Ştefan Ciobâcă, Stéphanie Delaune, and Steve Kremer

Computing knowledge in security protocols under convergent equational theories

Research Report LSV-09-05

March, 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

Computing knowledge in security protocols under convergent equational theories ⋆

Ştefan Ciobâcă, Stéphanie Delaune, and and Steve Kremer

LSV, ENS Cachan & CNRS & INRIA, France

Abstract. The analysis of security protocols requires reasoning about the knowledge an attacker acquires by eavesdropping on network traffic. In formal approaches, the messages exchanged over the network are modeled by a term algebra equipped with an equational theory axiomatizing the properties of the cryptographic primitives (e.g. encryption, signature). In this context, two classical notions of knowledge, deducibility and indistinguishability, yield corresponding decision problems.
We propose a procedure for both problems under arbitrary convergent equational theories. Since the underlying problems are undecidable we cannot guarantee termination. Nevertheless, our procedure terminates on a wide range of equational theories. In particular, we obtain a new decidability result for a theory we encountered when studying electronic voting protocols. We also provide a prototype implementation.

1 Introduction

Cryptographic protocols are small distributed programs that use cryptographic primitives such as encryption and digital signatures to communicate securely over a network. It is essential to gain as much confidence as possible in their correctness. Therefore, symbolic methods have been developed to analyse such protocols [4, 17, 19]. In these approaches, one of the most important aspects is to be able to reason about the *knowledge* of the attacker.

Traditionally, the knowledge of the attacker is expressed in terms of *deducibility* (e.g. [19, 10]). A message s (intuitively the secret) is said to be deducible from a set of messages φ, if an attacker is able to compute s from φ. To perform this computation, the attacker is allowed, for example, to decrypt deducible messages by deducible keys.

However, deducibility is not always sufficient. Consider for example the case where a protocol participant sends over the network the encryption of one of the constants "yes" or "no" (e.g. the value of a vote). Deducibility is not the right notion of knowledge in this case, since both possible values ("yes" and "no") are indeed "known" to the attacker. In this case, a more adequate form of knowledge is *indistinguishability* (e.g. [1]): is the attacker able to distinguish between two transcripts of the protocol, one running with the value "yes" and the other one running with the value "no"?

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

In symbolic approaches to cryptographic protocol analysis, the protocol messages and cryptographic primitives (e.g. encryption) are generally modeled using a term algebra. This term algebra is interpreted modulo an equational theory. Using equational theories provides a convenient and flexible framework for modeling cryptographic primitives [14]. For instance, a simple equational theory for symmetric encryption can be specified by the equation $dec(enc(x, y), y) = x$. This equation models the fact that decryption cancels out encryption when the same key is used. Different equational theories can also be used to model randomized encryption or even more complex primitives arising when studying electronic voting protocols [15, 5] or direct anonymous attestation [6]: blind signatures, trapdoor commitments, zero-knowledge proofs, ...

The two notions of knowledge that we consider do not take into account the dynamic behaviour of the protocol. Nevertheless, in order to establish that two dynamic behaviors of a protocol are indistinguishable, an important subproblem is to establish indistinguishability between the sequences of messages generated by the protocol [19, 2]. Indistinguishability, also called static equivalence in the applied-pi calculus framework [2], plays an important role in the study of guessing attacks (e.g. [12, 7]), as well as for anonymity properties in e-voting protocols (e.g. [15, 5]). This was actually the starting point of this work. During the study of e-voting protocols, we came across several equational theories for which we needed to show static equivalence while no decision procedure for deduction or static equivalence existed.

Our contributions. We provide a procedure which is correct, in the sense that if it terminates it gives the right answer, for any convergent equational theory. As deduction and static equivalence are undecidable for this class of equational theories [1], the procedure does not always terminate. However, we show that it does terminate for the class of *subterm convergent* equational theories (already shown decidable in [1]) and several other theories among which the theory of *trapdoor commitment* encountered in our electronic voting case studies [15].

