\phi_2}^{\mathcal{B}}$.*

Proof. ($\Rightarrow$) Assume that $\phi_1 \approx_{\mathsf{E}} \phi_2$. We have that $\overline{\phi_1}^{\mathcal{B}} = \nu\tilde{n}.(\sigma_1 \cup \sigma_1^0)$ and $\overline{\phi_2}^{\mathcal{B}} = \nu\tilde{n}.(\sigma_2 \cup \sigma_2^0)$ for some substitutions σ_1^0 and σ_2^0 such that $\sigma_1^0 = \sigma_2^0$. Indeed, otherwise, we will obtain a test of the form $x = n_i$ with $x \in dom(\phi_1)$ and $n_i \in \mathcal{B} \setminus \tilde{n}$ such that $(x =_{\mathsf{E}} n_i)\phi_1 \not\Leftrightarrow (x =_{\mathsf{E}} n_i)\phi_2$. Hence, we have that $dom(\overline{\phi_1}^{\mathcal{B}}) = dom(\overline{\phi_2}^{\mathcal{B}})$. Now, assume that $\overline{\phi_1}^{\mathcal{B}} \not\approx_{\mathsf{E}} \overline{\phi_2}^{\mathcal{B}}$, then there exists a test (M,N) such that $(M =_{\mathsf{E}} N)\overline{\phi_1}^{\mathcal{B}}$ whereas $(M \neq_{\mathsf{E}} N)\overline{\phi_2}^{\mathcal{B}}$ (or the converse). Let $M' = M\sigma_1^0$ and $N' = N\sigma_1^0$. We have $(M' =_{\mathsf{E}} N')\phi_1$ whereas $(M' \neq_{\mathsf{E}} N')\phi_2$. Hence contradiction.
($\Leftarrow$) Assume that $\phi_1 \not\approx_{\mathsf{E}} \phi_2$. Let M, N be such that $(M =_{\mathsf{E}} N)\phi_1$ whereas $(M \neq_{\mathsf{E}} N)\phi_2$ (or the converse). It is clear that $\overline{\phi_1}^{\mathcal{B}} \not\approx_{\mathsf{E}} \overline{\phi_2}^{\mathcal{B}}$. Indeed, a witness of this fact is the test (M,N).

Lastly, if we have that $\phi_1 \not\approx_{\mathsf{E}} \phi_2$, then there exists a witness (M,N) such that $fn(M) \cup fn(N) \subseteq \mathcal{B} \setminus \tilde{n}$. Hence, if we consider M' and N' the terms obtained from M and N by replacing any occurrence of a name in $\mathcal{B} \setminus \tilde{n}$ by the corresponding variables in $dom(\overline{\phi_1}^{\mathcal{B}})$ which refers to this name. This allows us to easily conclude. □

Reduction. Let $\phi_1 = \nu\tilde{n}.\sigma_1$ and $\phi_2 = \nu\tilde{n}.\sigma_2$ be two frames having the same domain. Let $\mathcal{B}$ be a base of names in which the two frames are decomposable. We assume w.l.o.g. that ϕ_1 and ϕ_2 are saturated w.r.t. $\mathcal{B}$. Let $m = |\mathcal{B}|$. Let $A_1 = \psi_{\mathcal{B}}(\phi_1)$ and $A_2 = \psi_{\mathcal{B}}(\phi_2)$, two matrices of size $\ell \times m$, over $\mathcal{S}_{\mathsf{E}}$.

Proof. (of Theorem 56) The construction above is such that $\phi_1 \approx_{\mathsf{E}} \phi_2$ iff
$\{(X,Y) \in \mathcal{S}_{\mathsf{E}}^{\ell} \times \mathcal{S}_{\mathsf{E}}^{\ell} \mid X \cdot A_1 = Y \cdot A_1\} = \{(X,Y) \in \mathcal{S}_{\mathsf{E}}^{\ell} \times \mathcal{S}_{\mathsf{E}}^{\ell} \mid X \cdot A_2 = Y \cdot A_2\}$.

($\Rightarrow$) Assume by contradiction that there exists (X_M, X_N) such that $X_M \cdot A_1 = X_N \cdot A_1$ and $X_M \cdot A_2 \neq X_N \cdot A_2$ (or the converse). Let $M = \psi^{-1}_{dom(\phi_1)}(X_M)$ and $N = \psi^{-1}_{dom(\phi_1)}(X_N)$. We have that

- $(M =_{\mathsf{E}} N)\phi_1$. For this, it is sufficient to show that $\psi_{\mathcal{B}}(M\sigma_1) = \psi_{\mathcal{B}}(N\sigma_1)$, *i.e.* $\psi_{dom(\phi_1)}(M) \cdot \psi_{\mathcal{B}}(\phi_1) = \psi_{dom(\phi_1)}(N) \cdot \psi_{\mathcal{B}}(\phi_1)$ thanks to Lemma 50. Now to conclude, it is sufficient to notice that we have $X_M = \psi_{dom(\phi_1)}(M)$, $X_N = \psi_{dom(\phi_1)}(N)$ and $A_1 = \psi_{\mathcal{B}}(\phi_1)$ and to rely on the hypothesis.
- $(M \neq_{\mathsf{E}} N)\phi_2$ can be shown similarly.

($\Leftarrow$) Assume that $\phi_1 \not\approx_{\mathsf{E}} \phi_2$. We have that there exists a test (M, N) such that $(M =_{\mathsf{E}} N)\phi_1$ and $(M \neq_{\mathsf{E}} N)\phi_2$ (or the converse). Thanks to Lemma 57 and the fact that the frames are saturated, we can assume that $M, N \in \mathcal{T}(\Sigma, dom(\phi_1))$. Let $X_M = \psi_{dom(\phi_1)}(M)$ and $X_N = \psi_{dom(\phi_1)}(N)$. We have

- $X_M \cdot A_1 = X_N \cdot A_1$. We have $M\sigma_1 =_{\mathsf{E}} N\sigma_1$, hence $\psi_B(M\sigma_1) = \psi_{\mathcal{B}}(N\sigma_1)$. By Lemma 50, we have that $\psi_{dom(\phi_1)}(M) \cdot \psi_{\mathcal{B}}(\phi_1) = \psi_{dom(\phi_1)}(M) \cdot \psi_{\mathcal{B}}(\phi_1)$, *i.e.* $X_M \cdot A_1 = X_N \cdot A_1$.
- $X \cdot A_2 \neq Y \cdot A_2$ can be established in a similar way. □

Going further. Thanks to Theorem 56, we give a way to decide static equivalence in monoidal equational theories provided we can decide whether two sets of linear equations over $\mathcal{S}_{\mathsf{E}}$ have the same set of solutions. Actually, when $\mathcal{S}_{\mathsf{E}}$ is a ring or when we can extend the semiring $\mathcal{S}_{\mathsf{E}}$ into a ring $\mathcal{R}_{\mathsf{E}}$, the static equivalence problem is equivalent to the problem of deciding whether the equality

$$\{Z \in \mathcal{R}^{\ell}_{\mathsf{E}} \mid Z \cdot A_1 = 0\} = \{Z \in \mathcal{R}^{\ell}_{\mathsf{E}} \mid Z \cdot A_2 = 0\}$$

holds. When $\mathcal{R}_{\mathsf{E}}$ is commutative, it is equivalent to deciding whether $\mathsf{Ker}(A_1) = \mathsf{Ker}(A_2)$, where $\mathsf{Ker}(M)$ denotes the kernel of the matrices M, *i.e.* the set $\{X \mid M \cdot X = 0\}$.

