Mathieu Baudet, Véronique Cortier, and Stéphanie Delaune

YAPA: A generic tool for computing intruder knowledge

Research Report LSV-09-03

February 2009

Laboratoire Spécification et Vérification

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

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

YAPA: A generic tool for computing intruder knowledge*

Mathieu Baudet[1], Véronique Cortier[2], and Stéphanie Delaune[3]

[1] DCSSI, France
[2] LORIA, CNRS & INRIA project Cassis, France
[3] LSV, ENS Cachan & CNRS & INRIA, France

Abstract. Reasoning about the knowledge of an attacker is a necessary step in many formal analyses of security protocols. In the framework of the applied pi calculus, as in similar languages based on equational logics, knowledge is typically expressed by two relations: deducibility and static equivalence. Several decision procedures have been proposed for these relations under a variety of equational theories. However, each theory has its particular algorithm, and none has been implemented so far.

We provide a generic procedure for deducibility and static equivalence that takes as input any convergent rewrite system. We show that our algorithm covers all the existing decision procedures for convergent theories. We also provide an efficient implementation, and compare it briefly with the more general tool ProVerif.

1 Introduction

Understanding security protocols often requires reasoning about the information accessible to an online attacker. Accordingly, many formal approaches to security rely on a notion of *deducibility* [17, 18] that models whether a piece of data, typically a secret, is retrievable from a finite set of messages. Deducibility, however, does not always suffice to reflect the knowledge of an attacker. Consider for instance a protocol sending an encrypted Boolean value, say, a vote in an electronic voting protocol. Rather than deducibility, the key idea to express confidentiality of the plaintext is that an attacker should not be able to *distinguish* between the sequences of messages corresponding to each possible value.

In the framework of the applied pi-calculus [3], as in similar languages based on equational logics [9], indistinguishability corresponds to a relation called *static equivalence*: roughly, two sequences of messages are *statically equivalent* when they satisfy the same algebraic relations from the attacker's point of view. Static equivalence plays an important role in the study of guessing attacks (e.g. [12, 5, 1]), as well as for anonymity properties and electronic voting protocols (e.g. [16]). In several cases, this notion has also been shown to imply the more complex and precise notion of cryptographic indistinguishability [7, 1], related to probabilistic polynomial-time Turing machines.

* This work has been partly supported by the ANR SeSur AVOTÉ.

We emphasize that both deducibility and static equivalence apply to observations on finite sets of messages, and do not take into account the dynamic behavior of protocols. Nevertheless, deducibility is used as a subroutine by many general decision procedures [11, 10]. Besides, it has been shown that observational equivalence in the applied pi-calculus coincides with labeled bisimulation [3], that is, corresponds to checking a number of static equivalences and some standard bisimulation conditions.

Deducibility and static equivalence rely on an underlying equational theory for axiomatizing the properties of cryptographic functions. Many decision procedures [2, 13] have been proposed to compute these relations under a variety of equational theories, including symmetric and asymmetric encryptions, signatures, exclusive OR, and homomorphic operators. However, except for the class of subterm convergent theories [2], which covers the standard flavors of encryption and signature, each of these decision results introduces a new procedure, devoted to a particular theory. Even in the case of the general decidability criterion given in [2], we note that the algorithm underlying the proof has to be adapted for each theory, depending on how the criterion is fulfilled.

Perhaps as a consequence of this fact, none of these decision procedures has been implemented so far. Up to our knowledge the only tool able to verify static equivalence is ProVerif [8, 9]. This general tool can handle various equational theories and analyze security protocols under active adversaries. However termination of the verifier is not guaranteed in general, and protocols are subject to (safe) approximations.

The present work aims to fill this gap between theory and implementation and propose an efficient tool for deciding deducibility and static equivalence in a uniform way. It is initially inspired from a procedure for solving more general constraint systems related to active adversaries and equivalence of finite processes, presented in [5], with corrected extended version in [6] (in French). However, due to the complexity of the constraint systems, this decision procedure was only studied for subterm convergent theories, and remains too complex to allow for an efficient implementation.

Our first contribution is to provide and study a generic procedure for checking deducibility and static equivalence, taking as input any convergent theory (that is, any equational theory described by a finite convergent rewrite system). We prove the algorithm sound and complete, up to explicit failure cases. Note that (unfailing) termination cannot be guaranteed in general since the problem of checking deducibility and static equivalence is undecidable, even for convergent theories [2]. To address this issue and turn our algorithm into a decision procedure for a given theory, we provide two criteria. First, we define a syntactic criterion on the rewrite rules that ensures that the algorithm never fails. This criterion is enjoyed in particular by any convergent subterm theory, as well as the theories of blind signature and homomorphic encryption. Termination often follows from a simple analysis of the rules of the algorithm: as a proof of concept, we obtain a new decidability result for deducibility and static equivalence for the prefix theory, representing encryption in CBC mode. Second, we provide a termination criterion based on deducibility: provided that failure cannot occur, termination on a given input is equivalent to the existence of some natural finite representation of deducible terms. As a consequence, we obtain that our algorithm can decide deducibility and static equivalence for all the convergent theories previously known to be decidable [2].

Our second contribution is an efficient implementation of this generic procedure, called YAPA. After describing the main features of the implementation, we report several experiments suggesting that our tool computes static equivalence faster and for more convergent theories than the general tool ProVerif [8, 9].

2 Preliminaries

2.1 Term algebra

We start by introducing the necessary notions to describe cryptographic messages in a symbolical way. For modeling cryptographic primitives, we assume a given set of *function symbols* $\mathcal{F}$ together with an arity function $\mathrm{ar} : \mathcal{F} \to \mathbb{N}$. Symbols in $\mathcal{F}$ of arity 0 are called *constants*. We consider a set of *variables* $\mathcal{X}$ and a set of additional constants $\mathcal{W}$ called *parameters*. The (usual, first-order) term algebra generated by $\mathcal{F}$ over $\mathcal{W}$ and $\mathcal{X}$ is written $\mathcal{F}[\mathcal{W} \cup \mathcal{X}]$ with elements denoted by $T, U, T_1 \ldots$ More generally, we write $\mathcal{F}'[A]$ for the least set of terms containing a set A and stable by application of symbols in $\mathcal{F}' \subseteq \mathcal{F}$.

We write $\mathrm{var}(T)$ (resp. $\mathrm{par}(T)$) for the set of variables (resp. parameters) that occur in a term T. These notations are extended to tuples and sets of terms in the usual way. The set of positions of a term T is written $\mathrm{pos}(T) \subseteq \mathbb{N}^*$. The subterm of T at position $p \in \mathrm{pos}(T)$ is written $T|_p$. The term obtained by replacing $T|_p$ with a term U in T is denoted $T[U]_p$.

A *(finite, partial) substitution* σ is a mapping from a finite subset of variables, called its *domain* and written $\mathrm{dom}(\sigma)$, to terms. The *image* of a substitution is its image as a mapping $\mathrm{im}(\sigma) = \{\sigma(x) \mid x \in \mathrm{dom}(\sigma)\}$. Substitutions are extended to endomorphisms of $\mathcal{F}[\mathcal{X} \cup \mathcal{W}]$ as usual. We use a postfix notation for their application. A term T (resp. a substitution σ) is *ground* iff $\mathrm{var}(T) = \emptyset$ (resp. $\mathrm{var}(\mathrm{im}(\sigma)) = \emptyset$).

For our cryptographic purposes, it is useful to distinguish a subset $\mathcal{F}_{\mathsf{pub}}$ of $\mathcal{F}$, made of *public function symbols*, that is, intuitively, the symbols made available to the attacker. A *recipe* (or *second-order term*) M, N, $M_1 \ldots$ is a term in $\mathcal{F}_{\mathsf{pub}}[\mathcal{W} \cup \mathcal{X}]$, that is, a term containing no *private* (non-public) function symbols. A *plain term* (or *first-order term*) t, r, s, $t_1 \ldots$ is a term in $\mathcal{F}[\mathcal{X}]$, that is, containing no parameters. A *(public, ground, non-necessarily linear) n-ary context* C is a recipe in $\mathcal{F}_{\mathsf{pub}}[\mathsf{w}_1, \ldots, \mathsf{w}_n]$, where we assume a fixed countable subset of parameters $\{\mathsf{w}_1, \ldots, \mathsf{w}_n, \ldots\} \subseteq \mathcal{W}$. If C is a n-ary context, $C[T_1, \ldots, T_n]$ denotes the term obtained by replacing each occurrence of w_i with T_i in C.

2.2 Rewriting

A *rewrite system* $\mathcal{R}$ is a finite set of *rewrite rules* $l \to r$ where $l, r \in \mathcal{F}[\mathcal{X}]$ and $\mathrm{var}(r) \subseteq \mathrm{var}(l)$. A term S *rewrites* to T by $\mathcal{R}$, denoted $S \to_{\mathcal{R}} T$, if there exist

$l \to r$ in $\mathcal{R}$, $p \in \text{pos}(S)$ and a substitution σ such that $S|_p = l\sigma$ and $T = S[r\sigma]_p$. We write $\to^+_{\mathcal{R}}$ for the transitive closure of $\to_{\mathcal{R}}$, $\to^*_{\mathcal{R}}$ for its reflexive and transitive closure, and $=_{\mathcal{R}}$ for its reflexive, symmetric and transitive closure.

A rewrite system $\mathcal{R}$ is *convergent* if is *terminating*, i.e. there is no infinite chains $T_1 \to_{\mathcal{R}} T_2 \to_{\mathcal{R}} \ldots$, and *confluent*, i.e. for every terms S, T such that $S =_{\mathcal{R}} T$, there exists U such that $S \to^*_{\mathcal{R}} U$ and $T \to^*_{\mathcal{R}} U$.

A term T is *$\mathcal{R}$-reduced* if there is no term S such that $T \to_{\mathcal{R}} S$. If $T \to^*_{\mathcal{R}} S$ and S is $\mathcal{R}$-reduced then S is *a $\mathcal{R}$-reduced form of* T. When this reduced form is unique (in particular if $\mathcal{R}$ is convergent), we write $S = T{\downarrow_{\mathcal{R}}}$.

2.3 Equational theories

We equip the signature $\mathcal{F}$ with an equational theory represented by a set of equations $\mathcal{E}$ of the form $s = t$ with $s, t \in \mathcal{F}[\mathcal{X}]$. The equational theory E generated by $\mathcal{E}$ is the least set of equations containing $\mathcal{E}$ that is stable under the axioms of congruence (reflexivity, symmetry, transitivity, application of function symbols) and under application of substitutions. We write $=_{\mathsf{E}}$ for the corresponding relation on terms. Equational theories have proved very useful for modeling algebraic properties of cryptographic primitives [14, 2].

We are particularly interested in theories E that can be represented by a convergent rewrite system $\mathcal{R}$, i.e. theories for which there exists a convergent rewrite system $\mathcal{R}$ such that the two relations $=_{\mathcal{R}}$ and $=_{\mathsf{E}}$ coincide. The rewrite system $\mathcal{R}$ —and by extension the equational theory E— is *subterm convergent* if, in addition, we have that for every rule $l \to r \in \mathcal{R}$, r is either a subterm of l or a ground $\mathcal{R}$-reduced term. This class encompasses the one of the same name used in [2], the class of dwindling theories used in [4], and the class of public-collapsing theories introduced in [15].

Example 1. Consider the signature $\mathcal{F}_{\mathsf{enc}} = \{\mathsf{dec}, \mathsf{enc}, \langle \_, \_ \rangle, \pi_1, \pi_2\}$. The symbols $\mathsf{dec}, \mathsf{enc}$ and $\langle \_, \_ \rangle$ are functional symbols of arity 2 that represent respectively the decryption, encryption and pairing functions, whereas π_1 and π_2 are functional symbols of arity 1 that represent the projection function on the first and the second component of a pair, respectively. The equational theory of pairing and symmetric (deterministic) encryption, denoted by $\mathsf{E}_{\mathsf{enc}}$, is generated by the equations $\mathcal{E}_{\mathsf{enc}} = \{\mathsf{dec}(\mathsf{enc}(x, y), y) = x,\ \ \pi_1(\langle x, y\rangle) = x,\ \ \pi_2(\langle x, y\rangle) = y\}$.

Motivated by the modeling of the ECB mode of encryption, we may also consider an encryption symbol that is homomorphic with respect to pairing:

$$\mathcal{E}_{\mathsf{hom}} = \mathcal{E}_{\mathsf{enc}} \cup \left\{ \begin{array}{l} \mathsf{enc}(\langle x, y\rangle, z) = \langle \mathsf{enc}(x, z), \mathsf{enc}(y, z)\rangle \\ \mathsf{dec}(\langle x, y\rangle, z) = \langle \mathsf{dec}(x, z), \mathsf{dec}(y, z)\rangle \end{array} \right\}.$$

If we orient the equations from left to right, we obtain two rewrite systems $\mathcal{R}_{\mathsf{enc}}$ and $\mathcal{R}_{\mathsf{hom}}$. Both rewrite systems are convergent, only $\mathcal{R}_{\mathsf{enc}}$ is subterm convergent.