Our second contribution is an efficient prototype implementation of this generic procedure. Our procedure relies on a simple fixed point computation based on a few saturation rules, making it convenient to implement.

Related work. Many decision procedures have been proposed for deducibility (e.g. [10, 3, 16]) under a variety of equational theories modeling encryption, digital signatures, exclusive OR, and homomorphic operators. Several papers are also devoted to the study of static equivalence. Most of these results introduce a new procedure for each particular theory and even in the case of the general decidability criterion given in [1, 13], the algorithm underlying the proof has to be adapted for each particular theory, depending on how the criterion is fulfilled.

The first generic algorithm that has been proposed handles subterm convergent equational theories [1] and covers the classical theories for encryption and signatures. This result is encompassed by the recent work of Baudet *et al.* [9] in which the authors propose a generic procedure that works for any convergent equational theory, but which may fail or not terminate. This procedure has been implemented in the YAPA tool [8] and has been shown to terminate without failure in several cases (e.g. subterm convergent theories and blind signatures). However, due to its simple representation of deducible terms (represented by a finite set of *ground* terms), the procedure fails on several interesting equational theories like the theory of trapdoor commitments. Our representation of deducible terms overcomes this limitation by including terms with variables which can be substituted by any deducible terms.

2 Formal model

2.1 Term algebras

As usual, messages will be modeled using a term algebra. Let $\mathcal{F}$ be a finite set of *function symbols* coming with an arity function $\mathrm{ar} : \mathcal{F} \to \mathbb{N}$. Function symbols of arity 0 are called *constants*. We consider several kind of *atoms* among which an infinite set of *names* $\mathcal{N}$, an infinite set of *variables* $\mathcal{X}$ and a set of parameters $\mathcal{P}$. The set of terms $\mathcal{T}(\mathcal{F}, \mathcal{A})$ built over $\mathcal{F}$ and the atoms in $\mathcal{A}$ is defined as

$$
\begin{array}{lll}
t, t_1, \ldots ::= & & \text{term} \\
\quad\quad\quad\quad \mid & a & \text{atom } a \in \mathcal{A} \\
\quad\quad\quad\quad \mid & f(t_1, \ldots, t_k) & \text{application of symbol } f \in \mathcal{F}, \mathrm{ar}(f) = k
\end{array}
$$

A term t is said to be *ground* when $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$. We assume the usual definitions to manipulate terms. We write $\mathrm{fn}(t)$ (resp. $\mathrm{var}(t)$) the set of (free) names (resp. variables) that occur in a term t and $\mathrm{st}(t)$ the set of its (syntactic) subterms. These notations are extended to tuples and sets of terms in the usual way. We denote by $|t|$ the *size* of t defined as the number of symbols that occur in t (variables do not count), and $\#T$ denotes the *cardinality* of the set T.

The set of positions of a term t is written $\mathrm{pos}(t) \subseteq \mathbb{N}^*$. If p is a position of t then $t|_p$ denotes the subterm of t at the position p. The term $t[u]_p$ is obtained from t by replacing the occurrence of $t|_p$ at position p with u. A *context* C is a term with (1 or more) holes and we write $C[t_1, \ldots t_n]$ for the term obtained by replacing these holes with the terms $t_1, \ldots, t_n$. A context is *public* if it only consists of function symbols and holes.

Substitutions are written $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ with $\mathrm{dom}(\sigma) = \{x_1, \ldots, x_n\}$. The application of a substitution σ to a term t is written $t\sigma$. The substitution σ is *grounding for t* if the resulting term $t\sigma$ is ground. We use the same notations for *replacements* of names and parameters by terms.

2.2 Equational theories and rewriting systems

Equality between terms will generally be interpreted modulo an *equational theory*. An equational theory $\mathcal{E}$ is defined by a set of equations $M \sim N$ with $M, N \in \mathcal{T}(\mathcal{F}, \mathcal{X})$. Equality modulo $\mathcal{E}$, written $=_\mathcal{E}$, is defined to be the smallest equivalence relation on terms such that $M =_\mathcal{E} N$ for all $M \sim N \in \mathcal{E}$ and which is closed under substitution of terms for variables and application of contexts.