In particular, when E is a group theory, we can choose $\mathcal{R}_{\mathsf{E}}$ to be $\mathcal{S}_{\mathsf{E}}$ since $\mathcal{S}_{\mathsf{E}}$ is actually a ring [31]. Otherwise, it might be possible to extend the equational theory E with a new unary symbol $-$ and the law $x + -(x) = 0$ in order to obtain a theory E' that is consistent with E, *i.e.* for all $u, v \in \mathcal{S}_{\mathsf{E}}$ such that $u =_{\mathsf{E}'} v$, we have also that $u =_{\mathsf{E}} v$. In such a case, the ring $\mathcal{R}_{\mathsf{E}}$ is the semiring $\mathcal{S}_{\mathsf{E}'}$ associated to E' as explained in Section 6.1.

Example 58. *We have seen that the semiring associated to* AG *is isomorphic to* $\mathbb{Z}$ *which is a commutative ring. Hence, we have that* $\mathcal{R}_{\mathsf{E}}$

is isomorphic to $\mathbb{Z}$*. The associated semiring to the monoidal equational theory* ACU *is isomorphic to* $\mathbb{N}$ *whereas its associated ring is* $\mathbb{Z}$*.*

Note that the transformation described above does not allow us to associate a ring to any semiring. For instance, if we consider the theory ACUI and the theory E' obtained by the transformation described above, we have that $0 =_{\mathsf{E}'} (\mathbf{1} + \mathbf{1}) + -(\mathbf{1}) =_{\mathsf{E}'} \mathbf{1} + (\mathbf{1} + -(\mathbf{1})) =_{\mathsf{E}'} \mathbf{1}$ whereas this equality does not hold in ACUI.

— PART III: Summary of decidability results —

In this part, we give an overview of existing results for deduction and static equivalence for many relevant equational theories. Several of them are obtained thanks to the techniques developed in the two previous parts of this paper. A summary is given in Figure 1.

9. Monoidal theories

In this section, we show that several interesting monoidal equational theories induce a ring or a semiring for which solving linear systems or checking for equalities of sets of solutions of linear systems are decidable.

Theory ACU. This equational theory is the simplest monoidal theory. The semiring corresponding to this theory is $\mathbb{N}$ whereas its associated ring is $\mathbb{Z}$. This equational theory has been particularly studied. Since the problem of solving linear equations over $\mathbb{N}$ is strongly NP-complete, we obtain that deduction is a NP-complete problem. The problem of static equivalence for this theory has been shown decidable in [2]. Actually thanks to the algebraic characterization given in this paper, this problem can be solved in polynomial time [35].

At first sight, it might seem surprising since it has been shown [2] that deduction in a given theory E can be reduced in polynomial time to static equivalence in E. However, this reduction required the presence of a free function symbol and such a function symbol is not available in the theory ACU. Hence, the polynomial reduction provided in [2] does not apply in this setting.

Theories ACUI and ACUN (Exclusive Or). The semirings corresponding to these equational theories are respectively the Boolean semiring $\mathbb{B}$, which is finite, and the finite field $\mathbb{Z}/2\mathbb{Z}$. The theory ACUN has already been studied in terms of deduction [19, 13] and static equivalence [2]. Deduction and static equivalence are both decidable in polynomial time. As far as we know the theory ACUI has only been studied in term of deduction [22]. Actually, since its associated semiring is finite, we easily deduce that deduction and static equivalence are decidable.

Theory AG (Abelian Groups). The semiring associated to this equational theory is in fact a ring, namely the ring $\mathbb{Z}$ of all integers. There exist several algorithms to compute solutions of linear equations

over $\mathbb{Z}$ and to compute a base of the set of solutions (see for instance [35]). Hence, we easily deduce that both problems are decidable in PTIME. Deduction for this theory has already been studied in [19] and [12].

Theories ACUh, ACUNh and AGh. The semiring associated to ACUh is $\mathbb{N}[\mathsf{h}]$, the semiring of polynomials in one indeterminate over $\mathbb{N}$, whereas the ring associated to ACUh is $\mathbb{Z}[\mathsf{h}]$. For the theory ACUNh (resp. AGh) the associated semiring is $\mathbb{Z}/2\mathbb{Z}[\mathsf{h}]$ (resp. $\mathsf{Z}[\mathsf{h}]$). Deduction for these three equational theories has already been studied in [25, 21]. However, results obtained on static equivalence are new.

1. ACUh and AGh: Deciding static equivalence for both these theories is reducible to the problem of deciding whether $\mathsf{Ker}(A) = \mathsf{Ker}(B)$ where A and B are matrices built over $\mathsf{N}[\mathsf{h}]$ in the case of ACUh and $\mathsf{Z}[\mathsf{h}]$ in the case of AGh. This problem has been solved by F. Baader to obtain a unification algorithm for the theory AGh (see [5]). This is done by the help of Gröbner Base methods in a more general settings. Actually, he provides an algorithm even in the case of several commuting homomorphisms.

2. ACUNh: Deciding static equivalence in ACUNh is reducible to the problem of deciding whether $\mathsf{Ker}(A) = \mathsf{Ker}(B)$ where A and B are matrices built over $\mathsf{Z}/2\mathsf{Z}[\mathsf{h}]$. This is achieved in [26] by using an automata-theoretic approach.

Theory ACUIh. The semiring associated to ACUIh is $\mathbb{B}[\mathsf{h}]$. Deduction for this theory has never been studied but is clearly decidable. Indeed, to find a solution to $A \cdot X = b$, it is easy to see that each component of a solution to $A \cdot X = b$ has a degree smaller than the degree of b. Hence, the question of deciding whether there exists X such that $A \cdot X = b$ can be reduced to solving a system of linear equations over $\mathbb{B}$. Theorem 56 does not help us to provide an algorithm to solve static equivalence. Note also that we cannot reduce the problem to the problem of deciding whether $\mathsf{Ker}(A) = \mathsf{Ker}(B)$ since, as for ACUI, we are not able to associate a ring to this theory.

Adding more equations. A monoidal theory on a signature Σ may contain arbitrary additional equalities over Σ. The only requirement is, that at least the laws given in Definition 43 hold. Hence, the techniques developed in Section 7 and 8 can be applied to many different theories. We illustrate this by providing some examples.

Example 59. *Consider the theory* E_1 *over* $\Sigma_1 = \{+, 0, -, \mathsf{h}\}$ *which consists of the equalities of* AGh *and the additional equality* $\mathsf{h}(\mathsf{h}(x)) = x$ *which states that* h *is an involution. The theory* E_1 *is a monoidal theory and its associated semiring* $\mathcal{S}_{\mathsf{E}_1}$ *that is actually a ring is isomorphic to* $\mathbb{Z}[\mathsf{h}]/_{(\mathsf{h}^2-1)}$, i.e. *the ring* $\mathbb{Z}[\mathsf{h}]$ *quotiented by the ideal generated by the polynomial* $\mathsf{h}^2 - 1$.

We can also consider more complex equational theories by simply associating each equation to a polynomial. This is illustrated in the next example.

Example 60. *Consider the signature* $\Sigma_2 = \{+, 0, -, \mathsf{h}_1, \mathsf{h}_2\}$ *and the theory* E_2 *made up of the axioms of* AG *extending by* $\mathsf{h}_1(\mathsf{h}_2(x)) = \mathsf{h}_2(\mathsf{h}_1(x))$, *the following homomorphism laws*

$$\begin{array}{rclcrcl} \mathsf{h}_1(x+y) & = & \mathsf{h}_1(x) + \mathsf{h}_1(y) & \qquad & \mathsf{h}_1(0) & = & 0 \\ \mathsf{h}_2(x+y) & = & \mathsf{h}_2(x) + \mathsf{h}_2(y) & & \mathsf{h}_2(0) & = & 0 \end{array}$$

and the following axioms

$$\begin{array}{rcl} \mathsf{h}_1(\mathsf{h}_1(\mathsf{h}_2(x))) + \mathsf{h}_2(\mathsf{h}_2(x)) & = & 0 \\ \mathsf{h}_1(x) + \mathsf{h}_1(\mathsf{h}_2(\mathsf{h}_2(x))) & = & 0 \end{array}$$

The theory E_2 *is a monoidal theory and it is easy to see that its associated semiring* $\mathcal{S}_{\mathsf{E}_2}$ *is isomorphic to* $\mathbb{Z}[\mathsf{h}_1, \mathsf{h}_2]/_{(\mathsf{h}_1^2\mathsf{h}_2+\mathsf{h}_2^2, \mathsf{h}_1+\mathsf{h}_1\mathsf{h}_2^2)}$, i.e. *the ring* $\mathbb{Z}[\mathsf{h}]$ *quotiented by the ideal generated by the polynomials* $\mathsf{h}_1^2\mathsf{h}_2 + \mathsf{h}_2^2$ *and* $\mathsf{h}_1 + \mathsf{h}_1\mathsf{h}_2^2$.