From now on, we assume a given equational theory E represented by a convergent rewrite system $\mathcal{R}$. A symbol f is *free* if f does not occur in $\mathcal{R}$. In order to model (an unbounded number of) random values possibly generated by the attacker, we assume that $\mathcal{F}_{\mathsf{pub}}$ contains infinitely many free public constants. We will use free private constants to model secrets, for instance the secret keys used to encrypt a message. Private (resp. public) free constants are closely related to bound (resp. free) *names* in the framework of the applied pi calculus [3]. Our formalism also allows one to consider non-constant private symbols.

3 Deducibility and static equivalence

In order to describe the cryptographic messages observed or inferred by an attacker, we introduce the following notions of deduction facts and frames.

A *deduction fact* is a pair, written $M \rhd t$, made of a recipe $M \in \mathcal{F}_{\mathsf{pub}}[\mathcal{W} \cup \mathcal{X}]$ and a plain term $t \in \mathcal{F}[\mathcal{X}]$. Such a deduction fact is *ground* if $\mathrm{var}(M, t) = \emptyset$. A *frame*, denoted by letters φ, Φ, $\Phi_0 \ldots$, is a finite set of ground deduction facts. The *image* of a frame is defined by $\mathrm{im}(\Phi) = \{t \mid M \rhd t \in \Phi\}$. A frame Φ is *one-to-one* if $M_1 \rhd t$, $M_2 \rhd t \in \Phi$ implies $M_1 = M_2$.

A frame φ is *initial* if it is of the form $\varphi = \{w_1 \rhd t_1, \ldots, w_\ell \rhd t_\ell\}$ for some distinct parameters $w_1, \ldots, w_\ell \in \mathcal{W}$. Initial frames are closely related to the notion of frames in the applied pi-calculus [3]. The parameters w_i can be seen as labels that refer to the messages observed by an attacker. Given such an initial frame φ, we denote by $\mathrm{dom}(\varphi)$ its *domain* $\mathrm{dom}(\varphi) = \{w_1, \ldots, w_\ell\}$. If $\mathrm{par}(M) \subseteq \mathrm{dom}(\varphi)$, we write $M\varphi$ for the term obtained by replacing each w_i by t_i in M. We note that if in addition M is ground then $t = M\varphi$ is a ground plain term.

3.1 Deducibility, recipes

Classically (see e.g. [2]), a ground term t is *deducible* modulo E from an initial frame φ if there exists $M \in \mathcal{F}_{\mathsf{pub}}[\mathrm{dom}(\varphi)]$ such that $M\varphi =_{\mathsf{E}} t$. This corresponds to the intuition that the attacker may compute (infer) t from φ. For the purpose of our study, we generalize this notion to arbitrary frames, and even sets of (non-necessarily ground) deductions facts ϕ, using the notations $\rhd_\phi$ and $\rhd_\phi^{\mathsf{E}}$ defined as follows.

Definition 1 (deducibility). *Let ϕ be finite set of deductions facts, for instance a frame. We say that M* is a recipe of t in ϕ, *written $M \rhd_\phi t$, iff there exist a (public, ground, non-necessarily linear) n-ary context C and some deduction facts $M_1 \rhd t_1, \ldots, M_n \rhd t_n$ in ϕ such that $M = C[M_1, \ldots, M_n]$ and $t = C[t_1, \ldots, t_n]$. In that case, we say that t is* syntactically deducible *from ϕ, also written $\phi \vdash t$.*

We say that M is a recipe of t in ϕ modulo E, *written $M \rhd_\phi^{\mathsf{E}} t$, iff there exists a term t' such that $M \rhd_\phi t'$ and $t' =_{\mathsf{E}} t$. In that case, we say that t is* deducible from ϕ modulo E, *written $\phi \vdash_{\mathsf{E}} t$.*

We note that $M \rhd_\varphi t$ is equivalent to $M\varphi = t$ when φ is an initial frame and when t (or equivalently M) is ground.

Example 2. Consider the equational theory $\mathsf{E}_{\mathsf{enc}}$ given in Example 1. Let $\varphi = \{\mathsf{w}_1 \rhd \langle \mathsf{enc}(\mathsf{s}_1, \mathsf{k}), \mathsf{enc}(\mathsf{s}_2, \mathsf{k})\rangle, \mathsf{w}_2 \rhd \mathsf{k}\}$ where s_1, s_2 and k are private constant symbols. We have that $\langle \mathsf{w}_2, \mathsf{w}_2\rangle \rhd_\varphi \langle \mathsf{k}, \mathsf{k}\rangle$, and $\mathsf{dec}(\mathsf{proj}_1(\mathsf{w}_1), \mathsf{w}_2) \rhd_\varphi^{\mathsf{E}_{\mathsf{enc}}} \mathsf{s}_1$.

3.2 Static equivalence, visible equations

Deducibility does not always suffice for expressing the knowledge of an attacker. In particular, it does not account for the partial information that an attacker may obtain about secrets. This issue motivates the study of visible equations and static equivalence [3], defined as follows.

Definition 2 (static equivalence). *Let φ be an initial frame. The set of* visible equations of φ modulo E *is defined as*

$$\mathrm{eq}_{\mathsf{E}}(\varphi) = \{M \bowtie N \mid M, N \in \mathcal{F}_{\mathsf{pub}}[\mathrm{dom}(\varphi)],\ M\varphi =_{\mathsf{E}} N\varphi\}$$

where $\bowtie$ is a dedicated commutative symbol. Two initial frames φ_1 and φ_2 with the same domain are statically equivalent *modulo* E*, written $\varphi_1 \approx_{\mathsf{E}} \varphi_2$, if their sets of visible equations are equal, i.e.* $\mathrm{eq}_{\mathsf{E}}(\varphi_1) = \mathrm{eq}_{\mathsf{E}}(\varphi_2)$.

This definition is in line with static equivalence in the applied pi calculus [3]. For the purpose of finitely describing the set of visible equations $\mathrm{eq}_{\mathsf{E}}(\varphi)$ of an initial frame, we introduce *quantified equations* of the form $\forall z_1, \ldots, z_q.M \bowtie N$ where $z_1, \ldots, z_q \in \mathcal{X}$, $q \geq 0$ and $\mathrm{var}(M, N) \subseteq \{z_1, \ldots, z_q\}$. In the following, finite sets of quantified equations are denoted Ψ, Ψ_0,... We write $\Psi \models M \bowtie N$ when the ground equation $M \bowtie N$ is a consequence of Ψ in the usual, first-order logics with equality axioms for the relation $\bowtie$ (that is, reflexivity, symmetry, transitivity and compatibility with symbols in $\mathcal{F}_{\mathsf{pub}}$). When no confusion arises, we may refer to quantified equations simply as *equations*. As usual, quantified equations are considered up to renaming of bound variables.

Example 3. Consider again the equational theory $\mathsf{E}_{\mathsf{enc}}$ given in Example 1. Let $\varphi_1 = \{\mathsf{w}_1 \rhd \mathsf{enc}(\mathsf{c}_0, \mathsf{k}),\ \mathsf{w}_2 \rhd \mathsf{k}\}$ and $\varphi_2 = \{\mathsf{w}_1 \rhd \mathsf{enc}(\mathsf{c}_1, \mathsf{k}),\ \mathsf{w}_2 \rhd \mathsf{k}\}$ where c_0, c_1 are public constants and k is a private constant. Let $\Psi_1 = \{\mathsf{enc}(\mathsf{c}_0, \mathsf{w}_2) \bowtie \mathsf{w}_1\}$ and $\Psi_2 = \{\mathsf{enc}(\mathsf{c}_1, \mathsf{w}_2) \bowtie \mathsf{w}_1\}$. We have that $\Psi_i \models \mathrm{eq}_{\mathsf{E}_{\mathsf{enc}}}(\varphi_i)$ for $i = 1, 2$. Hence, $\mathrm{eq}_{\mathsf{E}_{\mathsf{enc}}}(\varphi_1) \neq \mathrm{eq}_{\mathsf{E}_{\mathsf{enc}}}(\varphi_2)$ and the two frames φ_1 and φ_2 are not statically equivalent. However, it can be shown that $\{\mathsf{w}_1 \rhd \mathsf{enc}(\mathsf{c}_0, \mathsf{k})\} \approx_{\mathsf{E}_{\mathsf{enc}}} \{\mathsf{w}_1 \rhd \mathsf{enc}(\mathsf{c}_1, \mathsf{k})\}$.

4 Main procedure

In this section, we describe our algorithms for checking deducibility and static equivalence on convergent rewrite systems. After some additional notations, we present the core of the procedure, which consists of a set of transformation rules used to saturate a frame and a finite set of quantified equations. We then show how to use this procedure to decide deducibility and static equivalence, provided that saturation succeeds.

Soundness and completeness of the saturation procedure are detailed in Section 5. We provide sufficient conditions on the rewrite systems to ensure success of saturation in Section 6.

4.1 Decompositions of rewrite rules

Before stating the procedure, we introduce the following notion of *decomposition* to account for the possible superpositions of an attacker's context with a left-hand side of rewrite rule.

Definition 3 (decomposition). *Let n, p, q be non-negative integers. A (n, p, q)-*decomposition *of a term l (and by an extension of any rewrite rule $l \to r$) is a (public, ground, non-necessarily linear) context $D \in \mathcal{F}_{\mathsf{pub}}[\mathcal{W}]$ such that* $\mathrm{par}(D) = \{\mathsf{w}_1, \ldots, \mathsf{w}_{n+p+q}\}$ *and $l = D[l_1, \ldots, l_n, y_1, \ldots, y_p, z_1, \ldots, z_q]$ where*

- *$l_1, \ldots, l_n$ are mutually-distinct non-variable terms,*
- *$y_1, \ldots, y_p$ and $z_1, \ldots, z_q$ are mutually-distinct variables, and*
- *$y_1, \ldots, y_p \in \mathrm{var}(l_1, \ldots, l_n)$ whereas $z_1, \ldots, z_q \notin \mathrm{var}(l_1, \ldots, l_n)$.*

A decomposition D is proper *if it is not a parameter (i.e. $D \neq \mathsf{w}_1$).*

Example 4. Consider the rewrite rule $\mathsf{dec}(\mathsf{enc}(x, y), y) \to x$. This rule admits two proper decompositions up to permutation of parameters:

- $D_1 = \mathsf{dec}(\mathsf{enc}(\mathsf{w}_1, \mathsf{w}_2), \mathsf{w}_2)$ where $n = 0$, $p = 0$, $q = 2$, $z_1 = x$, $z_2 = y$;
- $D_2 = \mathsf{dec}(\mathsf{w}_1, \mathsf{w}_2)$ where $n = 1$, $p = 1$, $q = 0$, $l_1 = \mathsf{enc}(x, y)$ and $y_1 = y$.

4.2 Transformation rules

To check deducibility and static equivalence, we proceed by saturating an initial frame, adding some deduction facts and equations satisfied by the frame. We consider *states* that are either the failure state $\perp$ or a couple (Φ, Ψ) formed by a one-to-one frame Φ in $\mathcal{R}$-reduced form and a finite set of quantified equations Ψ.

Given an initial frame φ, our procedure starts from an initial state associated to φ, denoted by $\mathrm{Init}(\varphi)$, obtained by reducing φ and replacing duplicated terms by equations. Formally, $\mathrm{Init}(\varphi)$ is the result of a procedure recursively defined as follows: $\mathrm{Init}(\emptyset) = (\emptyset, \emptyset)$, and assuming $\mathrm{Init}(\varphi) = (\Phi, \Psi)$, we have

$$\mathrm{Init}(\varphi \uplus \{w \rhd t\}) = \begin{cases} (\Phi, \Psi \cup \{w \bowtie w'\}) & \text{if there exists some } w' \rhd t{\downarrow_{\mathcal{R}}} \in \Phi \\ (\Phi \cup \{w \rhd t{\downarrow_{\mathcal{R}}}\}, \Psi) & \text{otherwise.} \end{cases}$$

The main part of our procedure consists in saturating a state (Φ, Ψ) by means of the transformation rules described in Figure 1. The **A** rules are designed for applying a rewrite step on top of existing deduction facts. If the resulting term is already syntactically deducible then a corresponding equation is added (rule **A.1**); or else if it is ground, the corresponding deduction fact is added to the state (rule **A.2**); otherwise, the procedure may fail (rule **A.3**). The **B** rules are meant to add syntactically deducible subterms (rule **B.2**) or related equations (rule **B.1**). For technical reasons, rule **A.1** is parametrized by a function Ctx with values of the form M or $\perp$, and satisfying the following properties:

(a) if $\phi \vdash t{\downarrow_{\mathcal{R}}}$, then for any Ψ and α, $\mathrm{Ctx}(\phi \vdash^?_{\mathcal{R}} t, \Psi, \alpha) \neq \perp$;

A. Inferring deduction facts and equations by context reduction
Assume that

$l = D[l_1, \ldots, l_n, y_1, \ldots, y_p, z_1, \ldots, z_q]$ is a proper decomposition of $(l \to r) \in \mathcal{R}$
$M_1 \rhd t_1, \ldots, M_{n+p} \rhd t_{n+p} \in \Phi$
$(l_1, \ldots, l_n, y_1, \ldots, y_p)\,\sigma = (t_1, \ldots, t_{n+p})$

1. If there exists $M = \mathrm{Ctx}(\Phi \cup \{z_1 \rhd z_1, \ldots, z_q \rhd z_q\} \vdash^?_{\mathcal{R}} r\sigma,\ \Psi,\ (l, r, D, \sigma))$, then

$$(\Phi, \Psi) \Longrightarrow (\Phi, \Psi \cup \{\forall z_1, \ldots, z_q.D[M_1, \ldots, M_{n+p}, z_1 \ldots, z_q] \bowtie M\}) \qquad \textbf{(A.1)}$$

2. Else, if $(r\sigma){\downarrow_{\mathcal{R}}}$ is ground, then

$$\begin{aligned}(\Phi, \Psi) \Longrightarrow (&\Phi \cup \{M_0 \rhd (r\sigma){\downarrow_{\mathcal{R}}}\},\\ &\Psi \cup \{\forall z_1, \ldots, z_q.D[M_1, \ldots, M_{n+p}, z_1 \ldots, z_q] \bowtie M_0\})\end{aligned} \qquad \textbf{(A.2)}$$

where $M_0 = D[M_1, \ldots, M_{n+p}, \mathsf{a}, \ldots, \mathsf{a}]$ for some fixed public constant a.