It is often more convenient to manipulate rewriting systems than equational theories. A *rewriting system* $\mathcal{R}$ is a set of rewriting rules $l \to r$ where $l, r \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ and $\mathrm{var}(r) \subseteq \mathrm{var}(l)$. A term t rewrites to t' by $\mathcal{R}$, denoted by $t \to_{\mathcal{R}} t'$, if there exists $l \to r \in \mathcal{R}$, a position $p \in \mathrm{pos}(t)$ and a substitution σ such that $t|_p = l\sigma$ and $t' = t[r\sigma]_p$. We denote by $\to_{\mathcal{R}}^{+}$ the transitive closure of $\to_{\mathcal{R}}$, $\to_{\mathcal{R}}^{*}$ its reflexive and transitive closure, and $=_{\mathcal{R}}$ its reflexive, symmetric and transitive closure.

A rewrite system $\mathcal{R}$ is *convergent* if is *terminating*, i.e. there is no infinite chains $u_1 \to_{\mathcal{R}} u_2 \to_{\mathcal{R}} \ldots$, and *confluent*, i.e. for every terms u_1, u_2 such that $u_1 =_{\mathcal{R}} u_2$, there exists u such that $u_1 \to_{\mathcal{R}}^{*} u$ and $u_2 \to_{\mathcal{R}}^{*} u$. A term u is in $\mathcal{R}$-*normal form* if there is no term u' such that $u \to_{\mathcal{R}} u'$. If $u \to_{\mathcal{R}}^{*} u'$ and u' is in $\mathcal{R}$-normal form then u' is *a* $\mathcal{R}$-*normal form of* u. When this reduced form is unique (in particular if $\mathcal{R}$ is convergent), we write $u' = u{\downarrow_{\mathcal{R}_{\mathcal{E}}}}$.

We are particularly interested in theories $\mathcal{E}$ 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 $=_{\mathcal{E}}$ coincide. Given an equational theory $\mathcal{E}$ we define the corresponding rewriting system $\mathcal{R}_{\mathcal{E}}$ by orienting all equations in $\mathcal{E}$ from left to right, i.e., $\mathcal{R}_{\mathcal{E}} = \{l \to r \mid l \sim r \in \mathcal{E}\}$. We say that $\mathcal{E}$ is *convergent* if $\mathcal{R}_{\mathcal{E}}$ is convergent.

Example 1. A classical equational theory modelling symmetric encryption is $\mathcal{E}_{enc} = \{dec(enc(x, y), y) \sim x\}$. As a running example we consider a slight extension of this theory modelling *malleable* encryption

$$\mathcal{E}_{mal} = \mathcal{E}_{enc} \cup \{mal(enc(x, y), z) \sim enc(z, y)\}.$$

This malleable encryption scheme allows one to arbitrarily change the plaintext of an encryption. This theory does certainly not model a realistic encryption scheme but it yields a simple example of a theory which illustrates well our procedures. In particular all existing decision procedure we are aware of fail on this example. The rewriting system $\mathcal{R}_{\mathcal{E}_{mal}}$ is convergent.

From now on, we assume given a convergent equational theory $\mathcal{E}$ built over a signature $\mathcal{F}$ and represented by the convergent rewriting system $\mathcal{R}_{\mathcal{E}}$.

2.3 Deducibility and static equivalence

In order to describe the messages observed by an attacker, we consider the following notions of *frame* that comes from the applied-pi calculus [2].