Thus decidability of deduction and static equivalence can be reduced to solving linear equations in the corresponding semiring and deciding the equalities of kernels of matrices in the corresponding ring. Hence, we can reduce our problems to rather classical problems of Algebra, which can often be solved using Gröbner basis for example. Moreover, existing tools for solving algebraic problems can also be used to implement our algorithms.

10. Combination of disjoint equational theories

Our combination results stated in the first part of this paper allows us to combine any existing decidability results for deduction and static equivalence provided the signatures of the equational theories are disjoint. Those combination algorithms can be applied for instance to combine a monoidal equational theory with any other equational theory for which deduction and static equivalence are known to be decidable. In order to give a complete picture of existing results in this area, we sum up some of the results obtained by others.

Subterm convergent equational theories. Deduction and static equivalence are decidable in polynomial time (in the DAG-size of the inputs) for any subterm convergent theory [2]. A subterm convergent theory is an equational theory induced by a finite set of equations of the form $u = v$ where v is either a subterm of u or a constant, and such that the associated rewriting system is convergent. For instance, $\mathsf{E}_{\mathsf{enc}}$ (see Example 2) is a subterm convergent theory.

Since we also know that deduction and static equivalence are decidable in polynomial time for the equational theory ACUN of the exclusive or and also for the theory AG of Abelian group. Applying Theorems 26 and 32, we get for instance the following new decidability result.

Proposition 61. *Let* E *be a subterm convergent theory. Deduction and static equivalence are decidable in polynomial time for* $\mathsf{E} \cup \mathsf{ACUN}$ *and* $\mathsf{E} \cup \mathsf{AG}$.

Blind signature. In [2], it has been shown that deduction and static equivalence are also decidable for the theory of blind signature described below.

$$\mathsf{open}(\mathsf{commit}(x,y),y) = x \qquad \mathsf{chksign}(\mathsf{sgn}(x,y),\mathsf{pk}(y)) = x$$
$$\mathsf{getpk}(\mathsf{host}(x)) = x \qquad \mathsf{unblind}(\mathsf{blind}(x,y),y) = x$$
$$\mathsf{unblind}(\mathsf{sgn}(\mathsf{blind}(x,y),z),y) = \mathsf{sign}(x,z)$$

This theory has been introduced by S. Kremer and M. Ryan in order to model blind signatures and related constructs in their analysis of an electronic voting protocols [24].

Addition. This simple theory for addition is studied in [2]. They show that deduction and static equivalence are decidable.

$$\mathsf{plus}(x,\mathsf{s}(y)) = \mathsf{plus}(\mathsf{s}(x),y) \qquad \mathsf{plus}(x,0) = x \qquad \mathsf{pred}(\mathsf{s}(x)) = x$$

Homomorphism encryption. In [2], they also consider the following equational theory and show that deduction and static equivalence are decidable.

$$\mathsf{enc}(\langle x,y\rangle,z) = \langle \mathsf{enc}(x,z),\mathsf{enc}(y,z)\rangle \qquad \mathsf{proj}_1(\langle x,y\rangle) = x$$
$$\mathsf{dec}(\langle x,y\rangle,z) = \langle \mathsf{dec}(x,z),\mathsf{dec}(y,z)\rangle \qquad \mathsf{proj}_2(\langle x,y\rangle) = y$$
$$\mathsf{dec}(\mathsf{enc}(x,y),y) = x$$

This theory represents an encryption scheme with a homomorphism property. Several results have been obtained for similar theories from the point of view of deduction. For instance, H. Comon-Lundh and R. Treinen have investigated a very similar equational theory [20]. They have shown that deduction is decidable in PTIME. There also exist some results due to P. Lafourcade *et al.* (*e.g.* [27]) for deduction under certain AC-like theories with distributive encryption.

Theory E	Deduction	Static Equivalence
subterm convergent	PTIME [2]	
blind sign., addition, homo. encryption	decidable [2]	
ACU	NP-complete	decidable [2] PTIME (*new*)
ACUI	decidable [22]	decidable (*new*)
ACUN	PTIME [13]	decidable [2] PTIME (*new*)
AG	PTIME [12]	PTIME (*new*)
ACUh	NP-complete [25]	decidable (*new*)
ACUIh	decidable (*new*)	?
ACUNh	PTIME [21]	decidable (*new*)
AGh	PTIME [21]	decidable (*new*)
$\mathsf{AGh}_1 \ldots \mathsf{h}_n$	decidable (*new*)	decidable (*new*)
sub. conv. $\uplus$ ACUN	PTIME (*new*)	
sub. conv. $\uplus$ AG	PTIME (*new*)	

Thanks to Theorem 32, deduction and static equivalence are also decidable for the union of any disjoint theories of this tabular.

Figure 1. Decidability results for deduction and static equivalence.

11. Conclusion

This paper provides many decidability and complexity results for deduction and static equivalence, two formal representations for knowledge in the analysis of security protocols. We propose a general setting for an important class of equational theories with associative and commutative properties and we show that existing decidability results can be combined for any disjoint equational theories.

The performance of the corresponding decision procedures obviously depend on the choice of equational theory. However, our algorithms for combining theories are polynomial (in the DAG-size of the inputs) and efficient existing tools for solving algebraic problems can be used to implement the algorithms for monoidal theories. Hence, as future work, we consider implementing the procedures described in this paper.

As further work, we also consider extending our combination result for non disjoint theories. This would allow us to consider some fragments of the modular exponentiation theory such as the Diffie-Hellman one, *i.e.* the axioms $\mathsf{exp}(x, 1) = x$ and $\mathsf{exp}(\mathsf{exp}(x, y), z) = \mathsf{exp}(x, y \times z)$ where $\times$ is an Abelian group operator; or to take into account the equation $\mathsf{exp}(x, y) \cdot \mathsf{exp}(x, z) = \mathsf{exp}(x, y + z)$. We might use for example a notion of hierarchy between theories like in [16].

Lastly, as indicated in the introduction, deduction and static equivalence are static notions. However, they play an important role in analysis with respect to active attacks, and it is challenging to obtain results in this case. For deduction, combination algorithms are given in [14, 16] and algorithms for deciding deduction in monoidal theories are provided in [22] (those works are described in the introduction). However, these two problems are not yet solved for observational equivalence. M. Baudet has proved that a notion of equivalence is decidable under convergent subterm theories [10] in presence of active attackers. It will be interesting to complete the picture of the active case and to provide a combination algorithm and procedures for monoidal theories in case of observational equivalence. This will allow us to decide the existence of guessing attacks for a large class of equational theories.

Acknowledgment: We wish to thank Jean-Charles Faugère, Daniel Lazard and Paul Zimmermann for fruitful discussions. We also would like to thank the anonymous referees who gave relevant comments which helped in improving the paper.