3. Otherwise, $(\Phi, \Psi) \Longrightarrow \perp$ **(A.3)**

B. Inferring deduction facts and equations syntactically
Assume that $M_0 \rhd t_0, \ldots, M_n \rhd t_n \in \Phi \qquad t = f(t_1, \ldots, t_n) \in \mathrm{st}(t_0) \qquad f \in \mathcal{F}_{\mathsf{pub}}$

1. If there exists M such that $(M \rhd t) \in \Phi$,

$$(\Phi, \Psi) \Longrightarrow (\Phi, \Psi \cup \{f(M_1, \ldots, M_n) \bowtie M\}) \qquad \textbf{(B.1)}$$

2. Otherwise, $(\Phi, \Psi) \Longrightarrow (\Phi \cup \{f(M_1, \ldots, M_n) \rhd t\}, \Psi)$ **(B.2)**

Fig. 1. Transformation rules

(b) if $M = \mathrm{Ctx}(\phi \vdash^?_{\mathcal{R}} t,\ \Psi, \alpha)$ then there exists M' and s such that $\Psi \models M \bowtie M'$, $M' \rhd_\phi s$ and $t \to^*_{\mathcal{R}} s$. (This justifies the notation $\phi \vdash^?_{\mathcal{R}} t$ used to denote a specific deducibility problem.)

Note that a simple choice for $\mathrm{Ctx}(\phi \vdash^?_{\mathcal{R}} t, \Psi, \alpha)$ is to solve the deducibility problem $\phi \vdash^? t{\downarrow_{\mathcal{R}}}$ in the empty equational theory, and then return a corresponding recipe M, if any. (This problem is easily solved by induction on $t{\downarrow_{\mathcal{R}}}$.) Yet, optimizing the function Ctx is a nontrivial task: on the one hand, letting $\mathrm{Ctx}(\phi \vdash^?_{\mathcal{R}} t, \Psi, \alpha) \neq \perp$ for more values ϕ, t, Ψ, α makes the procedure more likely to succeed; on the other hand, it is computationally more demanding. We explain in Section 6.2 the choice of Ctx made in our implementation.

We write $\Longrightarrow^*$ for the transitive and reflexive closure of $\Longrightarrow$. The definitions of Ctx and of the transformation rules ensure that whenever $S \Longrightarrow^* S'$ and S is a state, then S' is also a state, with the same parameters unless $S' = \perp$.

Example 5. Consider the frame φ_1 previously described in Example 3. We can apply rule **A.1** as follows. Consider the rewrite rule $\mathsf{dec}(\mathsf{enc}(x, y), y) \to x$, the decomposition D_2 given in Example 4 and $t_1 = \mathsf{enc}(\mathsf{c}_0, \mathsf{k})$. We have $\mathrm{Init}(\varphi_1) = (\varphi_1, \emptyset) \Longrightarrow (\varphi_1, \{\mathsf{dec}(\mathsf{w}_1, \mathsf{w}_2) \bowtie \mathsf{c}_0\})$. In other words, since we know the key k through w_2, we can check that the decryption of w_1 by w_2 leads to the public constant c_0. Next we apply rule **B.1** as follows: $(\varphi_1, \{\mathsf{dec}(\mathsf{w}_1, \mathsf{w}_2) \bowtie \mathsf{c}_0\}) \Longrightarrow (\varphi_1, \{\mathsf{dec}(\mathsf{w}_1, \mathsf{w}_2) \bowtie \mathsf{c}_0, \mathsf{enc}(\mathsf{c}_0, \mathsf{w}_2) \bowtie \mathsf{w}_1\})$. No more rules can then modify the state.

Main theorem. We now state the soundness and the completeness of the transformation rules provided that a *saturated state* is reached, that is, a state $S \neq \bot$ such that $S \Longrightarrow S'$ implies $S' = S$. The technical lemmas involved in the proof are detailed in Section 5.

Theorem 1 (soundness and completeness). *Let* E *be an equational theory generated by a convergent rewrite system* $\mathcal{R}$*. Let* φ *be an initial frame and* (Φ, Ψ) *be a saturated state such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi, \Psi)$.

1. *For all* $M \in \mathcal{F}_{\mathsf{pub}}[\mathrm{par}(\varphi)]$ *and* $t \in \mathcal{F}[\emptyset]$*, we have*
$$M\varphi =_{\mathsf{E}} t \quad \Leftrightarrow \quad \exists N,\ \Psi \models M \bowtie N \text{ and } N \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$$
2. *For all* M*,* $N \in \mathcal{F}_{\mathsf{pub}}[\mathrm{par}(\varphi) \cup \mathcal{X}]$*, we have that* $M\varphi =_{\mathsf{E}} N\varphi \Leftrightarrow \Psi \models M \bowtie N$.

While the saturation procedure is sound and complete, it may not terminate, or *fail* if rule **A.3** becomes the only applicable rule at some point of computation. In Section 6, we explore several sufficient conditions to prevent failure and ensure termination.

4.3 Application to deduction and static equivalence

Decision procedures for deduction and static equivalence follow from Theorem 1.

Algorithm for deduction. Let φ be an initial frame and t be a ground term. The procedure for checking $\varphi \vdash_{\mathsf{E}} t$ runs as follows:

1. Apply the transformation rules to obtain (if any) a saturated state (Φ, Ψ) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi, \Psi)$;
2. Return *yes* if there exists N such that $N \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$ (that is, the $\mathcal{R}$-reduced form of t is syntactically deducible from Φ); otherwise return *no*.

Algorithm for static equivalence. Let φ_1 and φ_2 be two initial frames. The procedure for checking $\varphi_1 \approx_{\mathsf{E}} \varphi_2$ runs as follows:

1. Apply the transformation rules to obtain (if possible) two saturated states (Φ_1, Ψ_1) and (Φ_2, Ψ_2) such that $\mathrm{Init}(\varphi_i) \Longrightarrow^* (\Phi_i, \Psi_i)$, $i = 1, 2$;
2. For $\{i, j\} = \{1, 2\}$, for every equation $(\forall z_1, \ldots, z_\ell. M \bowtie N)$ in Ψ_i, check that $M\varphi_j =_{\mathsf{E}} N\varphi_j$ — that is, in other words, $(M\varphi_j){\downarrow_{\mathcal{R}}} = (N\varphi_j){\downarrow_{\mathcal{R}}}$;
3. If so return *yes*; otherwise return *no*.

5 Soundness and completeness of the saturation

The proof of Theorem 1 is based on three main lemmas. First, the transformation rules are sound in the sense that, along the saturation process, we add only deducible terms and valid equations with respect to the initial frame.

Lemma 1 (soundness). *Let φ be an initial frame and (Φ, Ψ) be a state such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi, \Psi)$*. Then, we have that*

1. $M \rhd_\Phi t \;\Rightarrow\; M\varphi =_{\mathsf{E}} t$ *for all* $M \in \mathcal{F}_{\mathsf{pub}}[\mathrm{dom}(\varphi)]$ *and* $t \in \mathcal{F}[\emptyset]$*;*
2. $\Psi \models M \bowtie N \;\Rightarrow\; M\varphi =_{\mathsf{E}} N\varphi$ *for all* $M, N \in \mathcal{F}_{\mathsf{pub}}[\mathrm{dom}(\varphi) \cup \mathcal{X}]$*.*

The next two lemmas are dedicated to the completeness of **B** and **A** rules, respectively. Lemma 2 ensures that saturated states account for all the syntactic equations possibly visible. Lemma 3 deals with the reduction of a deducible term along the rewrite system $\mathcal{R}$. Using that $\mathcal{R}$ is convergent, this allows for proving that every deducible term from a saturated frame is syntactically deducible.

Lemma 2 (completeness, syntactic equations). *Let (Φ, Ψ) be a state, and M, N be two terms such that $M \rhd_\Phi t$ and $N \rhd_\Phi t$ for some term t. Then there exists (Φ', Ψ') such that $(\Phi, \Psi) \Longrightarrow^* (\Phi', \Psi')$ using **B** rules and $\Psi' \models M \bowtie N$.*

Lemma 3 (completeness, context reduction). *Let (Φ, Ψ) be a state and M, t, t' be three terms such that $M \rhd_\Phi t$ and $t \to_{\mathcal{R}} t'$. Then, either $(\Phi, \Psi) \Longrightarrow^* \bot$ or there exist (Φ', Ψ'), M' and t'' such that $(\Phi, \Psi) \Longrightarrow^* (\Phi', \Psi')$, $M' \rhd_{\Phi'} t''$ with $t' \to^*_{\mathcal{R}} t''$, and $\Psi' \models M \bowtie M'$.*

*Besides, in both cases, the corresponding derivation from (Φ, Ψ) can be chosen to consist of a number of **B** rules, possibly followed by one instance of **A** rule involving the same rewrite rule $l \to r$ as the rewrite step $t \to_{\mathcal{R}} t'$.*

6 Termination and non-failure

In the previous section, we proved that saturated frames yield sound and complete characterizations of deducible terms and visible equations of their initial frames. Yet, the saturation procedure may still not terminate, or fail due to rule **A.3**. In this section, we study different conditions on the rewrite system $\mathcal{R}$ so that failure never happens and/or termination is ensured.

6.1 A syntactic criterion to prevent failure

Our first criterion is syntactic and ensures that the algorithm never fails. It is enjoyed by a large class of equational theories, called *layered convergent*.

Definition 4 (layered rewrite system). *A rewrite system $\mathcal{R}$, and by extension its equational theory E, are* layered *if there exists an ascending chain of subsets $\emptyset = \mathcal{R}_0 \subseteq \mathcal{R}_1 \subseteq \ldots \subseteq \mathcal{R}_{N+1} = \mathcal{R}$ $(N \geq 0)$, such that for every $0 \leq i \leq N$, for every rule $l \to r$ in $\mathcal{R}_{i+1} - \mathcal{R}_i$, for every (n, p, q)-decomposition $l = D[l_1, \ldots, l_n, y_1, \ldots, y_p, z_1, \ldots, z_q]$, one of the following two conditions holds:*

(i) $\mathrm{var}(r) \subseteq \mathrm{var}(l_1, \ldots, l_n)$*;*
(ii) there exists $C_0, C_1, \ldots, C_k$ and $s_1, \ldots, s_k$ such that

– $r = C_0[s_1, \ldots, s_k]$;
– *for each* $1 \leq i \leq k$, $C_i[l_1, \ldots, l_n, y_1, \ldots, y_p, z_1, \ldots, z_q]$ *rewrites to* s_i *in zero or one step of rewrite rule in head position along* $\mathcal{R}_i$.

In the latter case, we say that the context $C = C_0[C_1, \ldots, C_k]$ *is* associated *to the decomposition* D *of* $l \to r$. *Note that* $C[l_1, \ldots, l_n, y_1, \ldots, y_p, z_1, \ldots, z_q] \to^*_{\mathcal{R}_i} r$.