A frame φ is a sequence of messages $u_1, \ldots, u_n$ meaning that the attacker observed each of these message in the given order. Furthermore, we distinguish the names that the attacker knows from those that were freshly generated by others and that are *a priori* unknown by the attacker. Formally, a frame is defined as $\nu\tilde{n}.\sigma$ where $\tilde{n}$ is its set of bound names, denoted by $\mathrm{bn}(\varphi)$, and a replacement $\sigma = \{w_1 \mapsto u_1, \ldots, w_n \mapsto u_n\}$. The parameters $w_1, \ldots, w_n$ enable us to refer to $u_1, \ldots, u_n \in \mathcal{T}(\mathcal{F}, \mathcal{N})$. The *domain* $\mathrm{dom}(\varphi)$ of φ is $\{w_1, \ldots, w_n\}$. Given terms M and N such that $\mathrm{fn}(M, N) \cap \tilde{n} = \emptyset$, we sometimes write $(M =_{\mathcal{E}} N)\varphi$ (resp. $M\varphi$) instead of $M\sigma =_{\mathcal{E}} N\sigma$ (resp. $M\sigma$).

Definition 1 (deducibility). *Let φ be a frame. A ground term t is* deducible *in $\mathcal{E}$ from φ, written $\varphi \vdash_{\mathcal{E}} t$, if there exists $M \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi))$, called the* recipe*, such that $\mathrm{fn}(M) \cap \mathrm{bn}(\varphi) = \emptyset$ and $M\varphi =_{\mathcal{E}} t$.*

Deducibility does not always suffice for expressing the knowledge of an attacker. For instance deducibility does not allow one to express indistinguishability between two sequences of messages. This is important when defining the confidentiality of a vote or anonymity-like properties. This motivates the following notion of static equivalence introduced in [2].

Definition 2 (static equivalence). *Let φ_1 and φ_2 be two frames such that $\mathrm{bn}(\varphi_1) = \mathrm{bn}(\varphi_2)$. They are* statically equivalent *in $\mathcal{E}$, written $\varphi_1 \approx_{\mathcal{E}} \varphi_2$, if*

- $\mathrm{dom}(\varphi_1) = \mathrm{dom}(\varphi_2)$
- *for all terms $M, N \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi_1))$ such that $\mathrm{fn}(M, N) \cap \mathrm{bn}(\varphi_1) = \emptyset$*
$$(M =_{\mathcal{E}} N)\varphi_1 \;\Leftrightarrow\; (M =_{\mathcal{E}} N)\varphi_2.$$

Example 2. Consider the two frames described below:

$$\varphi_1 = \nu a, k.\{w_1 \mapsto enc(a, k)\} \quad \text{and} \quad \varphi_2 = \nu a, k.\{w_1 \mapsto enc(b, k)\}.$$

We have that b and $enc(c, k)$ are deducible from φ_2 in $\mathcal{E}_{mal}$ with recipes b and $mal(w_1, c)$ respectively. We have that $\varphi_1 \not\approx_{\mathcal{E}_{mal}} \varphi_2$ since $(w_1 \neq_{\mathcal{E}_{mal}} mal(w_1, b))\varphi_1$ while $(w_1 =_{\mathcal{E}_{mal}} mal(w_1, b))\varphi_2$. Note that $\varphi_1 \approx_{\mathcal{E}_{enc}} \varphi_2$ (in the theory $\mathcal{E}_{enc}$).

3 Procedures for deduction and static equivalence

In this section we describe our procedures for checking deducibility and static equivalence on convergent equational theories. After some preliminary definitions, we present the main part of our procedure, i.e. a set of saturation rules used to reach a fixed point. Then, we show how to use this saturation procedure to decide deducibility and static equivalence. Soundness and completeness of the saturation procedure are stated in Theorem 1 and detailed in Section 4.

Since both problems are undecidable for arbitrary convergent equational theories [1], our saturation procedure does not always terminate. In Section 5, we exhibit (classes of) equational theories for which the saturation terminates.

3.1 Preliminary definitions

The main objects that will be manipulated by our procedure are *facts*, which are either *deduction facts* or *equational facts*.