References

1. Abadi, M., M. Baudet, and B. Warinschi: 2006, '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)*. Vienna, Austria, pp. 398–412.
2. Abadi, M. and V. Cortier: 2006, 'Deciding knowledge in security protocols under equational theories'. *Theoretical Computer Science* **387**(1-2), 2–32.
3. Abadi, M. and C. Fournet: 2001, 'Mobile Values, New Names, and Secure Communication'. In: *Proceedings of the 28th ACM Symposium on Principles of Programming Languages (POPL'01)*. London (UK), pp. 104–115.
4. Baader, F.: 1989, 'Unification in Commutative Theories'. *Journal of Symbolic Computation* **8**(5), 479–497.
5. Baader, F.: 1993, 'Unification in Commutative Theories, Hilbert's Basis Theorem, and Gröbner Bases.'. *Journal of the ACM* **40**(3), 477–503.
6. Baader, F. and W. Nutt: 1996, 'Combination Problems for Commutative/ Monoidal Theories or How Algebra Can Help in Equational Unification.'. *Applicable Algebra Engineering Communication and Computing* **7**(4), 309–337.

7. Baader, F. and K. U. Schulz: 1996, 'Unification in the Union of Disjoint Equational Theories: Combining Decision Procedures.'. *Journal of Symbolic Computation* **21**(2), 211–243.
8. Baader, F. and K. U. Schulz: 1998, 'Combination of Constraint Solvers for Free and Quasi-Free Structures'. *Theoretical Computer Science* **192**(1), 107–161.
9. Baader, F. and C. Tinelli: 2002, 'Deciding the Word Problem in the Union of Equational Theories'. *Information and Computation* **178**(2), 346–390.
10. Baudet, M.: 2005, 'Deciding Security of Protocols against Off-line Guessing Attacks'. In: *Proc. 12th ACM Conference on Computer and Communications Security (CCS'05)*. Alexandria (Virginia, USA), pp. 16–25.
11. Baudet, M., V. Cortier, and S. Kremer: 2005, 'Computationally Sound Implementations of Equational Theories against Passive Adversaries'. In: *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, Vol. 3580 of *LNCS*. Lisboa (Portugal), pp. 652–663.
12. Chevalier, Y., R. Küsters, M. Rusinowitch, and M. Turuani: 2003a, 'Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Product in Exponents'. In: *Proceedings of the 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS'03)*, Vol. 2914 of *LNCS*. Mumbai (India), pp. 124–135.
13. Chevalier, Y., R. Küsters, M. Rusinowitch, and M. Turuani: 2003b, '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).
14. Chevalier, Y. and M. Rusinowitch: 2005a, 'Combining Intruder Theories'. In: *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, Vol. 3580 of *LNCS*. Lisboa (Portugal), pp. 639–651.
15. Chevalier, Y. and M. Rusinowitch: 2005b, 'Combining Intruder Theories'. Technical Report 5495, INRIA. http://www.inria.fr/rrrt/rr-5495.html.
16. Chevalier, Y. and M. Rusinowitch: 2006, 'Hierarchical Combination of Intruder Theories'. In: *Proceedings of the 17th International Conference on Rewriting Techniques and Applications, (RTA'06)*, Vol. 4098 of *LNCS*. Seattle (WA), pp. 108–122.
17. Chevalier, Y. and M. Rusinowitch: 2008, 'Hierarchical combination of intruder theories'. *Information and Computation* **206**(2-4), 352–377.
18. Collins, D. J.: 1986, 'A simple presentation of a group with unsolvable word problem'. *Illinois Journal of Mathematics* **30**(2), 230–234.
19. Comon-Lundh, H. and V. Shmatikov: 2003, '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).
20. Comon-Lundh, H. and R. Treinen: 2003, 'Easy Intruder Deductions'. In: *Verification: Theory & Practice, Essays Dedicated to Zohar Manna on the Occasion of His 64th Birthday*, Vol. 2772 of *LNCS*. pp. 225–242.
21. Delaune, S.: 2006, 'Easy Intruder Deduction Problems with Homomorphisms'. *Information Processing Letters* **97**(6), 213–218.
22. Delaune, S., P. Lafourcade, D. Lugiez, and R. Treinen: 2008, 'Symbolic Protocol Analysis for Monoidal Equational Theories'. *Information and Computation* **206**(2-4), 312–351.
23. Dershowitz, N. and J.-P. Jouannaud: 1990, 'Rewrite Systems'. In: *Handbook of Theoretical Computer Science*, Vol. B. Elsevier, Chapt. 6.

24. Kremer, S. and M. D. Ryan: 2005, 'Analysis of an Electronic Voting Protocol in the Applied Pi-Calculus'. In: *Proceedings of the 14th European Symposium on Programming (ESOP'05)*, Vol. 3444 of *LNCS*. Edinburgh (UK), pp. 186–200.
25. Lafourcade, P., D. Lugiez, and R. Treinen: 2005, 'Intruder Deduction for AC-like Equational Theories with Homomorphisms'. In: *Proceedings 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, Vol. 3467 of *LNCS*. Nara (Japan), pp. 308–322.
26. Lafourcade, P., D. Lugiez, and R. Treinen: 2006, 'ACUNh: Unification and Disunification Using Automata Theory'. In: *Proc. 20th Int. Workshop on Unification (UNIF'06)*. Seattle (Washington, USA), pp. 6–20.
27. Lafourcade, P., D. Lugiez, and R. Treinen: 2007, 'Intruder Deduction for the Equational Theory of Abelian Groups with Distributive Encryption'. *Information and Computation* **205**(4), 581–623.
28. Lakhnech, Y., L. Mazaré, and B. Warinschi: 2006, 'Soundness of Symbolic Equivalence for Modular Exponentiation'. In: *Proceedings of the 2nd Workshop on Formal and Computational Cryptography (FCC'06)*. Venice (Italy), pp. 19–23.
29. Lowe, G.: 1996, '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)*, Vol. 1055 of *LNCS*. Berlin (Germany), pp. 147–166.
30. Millen, J. and V. Shmatikov: 2001, 'Constraint Solving for Bounded-Process Cryptographic Protocol Analysis'. In: *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS'01)*.
31. Nutt, W.: 1990, 'Unification in Monoidal Theories.'. In: *Proc. 10th Int. Conference on Automated Deduction, (CADE'90)*, Vol. 449 of *LNCS*. Kaiserslautern (Germany), pp. 618–632.
32. Paulson, L. C.: 1998, 'The Inductive Approach to Verifying Cryptographic Protocols.'. *Journal of Computer Security* **6**(1-2), 85–128.
33. Rusinowitch, M. and M. Turuani: 2003, 'Protocol insecurity with a finite number of sessions, composed keys is NP-complete'. *Theoretical Computer Science* **1-3**(299), 451–475.
34. Schmidt-Schauß, M.: 1989, 'Unification in a Combination of Arbitrary Disjoint Equational Theories.'. *Journal of Symbolic Computation* **8**(1/2), 51–99.
35. Schrijver, A.: 1986, *Theory of Linear and Integer Programming*. Wiley.

Appendix

A. Decidablity of the word problem *vs* the deduction problem

While apparently simpler, the decidability of the word problem modulo E is not a consequence of the decidability of the deduction problem modulo E. We provide below an example of a theory for which the deduction problem is decidable while the word problem is not. This example is based on the fact that the word problem might be undecidable but each function symbol could be invertible, in which case any name of a term would be accessible and thus any term could be deducible from any set of terms.