Proposition 1. *Assume that the function* Ctx *in use is* maximal*: for every* ϕ *and* t, *if there exists* s *such that* $\phi \vdash s$ *and* $t \to^*_{\mathcal{R}} s$, *then for any* Ψ, α, $\mathrm{Ctx}(\phi \vdash^?_{\mathcal{R}} t, \Psi, \alpha) \neq \perp$. *Then, provided that* $\mathcal{R}$ *is layered convergent, there exists no state* (Φ, Ψ) *from which* $(\Phi, \Psi) \Longrightarrow \perp$ *is the only applicable derivation.*

Practical considerations. Unfortunately, such a maximal Ctx is too inefficient in practice as one has to consider the syntactic deducibility problem $\phi \vdash^? s$ for every $t \to^*_{\mathcal{R}} s$. This is why we rather use the following lighter implementation:

– for every index $0 \leq i \leq N$, and every rule $l \to r$ in $\mathcal{R}_{i+1} - \mathcal{R}_i$, if $l = D[l_1, \ldots, l_n, y_1, \ldots, y_{p+q}]$ is a (n, p, q)-decomposition satisfying condition (ii) above for some (arbitrarily chosen) associated context C, then, for every ϕ and σ such that $\phi \vdash l\sigma$, we let

$$\mathrm{Ctx}(\phi \vdash^?_{\mathcal{R}} r\sigma,\, \Psi,\, (l, r, D, \sigma)) \;=\; C[M_1, \ldots, M_{n+p+q}]$$

  where the M_k are fixed recipes such that $(M_i \rhd l_i\sigma) \in \phi$ for $1 \leq i \leq n$ and $(M_{n+j} \rhd y_j\sigma) \in \phi$ for $1 \leq j \leq p + q$;
– otherwise, if $\phi \vdash t{\downarrow_{\mathcal{R}}}$, we let $\mathrm{Ctx}(\phi \vdash^?_{\mathcal{R}} t, \Psi, \alpha)$ be some fixed M such that $M \rhd_\phi t{\downarrow_{\mathcal{R}}}$;
– in any other case, we let $\mathrm{Ctx}(\phi \vdash^?_{\mathcal{R}} t, \Psi, \alpha) \;=\; \perp$.

Using Lemma 3 in a similar way as for proving Proposition 1, we can show that, for any convergent rewrite system $\mathcal{R}$, this choice of Ctx is compatible with property (b) of subsection 4.2 as long as, during saturation, the transformation rules **A** involve the rewrite rules of $\mathcal{R}_i$ with greater priority than those of $\mathcal{R}_j$, $i < j$. Moreover, when $\mathcal{R}$ is additionally layered, this definition ensures that the procedure never fails. Indeed, using the notations of Figure 1, $\mathrm{Ctx}(\Phi \cup \{z_1 \rhd z_1, \ldots, z_q \rhd z_q\} \vdash^?_{\mathcal{R}} r\sigma,\, \Psi,\, (l, r, D, \sigma)) \;=\; \perp$ implies that (ii) is false on D, thus (i) $\mathrm{var}(r) \subseteq \mathrm{var}(l_1, \ldots, l_n)$ holds and $(r\sigma){\downarrow_{\mathcal{R}}}$ is ground.

Example 6. Any convergent subterm rewrite system $\mathcal{R}$ is layered convergent. Indeed, let $N = 0$ and $\mathcal{R}_1 = \mathcal{R}$. For any $l \to r$ in $\mathcal{R}$ and for every decomposition $l = D[l_1, \ldots, l_n, y_1, \ldots, y_p, z_1, \ldots, z_q]$, the term r is a subterm of l, thus either $r = C[l_1, \ldots, l_n, y_1, \ldots, y_p, z_1, \ldots, z_q]$ for some context C, or r is a subterm of some l_i thus $\mathrm{var}(r) \subseteq \mathrm{var}(l_1, \ldots, l_n)$.

Example 7. Other examples are provided by the theory of homomorphism $\mathsf{E}_{\mathsf{hom}}$ defined in Section 2.3 as well as the convergent theories of blind signatures $\mathsf{E}_{\mathsf{blind}}$ and prefix encryption $\mathsf{E}_{\mathsf{pref}}$ defined by the following sets of equations.

$$\mathcal{E}_{\mathsf{blind}} = \mathcal{E}_{\mathsf{enc}} \cup \left\{ \begin{array}{c} \mathsf{unblind}(\mathsf{blind}(x, y), y) = x \\ \mathsf{unblind}(\mathsf{sign}(\mathsf{blind}(x, y), z), y) = \mathsf{sign}(x, z) \end{array} \right\}$$

$$\mathcal{E}_{\mathsf{pref}} = \mathcal{E}_{\mathsf{enc}} \cup \left\{ \mathsf{pref}(\mathsf{enc}(\langle x, y \rangle, z)) = \mathsf{enc}(x, z) \right\}$$

The theory $\mathsf{E}_{\mathsf{blind}}$ models primitives used in e-voting protocols [16]. The prefix theory represents the property of many chained modes of encryption (e.g. CBC) where an attacker can retrieve any encrypted prefix out of a ciphertext.

Let us check for instance that the prefix theory $\mathsf{E}_{\mathsf{pref}}$ is layered. Let $N = 1$, $\mathcal{R}_1$ be the rewrite system obtained from $\mathcal{E}_{\mathsf{enc}}$ by orienting the equations from left to right, and $\mathcal{R}_2 = \mathcal{R}_1 \cup \{\mathsf{pref}(\mathsf{enc}(\langle x, y \rangle, z)) \to \mathsf{enc}(x, z)\}$. The rewrite rules of $\mathcal{R}_1$ satisfy the assumptions since $\mathcal{R}_1$ forms a convergent subterm rewrite system. The additional rule $\mathsf{pref}(\mathsf{enc}(\langle x, y \rangle, z)) \to \mathsf{enc}(x, z)$ admits three decompositions up to permutation of parameters:

- $l = \mathsf{pref}(l_1)$, in which case $\mathrm{var}(r) \subseteq \mathrm{var}(l_1)$;
- $l = \mathsf{pref}(\mathsf{enc}(l_1, z))$, in which case $\mathsf{enc}(\pi_1(l_1), z) \to_{\mathcal{R}_0} r$;
- $l = \mathsf{pref}(\mathsf{enc}(\langle x, y \rangle, z))$, in which case $r = \mathsf{enc}(x, z)$.

Verifying that the convergent theories $\mathsf{E}_{\mathsf{hom}}$ and $\mathsf{E}_{\mathsf{blind}}$ are layered is similar.

6.2 Termination

In the previous subsection, we described a sufficient criterion for non-failure. To obtain decidability for a given layered convergent theory, there remains only to provide a termination argument. Such an argument is generally easy to develop by hand as we illustrate on the example of the prefix theory. For the case of existing decidability results from [2], such as the theories of blind signature and homomorphic encryption, we also provide a semantic criterion that allows us to directly conclude termination of the procedure.

Proving termination by hand. To begin with, we note that **B** rules always terminate after a polynomial number of steps. Let us write $\stackrel{\centerdot}{\Longrightarrow}^n$ for the relation made of exactly n *strict applications* of rules ($S \stackrel{\centerdot}{\Longrightarrow} S'$ iff $S \Longrightarrow S'$ and $S \neq S'$).

Proposition 2. *For every states $S = (\Phi, \Psi)$ and S' such that $S \stackrel{\centerdot}{\Longrightarrow}^n S'$ using only **B** rules, n is polynomially bounded in the size of* $\mathrm{im}(\Phi)$.

This is due to the fact that frames are one-to-one and that the rule **B.2** only adds deduction facts $M \rhd t$ such that t is a subterm of an existing term in Φ. Hence, for proving termination, we observe that it is sufficient to provide a function s mapping each frame Φ to a finite set of terms $s(\Phi)$ including the subterms of $\mathrm{im}(\Phi)$ and such that rule **A.2** only adds deduction facts $M \rhd t$ satisfying $t \in s(\Phi)$.

For subterm theories, we obtain polynomial termination by choosing $s(\Phi)$ to be the subterms of $\mathrm{im}(\Phi)$ together with the ground right-hand sides of $\mathcal{R}$.

Proposition 3. *Let E be a convergent subterm theory. For every $S = (\Phi, \Psi)$ and S' such that $S \stackrel{\centerdot}{\Longrightarrow}^n S'$, n is polynomially bounded in the size of* $\mathrm{im}(\Phi)$.

To conclude that deduction and static equivalence are decidable in polynomial time [2], we need to show that the deduction facts and the equations are of polynomial size. This requires a DAG representation for terms and visible equations. For our implementation, we have chosen not to use DAGs for the sake of simplicity (and perhaps efficiency) since DAGs require much heavier data structures. However, similar techniques as those described in [2] would apply to implement our procedure using DAGs.

For proving termination of the prefix theory, we let $s(\Phi)$ be the minimal set containing Φ, closed by subterm and such that $\mathsf{enc}(t_1, k) \in s(\Phi)$ whenever $\mathsf{enc}(\langle t_1, t_2 \rangle, k) \in s(\Phi)$. We then deduce that deduction and static equivalence are decidable for the equational theory $\mathsf{E}_{\mathsf{pref}}$, which is a new decidability result.

A criterion to ensure termination. We now provide a semantic criterion that more generally explains why our procedure succeeds on theories previously known to be decidable [2]. This criterion intuitively states that the set of deducible terms from any initial frame φ should be equivalent to a set of *syntactically* deducible terms. Provided that failures are prevented and assuming a *fair* strategy for rule application, we prove that this criterion is a necessary and sufficient condition for our procedure to terminate.

Definition 5 (fair derivation). *An infinite derivation* $(\Phi_0, \Psi_0) \Longrightarrow \ldots \Longrightarrow (\Phi_n, \Psi_n) \Longrightarrow \ldots$ *is* fair *iff along this derivation,*

(a) ***B*** *rules are applied with greatest priority, and*
(b) whenever a ***A*** *rule is applicable for some instance* $(l \to r, D, t_1, \ldots, t_n, \ldots)$*, eventually the same instance of rule is applied during the derivation.*

Fairness implies that any deducible term is eventually syntactically deducible.

Lemma 4. *Let* $S_0 = (\Phi_0, \Psi_0) \Longrightarrow \ldots \Longrightarrow (\Phi_n, \Psi_n) \Longrightarrow \ldots$ *be an infinite fair derivation from a state* S_0*. For every ground term* t *such that* $\Phi_0 \vdash_{\mathsf{E}} t$*, either* $(\Phi_0, \Psi_0) \Longrightarrow^* \bot$ *or there exists* i *such that* $\Phi_i \vdash t{\downarrow_{\mathcal{R}}}$*.*

Proposition 4 (criterion for saturation). *Let* φ *be an initial frame such that* $\mathrm{Init}(\varphi) \not\Longrightarrow^* \bot$*. The following conditions are equivalent:*

(i) There exists a saturated couple (Φ, Ψ) *such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi, \Psi)$*.*
(ii) There exists a (finite) initial frame φ_s *such that for every term* t*,* t *is deducible from* φ *modulo* E *iff* $t{\downarrow_{\mathcal{R}}}$ *is syntactically deducible from* φ_s*.*
(iii) There exists no fair infinite derivation starting from $\mathrm{Init}(\varphi)$*.*

Together with the syntactic criterion described in Section 6.1, this criterion (Property *(ii)*) allows us to prove that deduction and static equivalence are decidable for layered convergent theories that are *locally stable*, as defined in [2]. As a consequence, our procedure always saturates for the theories of blind signatures and homomorphic encryption since those theories are layered and have been proved locally stable [2]. Other examples of layered convergent theories enjoying this criterion can be found in [2] (e.g. a theory of addition).

7 Implementation: the YAPA tool

YAPA is an Ocaml implementation[4] of the saturation procedure presented in Section 4, using by default the optimized function Ctx defined in Section 6, and a fair strategy of rule application (see Definition 5).

The tool takes as input an equational theory described by a finite convergent rewrite system, as well as frame definitions and queries. A few optimizations may be activated for subterm theories, e.g. to accelerate normalization. The procedure starts by computing the decompositions of the rewrite system. Given an appropriate ordering of the rewrite rules, it is able to recognize (fully or partially) layered theories and to pre-compute the associated contexts C related to condition (ii) of Definition 4, and exploited by the function Ctx in use.

We have conducted several experiments on a PC Intel Core 2 Duo at 2.4 GHz with 2 Go RAM for various equational theories (see below) and found that YAPA provides an efficient way to check static equivalence and deducibility.

Equational theory	$\mathsf{E_{enc}}$ $n = 10$	$\mathsf{E_{enc}}$ $n = 14$	$\mathsf{E_{enc}}$ $n = 16$	$\mathsf{E_{enc}}$ $n = 18$	$\mathsf{E_{enc}}$ $n = 20$	$\mathsf{E_{blind}}$	$\mathsf{E_{pref}}$	$\mathsf{E_{hom}}$	$\mathsf{E_{add}}$
Execution time	< 1s	1,7s	8s	30s	< 3min	< 1s	< 1s	< 1s	< 1s

For the case of $\mathsf{E_{enc}}$, we have run YAPA on the frames $\varphi_n = \{\mathsf{w}_1 \rhd t_n^0, \mathsf{w}_2 \rhd \mathsf{c}_0, \mathsf{w}_3 \rhd \mathsf{c}_1\}$ and $\varphi'_n = \{\mathsf{w}_1 \rhd t_n^1, \mathsf{w}_2 \rhd \mathsf{c}_0, \mathsf{w}_3 \rhd \mathsf{c}_1\}$, where $t_0^i = \mathsf{c}_i$ and $t_{n+1}^i = \langle \mathsf{enc}(t_n^i, \mathsf{k}_n^i), \mathsf{k}_n^i \rangle$, $i \in \{0, 1\}$. These examples allow us to increase the (tree, non-DAG) size of the distinguishing tests exponentially, while the sizes of the frames grow linearly. Despite the size of the output, we have observed satisfactory performances for the tool. We have also experimented YAPA on several convergent theories, e.g. $\mathsf{E_{blind}}$, $\mathsf{E_{hom}}$, $\mathsf{E_{pref}}$ and the theory of addition $\mathsf{E_{add}}$ defined in [2].