Definition 3 (facts). *A* deduction fact *(resp. an* equational fact*) is an expression denoted $[U \rhd u \mid \Delta]$ (resp. $[U \sim V | \Delta]$) where Δ is a finite set of the form $\{X_1 \rhd t_1, \ldots, X_n \rhd t_n\}$ that contains the* side conditions *of the fact. Moreover, we assume that:*

- *$u, t_1, \ldots, t_n \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathcal{X})$ with $\mathrm{var}(u) \subseteq \mathrm{var}(t_1, \ldots, t_n)$;*

– $U, V \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathcal{X} \cup \mathcal{P})$ *and* $X_1, \ldots, X_n$ *are distinct variables;*
– $\mathrm{var}(U, V, X_1, \ldots, X_n) \cap \mathrm{var}(u, t_1, \ldots, t_n) = \emptyset$.

A fact is solved *if* $t_i \in \mathcal{X}$ $(1 \leq i \leq k)$. *Otherwise, it is* unsolved. *A deduction fact is* well-formed *if it is unsolved or if* $t \notin \mathcal{X}$.

For notational convenience we sometimes omit curly braces for the set of side conditions and write $[U \rhd u \mid X_1 \rhd t_1, \ldots, X_n \rhd t_n]$. When $n = 0$ we simply write $[U \rhd u]$ or $[U \sim V]$. We say that two facts are equivalent if they are equal up to bijective renaming of variables. In the following we implicitly suppose that all operations are carried out modulo the equivalence classes. In particular set union will not add equivalent facts and inclusion will test for equivalent facts. Also, we allow *on-the-fly* renaming of variables in facts to avoid variable clashes.

We now introduce the notion of generation of a term t from a set of facts F. Intuitively, t is generated if it can be syntactically "deduced" from F.

Definition 4 (generation). *Let* F *be a finite set of well-formed deduction facts. A term* t *is* generated by F with recipe R, *written* $\mathsf{F} \vdash^R t$, *if*

1. *either* $t = x \in \mathcal{X}$ *and* $R = x$*;*
2. *or there exist a solved fact* $[R_0 \rhd t_0 \mid X_1 \rhd x_1, \ldots, X_n \rhd x_n] \in \mathsf{F}$, *some terms* R_i *for* $1 \leq i \leq n$ *and a substitution* σ *with* $\mathrm{dom}(\sigma) \subseteq \mathrm{var}(t_0)$ *such that* $t = t_0\sigma$, $R = R_0[X_1 \mapsto R_1, \ldots, X_k \mapsto R_k]$, *and* $\mathsf{F} \vdash^{R_i} x_i\sigma$ *for every* $1 \leq i \leq n$.

A term t *is* generated by F, *written* $\mathsf{F} \vdash t$, *if there exists* R *such that* $\mathsf{F} \vdash^R t$.

From this definition follows a simple recursive algorithm for effectively deciding whether $\mathsf{F} \vdash t$, providing also the recipe. Termination is ensured by the fact that $|x_i\sigma| < |t|$ for every $1 \leq i \leq n$. Note that using memoization we can obtain an algorithm in polynomial time.

Given a finite set of equational facts E and terms M, N, we write $\mathsf{E} \models M \sim N$ if $M \sim N$ is a consequence, in the usual first order theory of equality, of

$$\{U\sigma \sim V\sigma \mid [U \sim V \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k] \in \mathsf{E}\} \text{ where } \sigma = \{X_i \mapsto x_i\}_{1 \leq i \leq k}.$$

Note that it may be the case that $x_i = x_j$ for $i \neq j$ (whereas $X_i \neq X_j$).