More formally, consider the finitely presented group G introduced by Collins [18]. This group is formed by the set of words on the alphabet

$$A = \{a, b, c, d, e, p, q, r, t, k, a^{-1}, b^{-1}, c^{-1}, d^{-1}, e^{-1}, p^{-1}, q^{-1}, r^{-1}, t^{-1}, k^{-1}\}$$

quotiented by the relations

$$\begin{array}{rclrclrcl}
p^{10}a & = & ap, & pacqr & = & rpcaq, & ra & = & ar \\
p^{10}b & = & bp, & p^2adq^2r & = & rp^2daq^2, & rb & = & br \\
p^{10}c & = & cp, & p^3bcq^3r & = & rp^3cbq^3, & rc & = & cr \\
p^{10}d & = & dp, & p^4bdq^4r & = & rp^4dbq^4, & rd & = & dr \\
p^{10}e & = & ep, & p^5ceq^5r & = & rp^5ecaq^5, & re & = & er \\
aq^{10} & = & qa, & p^6deq^6r & = & rp^6edbq^6, & pt & = & tp \\
bq^{10} & = & qb, & p^7cdcq^7r & = & rp^7cdceq^7, & qt & = & tq \\
cq^{10} & = & qc, & p^8ca^3q^8r & = & rp^8a^3q^8, & & & \\
dq^{10} & = & qd, & p^9da^3q^9r & = & rp^9a^3q^9, & & & \\
eq^{10} & = & qe, & a^{-3}ta^3k & = & ka^{-3}ta^3, & & &
\end{array}$$

where the straightforward equation $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$ (the empty word) is implicitly assumed for any $\alpha \in A$. Let

$$\Sigma = \{a, b, c, d, e, p, q, r, t, k, a^{-1}, b^{-1}, c^{-1}, d^{-1}, e^{-1}, p^{-1}, q^{-1}, r^{-1}, t^{-1}, k^{-1}\}$$

be a set of unary symbols. To simplify the notations, we are using the same symbols for letters and corresponding unary symbols. For each relation above, of the form $a_{i_1} \cdots a_{i_k} = b_{j_1} \cdots b_{j_l}$, we consider the corresponding equation $a_{i_1}(\cdots(a_{i_k}(x))) = b_{j_1}(\cdots(b_{j_l}(x)))$ in addition to the equations $\alpha(\alpha^{-1}(x)) = \alpha^{-1}(\alpha(x)) = x$ for any $\alpha \in \{a, b, c, d, e, p, q, r, t, k\}$. We denote by E_G the corresponding equational theory. The undecidability of the word problem in E_G is an immediate consequence of the undecidability of the word problem in G [18]. Conversely, since any symbol of Σ is invertible (due to the equations $\alpha(\alpha^{-1}(x)) = \alpha^{-1}(\alpha(x)) = x$), an attacker can access any private name $n \in \tilde{n}$ of a frame $\phi = \nu\tilde{n}.\sigma$ as

soon as n occurs in σ. Hence, a term M is deducible from ϕ if, and only if, $fn(M) \cap \tilde{n} \subseteq fn(M_1) \cup \ldots fn(M_\ell)$ where $\phi = \nu\tilde{n}.\{^{M_1}/_{x_1}, \ldots, ^{M_\ell}/_{x_\ell}\}$. Therefore, the deduction problem modulo E_G is decidable.

B. Proofs of Section 3

The proofs given in this appendix are similar to those provided in [15]. However, since we use a notion of factor that is slightly different from the one introduced in [15], we have to adapt them.

Remark: Let E be a consistent equational theory and n be a name. We necessarily have that $n = n{\downarrow}$. Indeed, assume that $n \neq n{\downarrow}$ and let $t = n{\downarrow}$. We distinguish two cases:

- either $n \notin fn(t)$ and we easily deduce that E is inconsistent.
- or $n \in fn(t)$ and by definition of $\prec$, we have that $n \prec t$. Hence t can not be the normal form of n.

In both case, we obtain a contradiction. Hence, we have that $n = n{\downarrow}$.

Lemma 62. *If E is a consistent equational theory then for any equation such that $l =_\mathsf{E} r$ with $l \neq r$, if there exists a substitution τ such that $r\tau \prec l\tau$ then l is not a variable.*

Proof. By contradiction, assume that l is a variable and there exists a substitution τ such that $r\tau \prec l\tau$. By monotonicity of $\prec$, we have that $l \notin fv(r)$. Let n_1, n_2 be two different names. We can built two substitutions τ_1 and τ_2 such that $dom(\tau_1) = dom(\tau_2) = fv(r) \cup \{l\}$, $l\tau_1 = n_1$, $l\tau_2 = n_2$ and $x\tau_i = x\tau$ for any $x \in fv(r)$ $(i = 1, 2)$. The equation $l = r$ implies that $n_1 =_\mathsf{E} r\tau =_\mathsf{E} n_2$. By transitivity of the equality, we obtain that $n_1 =_\mathsf{E} n_2$ which contradicts the fact that E is consistent. □

Lemma 63. *Let M be a ground term such that $\mathsf{sign}(M) = \Sigma_1$ (resp. Σ_2) with all its factors in normal form. If M' is minimal for $\prec$ in the set $\{N \mid M \to_\mathcal{O} N\}$ then*

- *either $\mathsf{sign}(M) = \mathsf{sign}(M')$ and $Fct(M') \subseteq Fct(M) \cup \{n_{min}\}$,*
- *or $\mathsf{sign}(M) \neq \mathsf{sign}(M')$ and $M' \in Fct(M) \cup \{n_{min}\}$.*

Moreover, we have that the equation $l = r \in \mathcal{O}$ involved in the step $M \to_\mathcal{O} M'$ is such that $l = r \in \mathcal{O}_1$ (resp. $l = r \in \mathcal{O}_2$).

Proof. Let M be a ground term with all its factors in normal form and assume w.l.o.g. that $\mathsf{sign}(M) = \Sigma_1$. Let M' be the minimal term for $\prec$ among the terms N such that $M \to_{\mathcal{O}} N$. Let $l = r \in \mathcal{O}$ be the rule applied on M at position p with substitution σ in order to obtain M'.

By minimality of the term M' and monotonicity of $\prec$, we have that $fv(r)\sigma \subseteq fv(l)\sigma \cup \{n_{min}\}$. Indeed, if there exists $x \in fv(r) \setminus fv(l)$, then $x\sigma = n_{min}$ by minimality of M'. Moreover, by construction of $\mathcal{O}$, we have that l, r are terms (without names) both in $\mathcal{T}(\Sigma_1, \mathcal{X})$ or both in $\mathcal{T}(\Sigma_2, \mathcal{X})$. Thanks to Lemma 62, we know that l is not a variable. Since $\mathsf{sign}(M) = \Sigma_1$, we deduce that l, r are terms (without names) both in $\mathcal{T}(\Sigma_1, \mathcal{X})$. Hence, we deduce that:

- Either $\mathsf{sign}(l\sigma) \neq \mathsf{sign}(r\sigma)$. In such a case r is a variable and we have that $r\sigma \in Fct(l\sigma) \cup \{n_{min}\}$;
- Or $\mathsf{sign}(l\sigma) = \mathsf{sign}(r\sigma)$. In such a case $Fct(r\sigma) \subseteq Fct(l\sigma) \cup \{n_{min}\}$. Note that r can be a variable or not.

We distinguish two cases:

First case: $p = \epsilon$ and $\mathsf{sign}(l\sigma) \neq \mathsf{sign}(r\sigma)$. In such a case, we have that $M = l\sigma$ and $M' = r\sigma$. Thus $\mathsf{sign}(M) \neq \mathsf{sign}(M')$. We have shown that $r\sigma \in Fct(l\sigma) \cup \{n_{min}\}$, i.e. $M' \in Fct(M) \cup \{n_{min}\}$. This allows us to conclude for this case.

Second case: $p \neq \epsilon$ or $\mathsf{sign}(l\sigma) = \mathsf{sign}(r\sigma)$. If $p \neq \epsilon$, we have that $\mathsf{sign}(M) = \mathsf{sign}(M')$. Otherwise, we have that $\mathsf{sign}(l\sigma) = \mathsf{sign}(r\sigma)$ and thus we have also that $\mathsf{sign}(M) = \mathsf{sign}(M')$. Hence, in both cases, we have that $\mathsf{sign}(M) = \mathsf{sign}(M')$. To conclude, it remains to show that $Fct(M') \subseteq Fct(M) \cup \{n_{min}\}$.