In comparison with the tool ProVerif [8, 9], here instrumented to check static equivalences, our test samples suggest a running time between one and two orders of magnitude faster for YAPA. Also we did not succeed in making ProVerif terminate on the two theories $\mathsf{E_{hom}}$ and $\mathsf{E_{add}}$. Of course, these results are not entirely surprising given that ProVerif is tailored for the more general (and difficult) problem of protocol (in)security under active adversaries. In particular ProVerif's initial preprocessing of the rewrite system appears more substantial than ours and is not guaranteed to terminate, even for subterm convergent theories (e.g. in the case of the theory generated by $f(g(f(x))) = x$).

Altogether, these results suggest that YAPA significantly improves the state of the art for checking deducibility and static equivalence under convergent theories, both from practical and theoretical perspectives.

References

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

[4] Freely available at `http://www.lsv.ens-cachan.fr/~baudet/yapa/`

2. M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 387(1-2):2–32, 2006.
3. M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115. ACM, 2001.
4. S. Anantharaman, P. Narendran, and M. Rusinowitch. Intruders with caps. In *18th International Conference on Term Rewriting and Applications (RTA'07)*, volume 4533 of *LNCS*. Springer, 2007.
5. M. Baudet. Deciding security of protocols against off-line guessing attacks. In *12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 16–25. ACM Press, 2005.
6. M. Baudet. *Sécurité des protocoles cryptographiques : aspects logiques et calculatoires*. Thèse de doctorat, LSV, ENS Cachan, France, 2007.
7. M. Baudet, V. Cortier, and S. Kremer. Computationally sound implementations of equational theories against passive adversaries. In *32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *LNCS*, pages 652–663. Springer, 2005.
8. B. Blanchet. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In *14th Computer Security Foundations Workshop (CSFW'01)*, pages 82–96. IEEE Comp. Soc. Press, 2001.
9. B. Blanchet, M. Abadi, and C. Fournet. Automated Verification of Selected Equivalences for Security Protocols. In *Symposium on Logic in Computer Science*, pages 331–340. IEEE Comp. Soc. Press, 2005.
10. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with XOR. In *18th IEEE Symposium on Logic in Computer Science (LICS'03)*. IEEE Comp. Soc. Press, 2003.
11. H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *18th IEEE Symposium on Logic in Computer Science (LICS'03)*. IEEE Comp. Soc. Press, 2003.
12. R. Corin, J. Doumen, and S. Etalle. Analysing password protocol security against off-line dictionary attacks. In *Proc. 2nd International Workshop on Security Issues with Petri Nets and other Computational Models (WISP'04)*, volume 121 of *ENTCS*, pages 47–63, 2004.
13. V. Cortier and S. Delaune. Deciding knowledge in security protocols for monoidal equational theories. In *14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07)*, volume 4790 of *LNAI*, pages 196–210. Springer, 2007.
14. V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.
15. S. Delaune and F. Jacquemard. A decision procedure for the verification of security protocols with explicit destructors. In *11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 278–287, 2004.
16. S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 2008. To appear.
17. G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS'96)*, volume 1055 of *LNCS*, pages 147–166. Springer-Verlag, 1996.
18. J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *8th ACM Conference on Computer and Communications Security (CCS'01)*, 2001.

A Soundness and completeness

Before going through the proofs, we note the following fact that justifies the expression "saturation procedure" used throughout this paper.

Lemma 5 (monotony). *Let (Φ,Ψ) and (Φ',Ψ') be such that $(\Phi,\Psi) \Longrightarrow^* (\Phi',\Psi')$. We have that $\Phi \subseteq \Phi'$ and $\Psi \subseteq \Psi'$. In particular, we note that*

- *$M \rhd_\Phi t$ implies $M \rhd_{\Phi'} t$;*
- *$\Psi \models M \bowtie N$ implies $\Psi' \models M \bowtie N$.*

A.1 Soundness of the saturation procedure

Lemma 1 (soundness). *Let φ be an initial frame and (Φ,Ψ) be a state such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi,\Psi)$. Then, we have that*

1. *$M \rhd_\Phi t \;\Rightarrow\; M\varphi =_{\mathsf{E}} t$ for all $M \in \mathcal{F}_{\mathsf{pub}}[\mathrm{dom}(\varphi)]$ and $t \in \mathcal{F}[\emptyset]$;*
2. *$\Psi \models M \bowtie N \;\Rightarrow\; M\varphi =_{\mathsf{E}} N\varphi$ for all $M, N \in \mathcal{F}_{\mathsf{pub}}[\mathrm{dom}(\varphi) \cup \mathcal{X}]$.*

Proof. We prove this result by induction on the derivation $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi,\Psi)$.

Base case: We have that $(\Phi,\Psi) = \mathrm{Init}(\varphi)$ and we easily conclude.
Induction case: In such a case, we have $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi',\Psi') \Longrightarrow (\Phi,\Psi)$.
Let us first notice two facts.

1. Let M and t be such that $M \rhd_\Phi t$. By definition of $\rhd_\Phi$, there exist a public context C and some deduction facts $M'_1 \rhd t'_1, \ldots, M'_n \rhd t'_n \in \Phi$ such that $M = C[M'_1, \ldots M'_n]$ and $t = C[t'_1, \ldots, t'_n]$. In order to prove *1.*, it is sufficient to show that $M' \rhd^{\mathsf{E}}_\varphi t'$ for every $M' \rhd t' \in \Phi$. By induction hypothesis, this holds for the deduction facts in Φ', thus it remains to show that $M' \rhd^{\mathsf{E}}_\varphi t'$ for every fact $M' \rhd t' \in \Phi - \Phi'$.
2. Let M, N be two terms such that $\Psi \models M \bowtie N$. To establish *2.*, it is sufficient to prove that $M'\varphi =_{\mathsf{E}} N'\varphi$ for every $(\forall z_1, \ldots, z_q.M' \bowtie N')$ in Ψ. By induction hypothesis, this holds for the equations in Ψ', thus it remains to show that $M'\varphi =_{\mathsf{E}} N'\varphi$ for every equation $(\forall z_1, \ldots, z_q.M' \bowtie N')$ in $\Psi - \Psi'$.

Next we perform a case analysis on the inference rule used in $(\Phi',\Psi') \Longrightarrow (\Phi,\Psi)$. First, consider the case of rule **A**. Let $l \to r \in \mathcal{R}$ be the rewrite rule, D the decomposition, and $M_1 \rhd t_1, \ldots, M_{n+p} \rhd t_{n+p}$ the facts involved in this step.
*Rule **A.2***: We need to show that

- $D[M_1, \ldots, M_{n+p}, a, \ldots, a]\varphi =_{\mathsf{E}} (r\sigma){\downarrow_{\mathcal{R}}}$, and
- $D[M_1, \ldots, M_{n+p}, z_1, \ldots, z_q]\varphi =_{\mathsf{E}} D[M_1, \ldots, M_{n+p}, a, \ldots, a]\varphi$.

We note that $D[t_1, \ldots, t_{n+p}, z_1, \ldots, z_q] = l\sigma \to r\sigma \to^* (r\sigma){\downarrow_{\mathcal{R}}}$. Besides, by induction hypothesis we have that $M_i\varphi =_{\mathsf{E}} t_i$ for $1 \le i \le n+p$. Given that $(r\sigma){\downarrow_{\mathcal{R}}}$

is ground, and applying the substitution $\{z_1 \mapsto a, \ldots, z_q \mapsto a\}$ to the equation $D[t_1, \ldots, t_{n+p}, z_1, \ldots, z_q] =_{\mathsf{E}} (r\sigma){\downarrow_{\mathcal{R}}}$, we obtain:

$$\begin{aligned} D[M_1, \ldots, M_{n+p}, z_1, \ldots, z_q]\varphi &=_{\mathsf{E}} D[t_1, \ldots, t_{n+p}, z_1, \ldots, z_q] \\ &=_{\mathsf{E}} (r\sigma){\downarrow_{\mathcal{R}}} \\ &=_{\mathsf{E}} D[t_1, \ldots, t_{n+p}, a, \ldots, a] \\ &=_{\mathsf{E}} D[M_1, \ldots, M_{n+p}, a, \ldots, a]\varphi \end{aligned}$$

*Rule **A.1***: We need to show $D[M_1, \ldots, M_{n+p}, z_1, \ldots, z_q]\varphi =_{\mathsf{E}} M\varphi$. As before, we have $D[M_1, \ldots, M_{n+p}, z_1, \ldots, z_q]\varphi =_{\mathsf{E}} (r\sigma){\downarrow_{\mathcal{R}}}$. We also know that there exist M' and s such that $\Psi \models M \bowtie M'$, $M' \rhd_{\Phi^+} s$ and $r\sigma \rightarrow^*_{\mathcal{R}} s$ where $\Phi^+ = \Phi \cup \{z_1 \rhd z_1, \ldots, z_q \rhd z_q\}$. Let θ be the substitution $\{z_1 \mapsto a, \ldots, z_q \mapsto a\}$. We have $\Psi \models M\theta \bowtie M'\theta$ and $M'\theta \rhd_{\Phi} s$. Hence, using the induction hypothesis, we have that $M\theta\varphi =_{\mathsf{E}} M'\theta\varphi$ and $M'\theta\varphi =_{\mathsf{E}} s$ thus $M\varphi =_{\mathsf{E}} M'\varphi$ and $M'\varphi =_{\mathsf{E}} s$. Thus, we have that $M\varphi =_{\mathsf{E}} (r\sigma){\downarrow_{\mathcal{R}}}$. This allows us to conclude.

*Rule **A.3***: In such a case, the result trivially holds.

Second, we consider the case of **B** rules. Let $t = f(t_1, \ldots, t_n) \in \mathrm{st}(t_0)$, $f \in \mathcal{F}_{\mathsf{pub}}$ and $M_0 \rhd t_0, \ldots, M_n \rhd t_n \in \Phi$ be involved in the step $(\Phi', \Psi') \Longrightarrow (\Phi, \Psi)$.

*Rule **B.1***: By induction hypothesis, $M_i\varphi =_{\mathsf{E}} t_i$ for every $1 \leq i \leq n$, hence $f(M_1, \ldots, M_n)\varphi =_{\mathsf{E}} f(t_1, \ldots, t_n) = t$.

*Rule **B.2***: By induction hypothesis, $M_i\varphi =_{\mathsf{E}} t_i$ for every $1 \leq i \leq n$ and $M\varphi =_{\mathsf{E}} t$, hence $f(M_1, \ldots, M_n)\varphi =_{\mathsf{E}} f(t_1, \ldots, t_n) = t =_{\mathsf{E}} M\varphi$. □

A.2 Completeness of the saturation procedure

Lemma 6 (completeness, syntactic deduction). *Let (Φ, Ψ) be a state, $M_0 \rhd t_0 \in \Phi$. Let N, t be two terms such that $t \in \mathrm{st}(t_0)$ and $N \rhd_{\Phi} t$. Then there exists (Φ', Ψ') and N' such that*

- *$(\Phi, \Psi) \Longrightarrow^* (\Phi', \Psi')$ using **B** rules, and*
- *$N' \rhd t \in \Phi'$ and $\Psi' \models N \bowtie N'$.*

Proof. By hypothesis, we have that $N \rhd_{\Phi} t$. This means that there exists a public context C and some facts $M_1 \rhd t_1, \ldots, M_n \rhd t_n \in \Phi$ such that $N = C[M_1, \ldots, M_n]$ and $t = C[t_1, \ldots, t_n]$. Let C be such a context whose size is minimal. We show the result by structural induction on C.

Base case: C is reduced to an hole. Let $(\Phi', \Psi') = (\Phi, \Psi)$ and $N' = N$. The result trivially holds.

Induction step: $C = f(C_1, \ldots, C_r)$ with $f \in \mathcal{F}_{\mathsf{pub}}$ of arity r. In such a case, we have $t = f(u_1, \ldots, u_r)$ and $C_i[M_1, \ldots, M_n] \rhd_{\Phi} u_i$ with $u_i \in \mathrm{st}(t_0)$ for each $1 \leq i \leq r$. Thus, we can apply our induction hypothesis. We deduce that there exists (Φ_1, Ψ_1) and terms $N'_1, \ldots N'_r$ such that:

– $(\Phi, \Psi) \Longrightarrow^* (\Phi_1, \Psi_1)$ using **B** rules,
– $N'_i \rhd u_i \in \Phi_1$ and $\Psi_1 \models C_i[M_1, \ldots, M_n] \bowtie N'_i$ for each $1 \leq i \leq r$.

From this we easily deduce that $\Psi_1 \models N \bowtie f(N'_1, \ldots, N'_r)$. We apply one **B** rule. We have that $M_0 \rhd t_0, N'_1 \rhd u_1, \ldots, N'_r \rhd u_r \in \Phi_1$, $t = f(u_1, \ldots, u_r) \in \mathrm{st}(t_0)$ and $f \in \mathcal{F}_{\mathsf{pub}}$. We distinguish two cases:

*Rule **B.1***: Assume that for all M_t we have that $(M_t \rhd t) \notin \Phi_1$.

Let $\Phi' = \Phi_1 \cup \{f(N'_1, \ldots, N'_r) \rhd t\}$, $\Psi' = \Psi_1$ and $N' = f(N'_1, \ldots, N'_r)$. In order to conclude it remains to show that $\Psi' \models N \bowtie N'$. This is an easy consequence of the fact that $\Psi_1 \models N \bowtie f(N'_1, \ldots, N'_r)$.

*Rule **B.2***. Assume that there exists M_t such that $M_t \rhd t \in \Phi_1$.

Let $\Phi' = \Phi_1$, $\Psi' = \Psi_1 \cup \{f(N'_1, \ldots, N'_r) \bowtie M_t\}$ and $N' = M_t$. In order to conclude it remains to show that $\Psi' \models N \bowtie N'$. We have $\Psi' \models f(N'_1, \ldots, N'_r) \bowtie N'$ and $\Psi' \models N \bowtie f(N'_1, \ldots, N'_r)$. This allows us to conclude. □

Lemma 2 (completeness, syntactic equations). *Let (Φ, Ψ) be a state, and M, N be two terms such that $M \rhd_\Phi t$ and $N \rhd_\Phi t$ for some term t. Then there exists (Φ', Ψ') such that $(\Phi, \Psi) \Longrightarrow^* (\Phi', \Psi')$ using **B** rules and $\Psi' \models M \bowtie N$.*

Proof. By hypothesis, we have that $M \rhd_\Phi t$ and $N \rhd_\Phi t$ for some term t. By definition of $\rhd_\Phi$, we have that

– $M = C[M_1, \ldots, M_k]$, $N = C'[N_1, \ldots, N_\ell]$ for some contexts C, C',
– the facts $M_1 \rhd t_1, \ldots, M_k \rhd t_k$ and $N_1 \rhd u_1, \ldots, N_\ell \rhd u_\ell$ are in Φ,
– $C[t_1, \ldots, t_k] = C'[u_1, \ldots, u_\ell]$.

We prove the result by structural induction on C and C'. We assume w.l.o.g. that C is smaller than C' (in terms of number of symbols).

Base case: C is reduced to an hole. We have that $C[M_1, \ldots, M_k] = M_1$. By hypothesis, we have that $N \rhd_\Phi t = t_1$ and thus $t \in \mathrm{st}(t_1)$. Thanks to Lemma 6, there exists (Φ', Ψ') and N' such that $(\Phi, \Psi) \Longrightarrow^* (\Phi', \Psi')$ using a **B** rule, $N' \rhd t_1 \in \Phi'$ and $\Psi' \models N \bowtie N'$. Since $M_1 \rhd t_1$ and $N' \rhd t_1$ are both in Φ', we deduce that $N' = M_1$. Hence we have that $N' = M$ and thus we easily conclude.

Induction step: $C = f(C_1, \ldots, C_r)$ and $C' = f(C'_1, \ldots, C'_r)$ where $f \in \mathcal{F}_{\mathsf{pub}}$ is a symbol of arity r and $C_1, \ldots, C_r, C'_1, \ldots, C'_r$ are contexts. Moreover, we have that $C_i[t_1, \ldots, t_k] = C'_i[u_1, \ldots, u_\ell]$ for every $1 \leq i \leq r$, By applying the induction hypothesis, we deduce that there exists (Φ', Ψ') such that

– $(\Phi, \Psi) \Longrightarrow^* (\Phi', \Psi')$, and
– $\Psi' \models C_i[M_1, \ldots, M_k] \bowtie C'_i[N_1, \ldots, N_\ell]$ for every $1 \leq i \leq r$.

Hence, we have that $\Psi' \models M \bowtie N$. This allows us to conclude. □

The following lemma justifies the notion of decomposition (Definition 3) as far as completeness is concerned.

Lemma 7 (decomposition of a context reduction). *Let Φ be a frame, l a (plain) term, σ a substitution, and M a term such that $M \rhd_\Phi l\sigma$. Then there exist*

- *a (n,p,q)-decomposition D of l, written $l = D[l_1, \dots, l_n, y_1, \dots y_{p+q}]$,*
- *n deduction facts $M_1 \rhd t_1, \dots, M_n \rhd t_n$ in Φ,*
- *$p+q$ recipes $N_1, \dots, N_{p+q}$*

such that

- *for every $1 \le i \le n$, $t_i = l_i\sigma$ and*
- *for every $1 \le j \le p+q$, $N_j \rhd_\Phi y_j\sigma$.*

In particular, $D[M_1, \dots, M_n, N_1, \dots N_{p+q}] \rhd_\Phi l\sigma$.

Besides, if l is a left-hand side of rule in $\mathcal{R}$ and Φ is $\mathcal{R}$-reduced, D is a proper decomposition (i.e. $D \neq \mathsf{w}_1$).

Proof. Since $M \rhd_\Phi l\sigma$, by definition there exists C and $M_1^0 \rhd t_1^0, \dots, M_m^0 \rhd t_m^0$ in Φ such that $M = C[M_1^0, \dots, M_m^0]$ and $l\sigma = C[t_1^0, \dots, t_m^0]$.

Let $x_1, \dots, x_m$ be fresh variables. Given that $C[x_1, \dots, x_m]$ and l unify and have distinct variables, there exists a largest common context D_0 such that $l = D_0[l_1^0, \dots, l_a^0, y_1^0, \dots, y_b^0]$ and $C = D_0[\mathsf{w}_{j_1}, \dots, \mathsf{w}_{j_a}, D_1, \dots, D_b]$ where the terms l_i^0 are not variables and D_0 uses all his parameters: in particular $l\sigma = C[t_1^0, \dots, t_m^0]$ means that

- for every $1 \le k \le a$, $l_k^0\sigma = t_{j_k}^0$, and
- for every $1 \le k \le b$, $y_k^0\sigma = D_k[t_1^0, \dots, t_m^0]$

Let n be the cardinal of $\{l_1^0, \dots, l_a^0\}$. For each distinct l_i in $\{l_1^0, \dots, l_a^0\}$ ($1 \le i \le n$), we choose k in $\{1, \dots, a\}$ such that $l_i = l_k^0$ and define $M_i = M_k^0$ and $t_i = l_k^0\sigma = l_i\sigma$. Besides, for every k' such that $l_{k'}^0 = l_k^0$, we define $w_{k'} = \mathsf{w}_i$.

Let p be the cardinal of $\{y_1^0, \dots, y_b^0\} \cap \mathrm{var}(l_1, \dots, l_n)$. For each distinct y_j in $\{y_1^0, \dots, y_b^0\}$ ($1 \le j \le p$), we choose k in $\{1, \dots, b\}$ such that $y_j = y_k^0$ and define $N_j = D_k[M_1^0, \dots, M_m^0]$. Besides, for every k' such that $y_{k'}^0 = y_k^0$, we define $w_{a+k'} = \mathsf{w}_{p+j}$.

Let $q = b - p$. We repeat the same operation for each distinct y_j in $\{y_1^0, \dots, y_b^0\} - \mathrm{var}(l_1, \dots, l_n)$ ($p+1 \le j \le p+q$).

Finally, we let $D = D_0[w_1, \dots, w_{a+b}]$. By construction, we have that

- $l = D[l_1, \dots, l_n, y_1, \dots y_{p+q}]$,
- the l_i are mutually distinct non-variable terms and the y_i are mutually distinct variables.
- $y_i \in \mathrm{var}(l_1, \dots, l_n)$ iff $i \le p$.
- $M_i \rhd t_i$ is in Φ,
- for every $1 \le i \le n$, $t_i = l_i\sigma$, and
- for every $1 \le j \le p+q$, $N_j \rhd_\Phi y_j\sigma$.

As for the last sentence, if D is a parameter, so is D_0. As $l = y_k^0$ is impossible for a convergent system $\mathcal{R}$, we have $D_0 = \mathsf{w}_k$ with $k \le a$. Hence $C = \mathsf{w}_{j_k}$ and $t_k^0 = C[t_1^0, \dots, t_k^0] = l\sigma$ is not $\mathcal{R}$-reduced. $\square$

Lemma 3 (completeness, context reduction). *Let (Φ,Ψ) be a state and M, t, t' be three terms such that $M \rhd_\Phi t$ and $t \to_\mathcal{R} t'$. Then, either $(\Phi,\Psi) \Longrightarrow^* \bot$ or there exist (Φ',Ψ'), M' and t'' such that $(\Phi,\Psi) \Longrightarrow^* (\Phi',\Psi')$, $M' \rhd_{\Phi'} t''$ with $t' \to_\mathcal{R}^* t''$, and $\Psi' \models M \bowtie M'$.*

Besides, in both cases, the corresponding derivation from (Φ,Ψ) can be chosen to consist of a number of ***B*** *rules, possibly followed by one instance of* ***A*** *rule involving the same rewrite rule $l \to r$ as the rewrite step $t \to_\mathcal{R} t'$.*

Proof. By hypothesis, there exist a (public) context C and some deduction facts $M_1^0 \rhd t_1^0, \ldots, M_{m_0}^0 \rhd t_{m_0}^0 \in \Phi$ such that $M = C[M_1^0,\ldots,M_{m_0}^0]$ and $t = C[t_1^0,\ldots,t_{m_0}^0]$.

Moreover, there exist a position α, a substitution σ and a rewrite rule $l \to r \in \mathcal{R}$ such that $t|_\alpha = l\sigma$ and $t' = t[r\sigma]_\alpha$.

We note that α must be a (symbol) position of C since the t_i^0 are $\mathcal{R}$-reduced. Hence we may write $C|_\alpha[t_1^0,\ldots,t_{m_0}^0] = l\sigma$.

By Lemma 7, we deduce that there exist

- a proper (n,p,q)-decomposition D of $l : l = D[l_1,\ldots,l_n,y_1,\ldots y_p,z_1,\ldots z_q]$,
- $M_1 \rhd t_1, \ldots, M_n \rhd t_n$ in Φ,
- $N_1, \ldots, N_{p+q}$

such that

- for every $1 \le i \le n$, $t_i = l_i\sigma$,
- for every $1 \le j \le p$, $N_j \rhd_\Phi y_j\sigma$, and
- for every $1 \le k \le q$, $N_{p+k} \rhd_\Phi z_k\sigma$.

In particular, we obtain that

$$M|_\alpha = C|_\alpha[M_1^0,\ldots,M_{m_0}^0] \rhd_\Phi C|_\alpha[t_1^0,\ldots,t_{m_0}^0] = l\sigma$$
$$D[M_1,\ldots,M_n,N_1,\ldots,N_{p+q}] \rhd_\Phi D[t_1,\ldots,t_n,y_1\sigma,\ldots,y_p\sigma,z_1\sigma,\ldots,z_q\sigma] = l\sigma$$

Thus, by Lemma 2, there exists a derivation $(\Phi,\Psi) \Longrightarrow^* (\Phi_1,\Psi_1)$ using **B** rules such that $\Psi_1 \models M|_\alpha \bowtie D[M_1,\ldots,M_n,N_1,\ldots,N_{p+q}]$.

Besides, since y_j belongs to $\mathrm{var}(l_1,\ldots,l_n)$ by definition of decompositions, $y_j\sigma$ is a subterm of some $l_i\sigma = t_i$. Since $N_j \rhd_\Phi y_j\sigma$, by applying Lemma 6 repeatedly, we deduce that there exist some term $M_{n+1}, \ldots, M_{n+p}$ and a derivation $(\Phi_1,\Psi_1) \Longrightarrow^* (\Phi_2,\Psi_2)$ using **B** rules such that for all j,

- $M_{n+j} \rhd y_j\sigma$ is in Φ_2, and
- $\Psi_2 \models M_{n+j} \bowtie N_j$.

Let $N = D[M_1,\ldots,M_{n+p},N_{p+1},\ldots,N_{p+q}]$. We deduce that $N \rhd_{\Phi_2} l\sigma$, and

$$\Psi_2 \models M|_\alpha \bowtie D[M_1,\ldots,M_n,N_1,\ldots,N_{p+q}] \bowtie N$$

We now consider the application to (Φ_2,Ψ_2) of a **A** rule that involves the rewrite rule $l \to r$, the decomposition D, the plain terms $(t_1,\ldots,t_{n+p}) =$

$(l_1,\ldots,l_n,y_1,\ldots,y_p)\sigma$ and the substitution $\sigma' = \sigma|_V$ obtained by restricted the σ to the domain $V = \mathrm{var}(l_1,\ldots,l_n) = \mathrm{var}(l_1,\ldots,l_n,y_1,\ldots,y_p)$.

Case **A.3**. If $(r\sigma')\downarrow_{\mathcal{R}}$ is not ground and $\mathrm{Ctx}(\Phi_2^+ \vdash_{\mathcal{R}}^? r\sigma', \Psi_2, (l,r,D,\sigma')) = \bot$ where $\Phi_2^+ = \Phi_2 \cup \{z_1 \rhd z_1,\ldots,z_q \rhd z_q\}$, then we may conclude that $(\Phi_2,\Psi_2) \Longrightarrow \bot$ by an instance of rule **A.3** involving $l \to r$, the decomposition D and the facts $M_1 \rhd t_1,\ldots,M_{n+p} \rhd t_{n+p}$.