Since the factors of M are in normal form, the position p is above or incomparable with any position corresponding to a factor of M. Thus all positions p' above p (including p) are labelled with $f \in \Sigma_1$.

Let q be a position of a factor F of M'. Either q is incomparable with p, and thus F is also a factor of M at position q; or there exists a variable x at a position $p' \in r$ such that $p.p' \leq q$. In such a case we have that:

- Either $\mathsf{sign}(l\sigma) \neq \mathsf{sign}(r\sigma)$. In such a case r has to be a variable and $F = r\sigma$;
- Or $\mathsf{sign}(l\sigma) = \mathsf{sign}(r\sigma)$. In such a case, we have that $F \in Fct(r\sigma)$.

We distinguish three cases:

1. Case $p = \epsilon$ and $\mathsf{sign}(l\sigma) = \mathsf{sign}(r\sigma)$. We have that $M = l\sigma$ and $M' = r\sigma$. We have that:

$$Fct(M') = Fct(r\sigma) \subseteq Fct(l\sigma) \cup \{n_{min}\} = Fct(M) \cup \{n_{min}\}.$$

2. Case $p \neq \epsilon$ and $\mathsf{sign}(l\sigma) \neq \mathsf{sign}(r\sigma)$. We have that $Fct(M') \subseteq Fct(M) \cup \{r\sigma\}$. We have shown that $r\sigma \in Fct(l\sigma) \cup \{n_{min}\}$. Moreover, we have that $Fct(l\sigma) \subseteq Fct(M)$. Thus we conclude that $Fct(M') \subseteq Fct(M) \cup \{n_{min}\}$.

3. Case $p \neq \epsilon$ and $\mathsf{sign}(l\sigma) = \mathsf{sign}(r\sigma)$. We have that $Fct(M') \subseteq Fct(M) \cup Fct(r\sigma)$. Hence, we have that

$$Fct(M') \subseteq Fct(M) \cup Fct(l\sigma) \cup \{n_{min}\} \subseteq Fct(M) \cup \{n_{min}\}.$$

The last inclusion comes from the fact that $Fct(l\sigma) \subseteq Fct(M)$. □

Lemma 16. *Let M be a ground term such that all its factors are in normal form. Then*

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

Proof. First of all, note that if M is in normal form (this case includes the case where M is a name), the result is straightforward. Otherwise, we assume w.l.o.g. that $\mathsf{sign}(M) = \Sigma_1$ and we consider a derivation normalising M such that at each step a minimal successor (w.r.t. $\prec$) for the relation $\rightarrow_{\mathcal{O}}$ is chosen. We have

$$M = M_1 \rightarrow_{\mathcal{O}} M_2 \rightarrow_{\mathcal{O}} \ldots \rightarrow_{\mathcal{O}} M_{n-1} \rightarrow_{\mathcal{O}} M_n = M{\downarrow}$$

By Lemma 63, we know that at each step, either $\mathsf{sign}(M_i) = \mathsf{sign}(M_{i+1})$ or M_{i+1} is in normal form. Hence we deduce that:

$$\mathsf{sign}(M_1) = \ldots = \mathsf{sign}(M_{n-1}) = \Sigma_1.$$

Thanks to Lemma 63, we easily obtain that $Fct(M_{n-1}) \subseteq Fct(M) \cup \{n_{min}\}$. Now, we distinguish two cases:

- Either $\mathsf{sign}(M_{n-1}) = \mathsf{sign}(M_n)$, and thus $\mathsf{sign}(M) = \mathsf{sign}(M{\downarrow})$. In such a case, by Lemma 63, we deduce that $Fct(M_n) \subseteq Fct(M_{n-1}) \cup \{n_{min}\}$ and thus $Fct(M{\downarrow}) \subseteq Fct(M) \cup \{n_{min}\}$.

- Or $\mathsf{sign}(M_{n-1}) \neq \mathsf{sign}(M_n)$, and thus $\mathsf{sign}(M) \neq \mathsf{sign}(M{\downarrow})$. In such a case, by Lemma 63, we deduce that $M_n \in Fct(M_{n-1}) \cup \{n_{min}\}$ and thus $M{\downarrow} \in Fct(M) \cup \{n_{min}\}$. □

Corollary 17. *Let M be a ground term: $St(M\downarrow) \subseteq St(M)\downarrow \cup \{n_{min}\}$.*

Proof. Let M be a ground term. We show this result by induction on the number n of subterms of M that are different from M itself and not in normal form, i.e.

$$n = \#\{N \in St(M) \mid N \neq M \text{ and } N\downarrow \neq N\}$$

Base case: $n = 0$. In such a case, we have that M is a term such that all its factors are in normal form. Therefore, we can apply Lemma 16. We distinghuish two cases:

- $M\downarrow \in Fct(M) \cup \{n_{min}\}$. In such a case, we have that

$$St(M\downarrow) \subseteq St(Fct(M)) \cup \{n_{min}\} = St(M)\downarrow \cup \{n_{min}\}$$

- $\mathsf{sign}(M) = \mathsf{sign}(M\downarrow)$ and $Fct(M\downarrow) \subseteq Fct(M) \cup \{n_{min}\}$. In such a case, we have that

$$\begin{array}{rcl} St(M\downarrow) & = & \{M\downarrow\} \cup St(Fct(M\downarrow)) \\ & \subseteq & \{M\downarrow, n_{min}\} \cup St(Fct(M)) = St(M)\downarrow \cup \{n_{min}\} \end{array}$$

In both cases, the last equality comes from the fact that terms in $Fct(M)$ are in normal form.

Induction step: $n > 0$. In such a case, there exists a ground term $N \in St(M)$ that is not in normal form and such that all the factors of N are in normal form. Actually, we have that $M = M[N]_p$ with $p \neq \epsilon$. We can apply our induction hypothesis on:

- the term N: we obtain that $St(N\downarrow) \subseteq St(N)\downarrow \cup \{n_{min}\}$.
- the term $M' = M[N\downarrow]_p$: $St(M'\downarrow) \subseteq St(M')\downarrow \cup \{n_{min}\}$.

Altogether, we have that

$$\begin{array}{rcl} St(M\downarrow) = St(M'\downarrow) & \subseteq & St(M')\downarrow \cup \{n_{min}\} \\ & = & St(M[N\downarrow]_p)\downarrow \cup \{n_{min}\} \\ & \subseteq & St(M)\downarrow \cup St(N\downarrow)\downarrow \cup \{n_{min}\} \\ & \subseteq & St(M)\downarrow \cup St(N)\downarrow \cup \{n_{min}\} = St(M)\downarrow \cup \{n_{min}\} \end{array}$$

The last inclusion comes from the fact that $N \in St(M)$. □

Lemma 19. *Let M be a ground term such that $\mathsf{sign}(M) = \Sigma_i$ ($i = \{1, 2\}$) and all its factors are in normal form. Then $M{\downarrow} = M{\downarrow_{\mathsf{E}_i}}$.*

Proof. We consider a derivation normalising M such that at each step a minimal successor (w.r.t. $\prec$) for the relation $\to_{\mathcal{O}}$ is chosen. We also assume that $\mathsf{sign}(M) = \Sigma_1$. We have that

$$M = M_1 \to_{\mathcal{O}} M_2 \to_{\mathcal{O}} \ldots \to_{\mathcal{O}} M_{n-1} \to_{\mathcal{O}} M_n = M{\downarrow}$$

By Lemma 63, we know that at each step, either $\mathsf{sign}(M_i) = \mathsf{sign}(M_{i+1})$ or M_{i+1} is in normal form. Hence we deduce that:

$$\mathsf{sign}(M_1) = \ldots = \mathsf{sign}(M_{n-1}) = \Sigma_1.$$

Thanks to Lemma 63, we know that the equations $l_1 = r_1, \ldots, l_{n-1} = r_{n-1} \in \mathcal{O}$ involved in each step are such that $l_i = r_i \in \mathcal{O}_1$. Hence, we have $M{\downarrow} = M{\downarrow_{\mathsf{E}_1}}$. □