Case **A.1**. If there exists $N_0 = \mathrm{Ctx}(\Phi_2^+ \vdash_{\mathcal{R}}^? r\sigma', \Psi_2, (l,r,D,\sigma'))$ where $\Phi_2^+ = \Phi_2 \cup \{z_1 \rhd z_1,\ldots,z_q \rhd z_q\}$. Let N_0' and s_0 be such that $\Psi_2 \models N_0 \bowtie N_0'$, $N_0' \rhd_{\Phi_2 \cup \{z_1,\ldots,z_q\}} s_0$ and $r\sigma' \to_{\mathcal{R}}^* s_0$, and define

- $\Phi' = \Phi_2$,
- $\Psi' = \Psi_2 \cup \{\forall z_1,\ldots,z_q.D[M_1,\ldots,M_{n+p},z_1,\ldots,z_q] \bowtie N_0\}$,
- $M' = M[M_0]_\alpha$ where $M_0 = N_0'\ \{z_i \mapsto N_{p+i}\}_{1\le i\le q}$,
- $t'' = t[t_0]_\alpha = t'[t_0]_\alpha$ where $t_0 = s_0\ \{z_i \mapsto z_i\sigma\}_{1\le i\le q}$.

By construction, we have $(\Phi_2,\Psi_2) \Longrightarrow (\Phi',\Psi')$ by an instance of rule **A.1**.

Besides, $r\sigma' \to_{\mathcal{R}}^* s_0$ implies $t'|_\alpha = r\sigma \to_{\mathcal{R}}^* t_0$ and $t' \to_{\mathcal{R}}^* t''$.

Given that $\alpha \in \mathrm{pos}(C)$ (where C is the previously context related to $M \rhd_\Phi t$) and $M_0 \rhd_{\Phi'} t_0$, we have that $M' = M[M_0]_\alpha \rhd_{\Phi'} t[t_0]_\alpha = t''$.

It remains to show that $\Psi' \models M \bowtie M'$. Indeed, we have seen that $\Psi_2 \models M|_\alpha \bowtie N$ where $N = D[M_1,\ldots,M_{n+p},z_1,\ldots,z_q]\{z_i \mapsto N_{p+i}\}_{1\le i\le q}$. Besides, we have $\Psi_2 \models N_0 \bowtie N_0'$, and by definition of Ψ', it holds that $\Psi' \supseteq \Psi_2$ and $\Psi' \models D[M_1,\ldots,M_{n+p},z_1,\ldots,z_q] \bowtie N_0$. Therefore, $\Psi' \models M|_\alpha \bowtie M_0$ and $\Psi' \models M \bowtie M[M_0]_\alpha = M'$.

Case **A.2**: if $(r\sigma')\downarrow_{\mathcal{R}}$ is ground and $\mathrm{Ctx}(\Phi_2^+ \vdash_{\mathcal{R}}^? r\sigma', \Psi_2, (l,r,D,\sigma')) = \bot$ where $\Phi_2^+ = \Phi_2 \cup \{z_1 \rhd z_1,\ldots,z_q \rhd z_q\}$, define

- $M_0 = D[M_1,\ldots,M_{n+p},\mathsf{a},\ldots,\mathsf{a}]$ and $t_0 = (r\sigma')\downarrow_{\mathcal{R}}$,
- $\Phi' = \Phi_2 \cup \{M_0 \rhd t_0\}$,
- $\Psi' = \Psi_2 \cup \{\forall z_1,\ldots,z_q.D[M_1,\ldots,M_{n+p},z_1,\ldots,z_q] \bowtie M_0\}$,
- $M' = M[M_0]_\alpha$, and
- $t'' = t[t_0]_\alpha$.

where a is the fixed public constant of rule **A.2**.

By construction, $(\Phi,\Psi) \Longrightarrow (\Phi',\Psi')$ by an instance of the **A.2** rule.

Since t_0 is ground and $\sigma = \sigma'\sigma$, we have $t_0 = (r\sigma)\downarrow_{\mathcal{R}}$. Therefore $t' = t[r\sigma]_\alpha \to_{\mathcal{R}}^* t[\,(r\sigma)\downarrow_{\mathcal{R}}\,]_\alpha = t''$.

Given that $\alpha \in \mathrm{pos}(C)$ and by construction $M_0 \rhd_{\Phi'} t_0$, we have $M' \rhd_{\Phi'} t''$.

It remains to show that $\Psi' \models M \bowtie M'$. Indeed, we have seen that $\Psi_2 \models M|_\alpha \bowtie N$ where $N = D[M_1,\ldots,M_{n+p},z_1,\ldots,z_q]\{z_i \mapsto N_{p+i}\}_{1\le i\le q}$. By definition of Ψ', it holds that $\Psi' \models N \bowtie M_0$ hence $\Psi' \models M \bowtie M[N]_\alpha \bowtie M[M_0]_\alpha = M'$.

The additional properties claimed on the derivation are clear from the construction above. $\square$

A.3 Proof of Theorem 1

Theorem 1 (soundness and completeness). *Let* E *be an equational theory generated by a convergent rewrite system* $\mathcal{R}$. *Let* φ *be an initial frame and* (Φ, Ψ) *be a saturated state such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi, \Psi)$.

1. *For all* $M \in \mathcal{F}_{\mathsf{pub}}[\mathrm{par}(\varphi)]$ *and* $t \in \mathcal{F}[\emptyset]$, *we have*
$$M\varphi =_{\mathsf{E}} t \quad \Leftrightarrow \quad \exists N,\ \Psi \models M \bowtie N \text{ and } N \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$$
2. *For all* M, $N \in \mathcal{F}_{\mathsf{pub}}[\mathrm{par}(\varphi) \cup \mathcal{X}]$, *we have that* $M\varphi =_{\mathsf{E}} N\varphi \Leftrightarrow \Psi \models M \bowtie N$.

Proof. Let φ be an initial frame and (Φ, Ψ) be a saturated state such that $\mathrm{Init}(\varphi) \Rightarrow^* (\Phi, \Psi)$.

1.($\Leftarrow$) Let M, N and t be such that $\Psi \models M \bowtie N$ and $N \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$ (thus in particular $N \rhd^{\mathsf{E}}_{\Phi} t$). Thanks to Lemma 1, we have that $M\varphi =_{\mathsf{E}} N\varphi =_{\mathsf{E}} t$.

($\Rightarrow$) Let M and t be such that $M\varphi =_{\mathsf{E}} t$. We have that $M \rhd_{\Phi} t_0 \to^* t{\downarrow_{\mathcal{R}}}$ for some term t_0. We show the result by induction on t_0 equipped with the order $<$ induced by the rewriting relation ($t < t'$ if and only if $t' \to^+ t$).
Base case: $M \rhd_{\Phi} t_0 = t{\downarrow_{\mathcal{R}}}$. Let $N = M$, we have $\Psi \models M \bowtie N$ and $N \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$.
Induction case: $M \rhd_{\Phi} t_0 \to^+ t{\downarrow_{\mathcal{R}}}$. Let t' be such that $M \rhd_{\Phi} t_0 \to t' \to^* t{\downarrow_{\mathcal{R}}}$. Thanks to Lemma 3 and since (Φ, Ψ) is already saturated,[5] we deduce that there exist N' and t'' such that $N' \rhd_{\Phi} t''$, $t' \to^* t''$, and $\Psi \models M \bowtie N'$. We have that $N' \rhd_{\Phi} t'' \to^* t{\downarrow_{\mathcal{R}}}$ and $t'' \leq t' < t_0$. Thus, we can apply our induction hypothesis and we obtain that there exists N such that $\Psi \models N' \bowtie N$ and $N \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$.

2.($\Leftarrow$) By Lemma 1, $\Psi \models M \bowtie N$ implies $M\varphi =_{\mathsf{E}} N\varphi$.

($\Rightarrow$) Let M and N such that $M\varphi =_{\mathsf{E}} N\varphi$. This means that there exists t such that $M\varphi =_{\mathsf{E}} t$ and $N\varphi =_{\mathsf{E}} t$. By applying 1, we deduce that there exists M', N' such that: $\psi \models M \bowtie M'$, $M' \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$, $\psi \models N \bowtie N'$ and $N' \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$. Thanks to Lemma 2 and since (Φ, Ψ) is already saturated, we easily deduce that $\Psi \models M' \bowtie N'$, and thus $\Psi \models M \bowtie N$. ☐

A.4 Application to deduction and static equivalence

Algorithm for deduction. Let φ be an initial frame and t be a ground term. The procedure for checking $\varphi \vdash_{\mathsf{E}} t$ runs as follows:

1. Apply the transformation rules to obtain (if any) a saturated state (Φ, Ψ) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi, \Psi)$;
2. Return *yes* if there exists N such that $N \rhd_{\Phi} t{\downarrow_{\mathcal{R}}}$ (that is, the $\mathcal{R}$-reduced form of t is syntactically deducible from Φ); otherwise return *no*.

[5] Note that rule **A.3** is never applicable on a saturated state.

Proof. If the algorithm returns *yes*, this means that there exists N such that $N \rhd_\Phi t{\downarrow_\mathcal{R}}$. Thanks to Theorem 1, we have that $N\varphi =_\mathsf{E} t$, i.e. $N \rhd_\varphi^\mathsf{E} t$.

Conversely, if t is deducible from φ, then there exists M such that $M\varphi =_\mathsf{E} t$. By Theorem 1, there exists N such that $N \rhd_\Phi t{\downarrow_\mathcal{R}}$. The algorithm returns *yes*. □

Algorithm for static equivalence. Let φ_1 and φ_2 be two initial frames. The procedure for checking $\varphi_1 \approx_\mathsf{E} \varphi_2$ runs as follows:

1. Apply the transformation rules to obtain (if possible) two saturated states (Φ_1, Ψ_1) and (Φ_2, Ψ_2) such that $\mathrm{Init}(\varphi_i) \Longrightarrow^* (\Phi_i, \Psi_i)$, $i = 1, 2$;
2. For $\{i, j\} = \{1, 2\}$, for every equation $(\forall z_1, \ldots, z_\ell . M \bowtie N)$ in Ψ_i, check that $M\varphi_j =_\mathsf{E} N\varphi_j$ — that is, in other words, $(M\varphi_j){\downarrow_\mathcal{R}} = (N\varphi_j){\downarrow_\mathcal{R}}$;
3. If so return *yes*; otherwise return *no*.

Proof. If the algorithm returns *yes*, this means that:

For every equation $(\forall z_1, \ldots, z_\ell . M \bowtie N)$ in Ψ_1, we have that $M\varphi_2 =_\mathsf{E} N\varphi_2$.

Let $M \bowtie N \in \mathrm{eq}_\mathsf{E}(\varphi_1)$. By definition of $\mathrm{eq}_\mathsf{E}(\varphi_1)$, we have that $M\varphi_1 =_\mathsf{E} N\varphi_1$. Thanks to Theorem 1, we have that $\Psi_1 \models M \bowtie N$. As all the equations in Ψ_1 are satisfied by φ_2 modulo E, we deduce that $M\varphi_2 =_\mathsf{E} N\varphi_2$, i.e. $M \bowtie N \in \mathrm{eq}(\varphi_2)$. The other inclusion, $\mathrm{eq}_\mathsf{E}(\varphi_2) \subseteq \mathrm{eq}_\mathsf{E}(\varphi_1)$, is proved in the same way.

Conversely, assume now that $\varphi_1 \approx_\mathsf{E} \varphi_2$, i.e. $\mathrm{eq}_\mathsf{E}(\varphi_1) = \mathrm{eq}_\mathsf{E}(\varphi_2)$. Consider a quantified equation $\forall z_1, \ldots, z_\ell . M \bowtie N$ in Ψ_1 and let us show that $M\varphi_2 =_\mathsf{E} N\varphi_2$. (The other case is done in a similar way, and we will conclude that the algorithm returns *yes*.)

Let $\mathsf{c}_1, \ldots, \mathsf{c}_\ell$ be free public constants not occurring in M and N, and let $(M', N') = (M, N)\{z_1 \mapsto \mathsf{c}_1, \ldots, z_\ell \mapsto \mathsf{c}_\ell\}$. Since $\Psi_1 \models M' \bowtie N'$, by Theorem 1, we have that $M'\varphi_1 =_\mathsf{E} N'\varphi_1$. Besides, M' and N' are ground and $\mathrm{par}(M', N') \subseteq \mathrm{par}(\Psi_1) \subseteq \mathrm{par}(\varphi_1)$. Thus, $(M' \bowtie N') \in \mathrm{eq}_\mathsf{E}(\varphi_1) \subseteq \mathrm{eq}_\mathsf{E}(\varphi_2)$ and $M'\varphi_2 =_\mathsf{E} N'\varphi_2$. As the constants $\mathsf{c}_1, \ldots, \mathsf{c}_\ell$ are free in E and do not occur in M and N, by replacement, we obtain that $M\varphi_2 =_\mathsf{E} N\varphi_2$. □

B Termination and non-Failure

B.1 Syntactic criterion

Proposition 1. *Assume that the function* Ctx *in use is* maximal*: for every ϕ and t, if there exists s such that $\phi \vdash s$ and $t \to_\mathcal{R}^* s$, then for any Ψ, α, $\mathrm{Ctx}(\phi \vdash_\mathcal{R}^? t, \Psi, \alpha) \neq \perp$. Then, provided that $\mathcal{R}$ is layered convergent, there exists no state (Φ, Ψ) from which $(\Phi, \Psi) \Longrightarrow \perp$ is the only applicable derivation.*

Proof. By contradiction, let (Φ, Ψ) be a state from which $(\Phi, \Psi) \Longrightarrow \perp$ is the only applicable derivation, and let $l \to r$ be the rewrite rule involved in the corresponding instance of rule **A.3**. We prove the property by induction on the index $i \in \{0 \dots N\}$ such that $l \to r \in \mathcal{R}_{i+1} - \mathcal{R}_i$. Using the notations of Figure 1 for the instance of **A.3** under consideration and the assumption on Ctx, we have that

(a) for every $r\sigma \to_{\mathcal{R}}^* s$, $\Phi \cup \{z_1 \rhd z_1, \dots, z_q \rhd z_q\} \nvdash s$, and
(b) $(r\sigma)\downarrow_{\mathcal{R}}$ is not ground.

In particular, (b) implies that $\mathrm{var}(r)$ is not included in $\mathrm{var}(l_1, \dots, l_n)$, otherwise we would have

$$\begin{aligned}\mathrm{var}((r\sigma)\downarrow_{\mathcal{R}}) \subseteq \mathrm{var}(r\sigma) \subseteq \mathrm{var}(\mathrm{var}(r)\sigma)\\ \subseteq \mathrm{var}(\mathrm{var}(l_1, \dots, l_n)\sigma) \subseteq \mathrm{var}(t_1, \dots, t_n) = \emptyset\end{aligned}$$

By assumption on the decomposition $l = D[l_1, \dots, l_n, y_1, \dots, y_p, z_1, \dots, z_q]$ of $l \to r \in \mathcal{R}_{i+1} - \mathcal{R}_i$, we deduce that there exists some contexts $C_0, \dots, C_k$ and some terms $s_1, \dots, s_k$ such that

- $r = C_0[s_1, \dots, s_k]$;
- for each $1 \leq i \leq k$, $C_i[l_1, \dots, l_n, y_1, \dots, y_p, z_1, \dots, z_q]$ rewrites to s_i in zero or one step of rewrite rule in head position along $\mathcal{R}_i$.

Let $C = C_0[C_1, \dots, C_k]$ and $t_0 = C[l_1, \dots, l_n, y_1, \dots, y_p, z_1, \dots, z_q]$. Note that $t_0 \to_{\mathcal{R}_i}^* r$.

If $t_0 = r$, we obtain that $r\sigma = C[t_1, \dots, t_{n+p}, z_1, \dots, z_q]$ is syntactically deducible from $\Phi \cup \{z_1 \rhd z_1, \dots, z_q \rhd z_q\}$, which contradicts (a). Hence $t_0 \to_{\mathcal{R}_i}^+ r$, and in particular $i > 0$.

Let μ be a substitution mapping the variable z_j to distinct fresh public constants a_j. For each $1 \leq i \leq k$, let $u_i = C_i[l_1, \dots, l_n, y_1, \dots, y_p, z_1, \dots, z_q]\sigma\mu$. The term $u_i = C_i[t_1, \dots, t_{n+p}, a_1, \dots, a_q]$ is syntactically deducible from Φ, and reduces to $u_i' = s_i\sigma\mu$ in zero or one step (in head position) along $\mathcal{R}_i$.

By induction hypothesis on $i - 1$, no applicable rule **A.3** from (Φ, Ψ) may involve a rule in $\mathcal{R}_i$. Besides, by assumption, (Φ, Ψ) is saturated for the rules **B.1**, **B.2**, **A.1** and **A.2**.

Therefore, Lemma 3 applied to $\Phi \vdash u_i$ and $u_i \to_{\mathcal{R}_i} u_i'$ implies that there exists u_i'' such that $u_i' \to_{\mathcal{R}}^* u_i''$ and $\Phi \vdash u_i''$. The same conclusion trivially holds if $u_i' = u_i$. Let $s = C_0[u_1'', \dots, u_k'']\mu^{-1}$ be the term obtained by replacing each a_i by z_i in $C[u_1'', \dots, u_k'']$. Since the a_i do not occur in $\mathcal{R}$ nor in Φ, we deduce that s satisfies $r\sigma = C_0[s_1\sigma, \dots, s_k\sigma] = C_0[u_1', \dots, u_k']\mu^{-1} \to_{\mathcal{R}}^* s$ and $\Phi \cup \{z_1 \rhd z_1, \dots, z_q \rhd z_q\} \vdash s$, in contradiction with the condition (a) stated at the beginning of the proof. □

B.2 Termination

Proving termination of the prefix theory $\mathsf{E}_{\mathsf{pref}}$. For proving termination for the prefix theory $\mathsf{E}_{\mathsf{pref}}$, it suffices to consider $s(\phi) = \mathrm{st}_{\mathsf{ext}}(\Phi)$, where the notion of extended subterm is recursively defined as follows:

– $\mathrm{st}_{\mathsf{ext}}(a) = \{a\}$ if a is a constant or a variable
– $\mathrm{st}_{\mathsf{ext}}(f(t_1, \ldots, t_n)) = \{f(t_1, \ldots, t_n)\} \cup \bigcup_{i=1}^{n} \mathrm{st}_{\mathsf{ext}}(t_i)$ $f \in \{\mathsf{dec}, \langle,\rangle, \pi_1, \pi_2, \mathsf{pref}\}$
– $\mathrm{st}_{\mathsf{ext}}(\mathsf{enc}(t, u)) = \{\mathsf{enc}(t, u), \mathsf{enc}(t_1, u)\} \cup \mathrm{st}_{\mathsf{ext}}(t) \cup \mathrm{st}_{\mathsf{ext}}(u)$ if $t = \langle t_1, t_2\rangle$
– $\mathrm{st}_{\mathsf{ext}}(\mathsf{enc}(t, u)) = \{\mathsf{enc}(t, u)\} \cup \mathrm{st}_{\mathsf{ext}}(t) \cup \mathrm{st}_{\mathsf{ext}}(u)$ otherwise.

Lemma 4. *Let $S_0 = (\Phi_0, \Psi_0) \Longrightarrow \ldots \Longrightarrow (\Phi_n, \Psi_n) \Longrightarrow \ldots$ be an infinite fair derivation from a state S_0. For every ground term t such that $\Phi_0 \vdash_{\mathsf{E}} t$, either $(\Phi_0, \Psi_0) \Longrightarrow^* \bot$ or there exists i such that $\Phi_i \vdash t\!\downarrow_{\mathcal{R}}$.*

Proof. Let t be a ground term in normal form deducible from Φ_0. There exist $M_1 \rhd t_1, \ldots, M_n \rhd t_n \in \Phi_0$, there exists a context C such that $C[t_1, \ldots, t_n] \to^* t$. We show that either $(\Phi_0, \Psi_0) \Longrightarrow^* \bot$ or there exists i such that t is syntactically deducible from Φ_i, by induction on $C[t_1, \ldots, t_n]$ equipped with the order $<$ induced by the rewriting relation (that is $t_1 < t_2$ if and only if $t_2 \to^+ t_1$).

The base case $t = C[t_1, \ldots, t_n]$ is obvious. Let now $v = C[t_1, \ldots, t_n]$ and assume $v \to v' \to^* t$. Since **B** rules are applied in priority, we choose the smallest i_1 such that no more **B** rules can be applied from (Φ_{i_1}, Ψ_{i_1}). Note indeed that there is no infinite derivation with only **B** rules (Proposition 2). We have $C[M_1, \ldots, M_n] \rhd_{\Phi_{i_1}} v \to v'$. Applying Lemma 3 and observing that no **B** rule can be applied from (Φ_{i_1}, Ψ_{i_1}), we deduce either $(\Phi_{i_1}, \Psi_{i_1}) \Longrightarrow^* \bot$ or there exist (Φ', Ψ'), M' and v'' such that

– $(\Phi_{i_1}, \Psi_{i_1}) \Longrightarrow (\Phi', \Psi')$ using a **A** rule
– $M' \rhd_{\Phi'} v''$ with $v' \to^+ v''$.

Since $(\Phi_{i_1}, \Psi_{i_1}) \Longrightarrow (\Phi', \Psi')$ using a **A** rule, there exist a rewrite rule $l \to r$, a decomposition D and terms $u_1, \ldots, u_n \in \mathrm{im}(\Phi_{i_1})$ such that $u \in \mathrm{im}(\Phi')$ where $u = (D[u_1, \ldots, u_n, z_1, \ldots, z_p])\downarrow$. Moreover, since $M' \rhd_{\Phi'} v''$, there exists a context C such that $v'' = C[v_1, \ldots, v_k]$, $v_i \in \mathrm{im}(\Phi')$. Note that we have

$$\{t \mid M \rhd t \in \Phi'\} = \{t \mid M \rhd t \in \Phi_{i_1}\} \cup \{u\}$$

By fairness, we know that a **A** rule will be applied for the same rewrite rule $l \to r$, decomposition D and terms $u_1, \ldots, u_n$ along the derivation. We deduce that there exists i_2 such that $u \in \mathrm{im}(\Phi_{i_2})$. Since no deduction facts are removed, we have

$$\{t \mid M \rhd t \in \Phi_{i_1}\} \subseteq \{t \mid M \rhd t \in \Phi_{i_2}\}$$

thus we deduce

$$\{t \mid M \rhd t \in \Phi'\} \subseteq \{t \mid M \rhd t \in \Phi_{i_2}\}$$

and thus $v'' = C[v_1, \ldots, v_k]$, $v_i \in \mathrm{im}(\Phi_{i_2})$. Since $v'' \to^* t$ and $v'' < v$, we deduce by induction that either $(\Phi_0, \Psi_0) \Longrightarrow^* \bot$ or there exists i such that t is syntactically deducible from Φ_i. $\square$

Proposition 4 (criterion for saturation). *Let φ be an initial frame such that* $\mathrm{Init}(\varphi) \not\Longrightarrow^* \bot$. *The following conditions are equivalent:*

(i) *There exists a saturated couple (Φ, Ψ) such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\Phi, \Psi)$.
(ii) *There exists a (finite) initial frame φ_s such that for every term t, t is deducible from φ modulo E iff $t\!\downarrow_{\mathcal{R}}$ is syntactically deducible from φ_s.*
(iii) *There exists no fair infinite derivation starting from* $\mathrm{Init}(\varphi)$.

Proof. $(iii) \Rightarrow (i)$: trivial. Indeed by using a fair derivation we will eventually reach a weakly saturated state. $(i) \Rightarrow (ii)$: Let $\Phi = \{M_1 \rhd s_1, \ldots, M_\ell \rhd s_\ell\}$ and $\varphi_s = \{\mathsf{w}_1 \rhd s_1, \ldots, \mathsf{w}_\ell \rhd s_\ell\}$. Let t be a ground term. By Theorem 1, we have that $\exists M \,.\, M \rhd^{\mathsf{E}}_{\varphi} t$ iff $\exists M \,.\, M \rhd_{\Phi} t\!\downarrow_{\mathcal{R}}$, i.e. $\exists M \,.\, M \rhd_{\varphi_s} t\!\downarrow_{\mathcal{R}}$. $(ii) \Rightarrow (iii)$: we need to prove that there exists no fair infinite derivation starting from $\mathrm{Init}(\varphi)$.

Let $\varphi_s = \{\mathsf{w}_1 \rhd s_1, \ldots, \mathsf{w}_\ell \rhd s_\ell\}$ an initial frame such that for every t, $\exists M \,.\, M \rhd^{\mathsf{E}}_{\varphi} t$ is equivalent to $\exists M \,.\, M \rhd_{\varphi_s} t\!\downarrow_{\mathcal{R}}$. Assume by contradiction that there is an infinite fair derivation $(\Phi_0, \Psi_0) \Longrightarrow \ldots \Longrightarrow (\Phi_n, \Psi_n) \Longrightarrow \ldots$ with $(\Phi_0, \Psi_0) = \mathrm{Init}(\varphi)$.

By Lemma 4 and since $\mathrm{Init}(\varphi) \not\Longrightarrow^* \bot$, we deduce that there exists i_0 such that each s_i, $1 \leq i \leq \ell$ is syntactically deducible from Φ_{i_0}. Since there is no infinite derivation with only **B** rules (Proposition 2), we can also assume that no **B** rule can be applied from Φ_{i_0}. We have that $\exists M \,.\, M \rhd^{\mathsf{E}}_{\varphi} t$ is now equivalent to $\exists M \,.\, M \rhd_{\Phi_{i_0}} t\!\downarrow_{\mathcal{R}}$ thus the **A.2** rule cannot be applied either. We deduce that no deduction facts are added to Φ_{i_0} along the derivation, that is $\Phi_j = \Phi_{i_0}$ for every $j \geq i_0$. Since no deduction fact are added, only a finite number of **A.1** rules can be applied, which contradicts the existence of an infinite chain. $\square$