Lemma 20. *Let M be a ground term such that all its factors are in normal form. Let $N \in Fct(M)$ and N' be a term alien to M. We have that*

$$(M\delta_{N,N'}){\downarrow} = ((M{\downarrow})\delta_{N,N'}){\downarrow}.$$

Proof. Let M be a ground term such that all its factors are in normal form. Either M is a name. In such a case, we have that $M{\downarrow} = M$ and we easily conclude. Otherwise, we can assume w.l.o.g. that $\mathsf{sign}(M) = \Sigma_1$. Thanks to Lemma 19, we have that $M{\downarrow} = M{\downarrow_{\mathsf{E}_1}}$. Consider the sequence

$$M = M_1 \to_{\mathcal{O}_1} M_2 \to_{\mathcal{O}_1} \ldots \to_{\mathcal{O}_1} M_{n-1} \to_{\mathcal{O}_1} M_n = M{\downarrow}.$$

The rule $l_i = r_i \in \mathcal{O}_1$ is applied above (and without interfering with) the factors of M_i. On the other hand the replacement is applied below (or at the level of) the factors of M_i. Therefore the sequence $M_1 \to_{\mathcal{O}_1} \ldots \to_{\mathcal{O}_1} M_n$ implies the equalities $M_1\delta_{N,N'} =_{\mathsf{E}_1} \ldots =_{\mathsf{E}_1} M_n\delta_{N,N'}$, thus $M\delta_{N,N'}{\downarrow} = ((M{\downarrow})\delta_{N,N'}){\downarrow}$. □

C. Proofs of Section 5

Lemma 40. *Let $\phi = \nu\tilde{n}.\sigma$ and $\psi = \nu\tilde{n}.\sigma'$ be two frames in normal form such that ϕ contains all its deducible subterms, $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$ and $\psi \models \mathsf{Eq}_{\mathsf{E}_2}(\phi)$. Let $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$ be such that $(fn(M) \cup fn(N)) \cap \tilde{n} = \emptyset$ and assume that for all terms M', N'*

$$(M', N') < (M, N) \quad \textit{implies} \quad (M' =_{\mathsf{E}} N')\phi \Rightarrow (M' =_{\mathsf{E}} N')\psi.$$

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. 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. Indeed, we have nothing to show since $\mathsf{sign}(\zeta\sigma) = \mathsf{sign}(\zeta\sigma{\downarrow})$. Now, we know that that there exists $\zeta^0, \zeta_1, \ldots, \zeta_\ell$ (ℓ might be equal to 0) 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 $M_1' = \zeta^0[\zeta_1, \ldots, x, \ldots, \zeta_\ell]$. We have that $|M_1'| < |M|$, $(M =_{\mathsf{E}} M_1')\phi$ and $(M =_{\mathsf{E}} M_1')\psi$.

Now, the remaining of the proof is devoted to deal with this third case.

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 $\zeta_i\sigma{\downarrow} \notin St(\phi)$ (note

that this case includes the case where $\ell = 0$ and $M = \zeta^0$ is built on Σ_1 only). 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 $\mathsf{sign}(M\sigma) \neq \mathsf{sign}(M\sigma\downarrow)$. (The other cases are take into account by the previous cases).

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 16, we have $M\sigma\downarrow \in St(\phi) \cup \{n_{min}\} \subseteq_{\mathsf{E}} \phi$ since ϕ contains all its deducible subterms. Hence, there exists $x \in dom(\phi)$ such that $(M =_{\mathsf{E}} x)\phi$. Thanks to Lemma 19, we deduce that $(M =_{\mathsf{E}_1} x)\phi$ and hence we have that $(M, x) \in \mathsf{Eq}_{\mathsf{E}_1}(\phi)$. Since $\psi \models \mathsf{Eq}_{\mathsf{E}_1}(\phi)$, we have also $(M =_{\mathsf{E}_1} x)\psi$, thus $(M =_{\mathsf{E}} x)\psi$. Let $M_1 = x$, we easily conclude.

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 names 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 20, we obtain

$$((\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow]\delta_1)\ldots\delta_k)\downarrow = (((M\sigma\downarrow)\delta_1\downarrow)\ldots)\delta_k\downarrow \qquad (8)$$

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

$$((\zeta^0[\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow]\delta_1)\ldots\delta_k) = \zeta^0[\zeta'_1\sigma\downarrow, \ldots, \zeta'_\ell\sigma\downarrow] =_{\mathsf{E}} M'\sigma.$$

Indeed, the replacements δ_j cannot affect $\zeta_j\sigma\downarrow$ when ζ_j is of sign $\perp$. Note that, in that case, ζ_i is a name or a variable and the terms in Δ are not subterm of ϕ.

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 16, we obtain that

$$M\sigma\downarrow \in \{\zeta_1\sigma\downarrow, \ldots, \zeta_\ell\sigma\downarrow, n_{min}\} \subseteq \Delta \cup St(\phi) \cup \{r_1, \ldots, r_\ell\}$$

where $r_1, \ldots, r_\ell$ are the public names of M.
From the equality (8), we can deduce that

- (Case 1) either $M\sigma\downarrow = t_j$ for some t_j $(1 \leq j \leq k)$ and we have $(M' =_{\mathsf{E}} n_j)\phi$,
- (Case 2) or $M\sigma\downarrow = r_j$ for some r_j $(1 \leq j \leq \ell)$ and we have $(M' =_{\mathsf{E}} r_j)\phi$,
- (Case 3) or $M\sigma\downarrow \in St(\phi)$ and in such a case, since ϕ contains all its deducible subterms, we know that there exists $x \in dom(\phi)$ such that $M\sigma\downarrow = x\sigma$. Hence we have that:

$$(((M\sigma\downarrow)\delta_1\downarrow)\ldots)\delta_k\downarrow = ((x\sigma)\delta_1\downarrow)\ldots)\delta_k\downarrow.$$

Since $t_i \notin St(\phi)$ for any $1 \leq i \leq k$, we have that $((x\sigma)\delta_1\downarrow)\ldots)\delta_k\downarrow = x\sigma$. Moreover, we have that

$$(((M\sigma\downarrow)\delta_1\downarrow)\ldots)\delta_k\downarrow = ((\zeta^0[\zeta_1\sigma\downarrow,\ldots,\zeta_\ell\sigma\downarrow]\delta_1)\ldots\delta_k)\downarrow =_{\mathsf{E}} M'\sigma.$$

Hence, we have that $(M' =_{\mathsf{E}} x)\phi$.

In every case, we 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 $(M' =_{\mathsf{E}_1} r_j)\psi$ (Case 2), or $(M' =_{\mathsf{E}_1} x)\psi$ (Case 3). 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 $\zeta^i \in \Delta_i$ by any witness of Δ_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 $(\zeta_i'\sigma'\downarrow)\delta' = (n_p\sigma'\downarrow)\delta' = \zeta^p\sigma'\downarrow = \zeta_i\sigma'\downarrow$. This ends the proof of the claim.

(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 by substitutions of terms for 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 $(M =_{\mathsf{E}} r_j)\phi$. Since $|r_j| < |M|$, it remains to show that $(M =_{\mathsf{E}} r_j)\psi$. We have shown that $(M' =_{\mathsf{E}_1} r_j)\psi$, *i.e.* $\zeta^0[\zeta_1'\sigma'\downarrow,\ldots,\zeta_\ell'\sigma'\downarrow] =_{\mathsf{E}} r_j$. Since E is closed by substitutions of terms for names, we easily deduce that $\zeta^0[(\zeta_1'\sigma'\downarrow)\delta',\ldots,(\zeta_1'\sigma'\downarrow)\delta'] =_{\mathsf{E}} r_j$. By using our claim, we obtain that $\zeta^0[\zeta_1\sigma'\downarrow,\ldots,\zeta_\ell\sigma'\downarrow] =_{\mathsf{E}} r_j$. We deduce that $(M =_{\mathsf{E}} r_j)\psi$.

(Case 3) 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 $(M' =_{\mathsf{E}_1} x)\psi$, *i.e.* $\zeta^0[\zeta_1'\sigma'\downarrow,\ldots,\zeta_\ell'\sigma'\downarrow] =_{\mathsf{E}} x\sigma'$. Since E is closed by substitutions of terms for names, we easily deduce 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 $\zeta^0[\zeta_1\sigma'\downarrow,\ldots,\zeta_\ell\sigma'\downarrow] =_{\mathsf{E}} x\sigma'\downarrow$. We deduce that $(M =_{\mathsf{E}} x)\psi$. □

Proposition 39. *Let ϕ and ψ be two frames in normal form such that ϕ contains all its deducible subterms. 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 19 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 $\phi = \nu\tilde{n}.\sigma$ for some substitution σ and $(\overline{M}, \overline{N}) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$. Let (M, N) obtained from $(\overline{M}, \overline{N})$ by renaming names in $\tilde{n}$ by fresh names (that do not occur in ϕ and ψ). Note that $(M, N) \in \mathsf{Eq}_{\mathsf{E}}(\phi)$. We prove, by induction on the size of (M, N), that $(M =_{\mathsf{E}} N)\psi$. This allows us to conclude that $(\overline{M} = \overline{N})\psi$. Now, 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 there exist $\zeta_M^0, \zeta_M^1, \ldots, \zeta_M^\ell$ 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 $\zeta_N^0, \zeta_N^1, \ldots, \zeta_N^p$ (p might be equal to 0 meaning that ζ_N^0 is reduced to a variable, a name, or N is built on one signature only) 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 $\mathsf{sign}(\zeta_N^0) = \Sigma_1$ or ζ_N^0 is a variable. Otherwise, we would have $\mathsf{sign}(M\sigma) \neq \mathsf{sign}(N\sigma)$ and we conclude thanks to Lemma 40, 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 40 on ζ_M^i and deduce $(M =_{\mathsf{E}} N)\psi$.

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

The remaining of the proof is devoted to this third case. *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 $1 \leq i \leq p$. (Note that this third case includes the cases where $\ell = 0$ and/or $p = 0$ and also the case where ζ_N^0 is a variable.) 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 20, 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 and since we have that $(\zeta_M^i, \zeta_X) < (M, N)$, we deduce that $(\zeta_M^i =_{\mathsf{E}} \zeta_X)\psi$. Hence we have $(\zeta_M'^i\sigma'\downarrow)\delta' = \zeta_X\sigma'\downarrow = \zeta_M^i\sigma'\downarrow$. This ends the proof of the claim.

Below, we assume that N', and thus N, are not reduced to a variable but this case can be done in a similar way.

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 by substitutions of terms for 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 $(M =_{\mathsf{E}} N)\psi$. □

Complexity. 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 $f_i(t_{\mathsf{dag}}(\phi) + t_{\mathsf{dag}}(\psi))$ for $i \in \{1, 2\}$,
- $M =_{\mathsf{E}} N$ can be decided in $f_0(t_{\mathsf{dag}}(M) + t_{\mathsf{dag}}(N))$.

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

Step 1. We first compute $\phi_1' = \overline{\phi_1}^{\Pi}$ and $\phi_2' = \overline{\phi_2}^{\Pi}$ where Π is a set of recipes compatible with ϕ_1 (and ϕ_2) such that:

- $St(\Pi) \subseteq \Pi \cup dom(\phi_i)$;
- $\{M \mid M \in St(\phi_1) \text{ and } \phi_1 \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \{\zeta\sigma \mid \zeta \in \Pi\} \cup \phi_1$;
- $\{M \mid M \in St(\phi_2) \text{ and } \phi_2 \vdash_{\mathsf{E}} M\} \cup \{n_{min}\} \subseteq_{\mathsf{E}} \{\zeta\sigma \mid \zeta \in \Pi\} \cup \phi_2$.

Π can be computed as follows: for each $M \in St(\phi_1)$ (resp. $M \in St(\phi_2)$), we check whether $\phi_1 \vdash_{\mathsf{E}} M$ (resp. $\phi_2 \vdash_{\mathsf{E}} M$) and obtain a corresponding recipe ζ if any. The sequence Π is formed by all the obtained recipes and is closed by subterm. Since each $M \in St(\phi_1) \cup St(\phi_2)$ is of size smaller than $\max(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2))$, the size of any ζ of Π is controlled by: $f_5(2\max(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)))$ and Π (and thus ϕ_1' and ϕ_2') can be computed in time

$$(t_{\mathsf{dag}}(\phi_1) + t_{\mathsf{dag}}(\phi_2))[f_4(2\max(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)))] \tag{9}$$

The (dag) size of ϕ_i' is controlled by

– the initial dag size of ϕ_i, which is smaller than $\max(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2))$,

– plus the sum of the sizes of the added recipes ζ, which is itself controlled by

$$(t_{\mathsf{dag}}(\phi_1) + t_{\mathsf{dag}}(\phi_2)) f_5(2\max(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2))),$$

– plus the number of added terms, that is at most $t_{\mathsf{dag}}(\phi_1)+t_{\mathsf{dag}}(\phi_2)$.

We deduce that the (dag) size of ϕ'_i is controlled by

$$A_1 = \max(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2))+ (t_{\mathsf{dag}}(\phi_1)+t_{\mathsf{dag}}(\phi_2)) f_5(2\max(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)))+t_{\mathsf{dag}}(\phi_1)+t_{\mathsf{dag}}(\phi_2).$$

Step 2. We then compute $\nu\tilde{n}_{F_2}.(\phi'_1{\downarrow})^{\rho_2}$ and $\nu\tilde{n}_{F_2}.(\phi'_2{\downarrow})^{\rho_2}$ (resp. $\nu\tilde{n}_{F_1}.(\phi'_1{\downarrow})^{\rho_1}$, and $\nu\tilde{n}_{F_1}.(\phi'_2{\downarrow})^{\rho_1}$). As explained in the complexity analysis of the decidability of the deduction problem, this can be computed (by possibly duplicating some nodes) in time

$$A_1{}^2 + A_1{}^2 + (A_1 + A_1) f_0(2(A_1 + A_1)) = 2A_1(A_1 + f_0(4A_1)) \quad (10)$$

and the number of nodes of the dag representation of $(\phi'_i{\downarrow})^{\rho_j}$ has at most doubled compared to the initial frame ϕ'_i. Thus the dag size of each resulting frame $(\phi'_i{\downarrow})^{\rho_j}$ is smaller than $2A_1$.

Checking $\nu\tilde{n}_{F_2}.(\phi'_1{\downarrow})^{\rho_2} \approx_{\mathsf{E}_1} \nu\tilde{n}_{F_2}.(\phi'_2{\downarrow})^{\rho_2}$ and $\nu\tilde{n}_{F_1}.(\phi'_1{\downarrow})^{\rho_1} \approx_{\mathsf{E}_2} \nu\tilde{n}_{F_1}.(\phi'_2{\downarrow})^{\rho_1}$ can therefore be done in time:

$$f_1(2A_1 + 2A_1) + f_2(2A_1 + 2A_1) = f_1(4A_1) + f_2(4A_1). \quad (11)$$

Summing (9), (10), and (11), we conclude that checking $\phi_1 \approx_{\mathsf{E}} \phi_2$ can be done in time

$$(t_{\mathsf{dag}}(\phi_1) + t_{\mathsf{dag}}(\phi_2))[f_4(2\max(t_{\mathsf{dag}}(\phi_1), t_{\mathsf{dag}}(\phi_2)))] + 2A_1(A_1 + f_0(4A_1)) + f_1(4A_1) + f_2(4A_1).$$