3.2 Saturation procedure

We define for each fact f its *canonical form* f which is obtained by first applying rule (1) and then rule (2) defined below. The idea is to ensure that each variable x_i occurs at most once in the side conditions and to get rid of those variables that do not occur in t. Unsolved deduction facts are kept unchanged.

$$(1) \quad \frac{[R \rhd t \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k] \;\; \{i, j\} \subseteq \{1, \ldots, n\} \;\; j \neq i \text{ and } x_j = x_i}{[R[X_i \mapsto X_j] \rhd t \mid X_1 \rhd x_1, \ldots, X_{i-1} \rhd x_{i-1}, X_{i+1} \rhd x_{i+1}, \ldots, X_k \rhd x_k]}$$

$$(2) \quad \frac{[R \rhd t \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k] \quad x_i \notin \mathrm{var}(t)}{[R \rhd t \mid X_1 \rhd x_1, \ldots, X_{i-1} \rhd x_{i-1}, X_{i+1} \rhd x_{i+1}, \ldots, X_k \rhd x_k]}$$

A *knowledge base* is a tuple (F, E) where F is a finite set of well-formed deduction facts that are in canonical form and E a finite set of equational facts.

Definition 5 (update). *Given a fact* $\mathsf{f} = [R \rhd t \mid X_1 \rhd t_1, \ldots, X_n \rhd t_n]$ *and a knowledge base* (F, E)*,* the update of (F, E) by f*, written* $(\mathsf{F}, \mathsf{E}) \oplus \mathsf{f}$*, is defined as*

$$\begin{cases} (\mathsf{F} \cup \{\mathsf{f}'\}, \mathsf{E}) & \textit{if } \mathsf{f} \textit{ is solved and } \mathsf{F} \not\vdash t \quad \textsf{useful fact} \\ \quad \textit{where } \mathsf{f}' \textit{ is the canonical form of } \mathsf{f} & \\ (\mathsf{F}, \mathsf{E} \cup \{[R' \sim R\{X_i \mapsto t_i\}_{1 \leq i \leq n}\}]) & \textit{if } \mathsf{f} \textit{ is solved and } \mathsf{F} \vdash t \quad \textsf{useless fact} \\ \qquad\qquad \textit{where } \mathsf{F} \vdash^{R'} t & \\ (\mathsf{F} \cup \{\mathsf{f}\}, \mathsf{E}) & \textit{if } \mathsf{f} \textit{ is not solved} \quad \textsf{unsolved fact} \end{cases}$$

The choice of the recipe R' in the *useless fact* case is defined by the implementation. While this choice does not influence the correctness of the procedure, it might influence its termination as we will see later. Note that, the result of updating a knowledge base by a (possibly not well-formed and/or not canonical) fact is again a knowledge base. Facts that are not well-formed will be captured by the *useless fact* case, which adds an equational fact.

Initialisation. Given a frame $\varphi = \nu\tilde{n}.\{w_1 \mapsto t_1, \ldots, w_n \mapsto t_n\}$, our procedure starts from an *initial knowledge base* associated to φ and defined as follows:

$$\begin{aligned} \mathrm{Init}(\varphi) = \quad & (\emptyset, \emptyset) \\ \textstyle\bigoplus_{1 \leq i \leq n} \; & [w_i \rhd t_i] \\ \textstyle\bigoplus_{n \in \mathrm{fn}(\varphi)} \; & [n \rhd n] \\ \textstyle\bigoplus_{f \in \mathcal{F}} \; & [f(X_1, \ldots, X_k) \rhd f(x_1, \ldots, x_k) \mid X_1 \rhd x_1, \ldots \rhd X_k \rhd x_k] \end{aligned}$$

Example 3. Consider the rewriting system $\mathcal{R}_{\mathcal{E}_{mal}}$ and $\varphi_2 = \nu a, k.\{w_1 \mapsto enc(b, k)\}$. The knowledge base $\mathrm{Init}(\varphi_2)$ is made up of the following deduction facts:

$$\begin{array}{llll} [\, w_1 \rhd enc(b,k) \mid \emptyset] & (\mathsf{f}_1) & [\, enc(Y_1, Y_2) \rhd enc(y_1, y_2) \mid Y_1 \rhd y_1, Y_2 \rhd y_2] & (\mathsf{f}_3) \\ [\, b \rhd b \mid \emptyset] & (\mathsf{f}_2) & [\, dec(Y_1, Y_2) \rhd dec(y_1, y_2) \mid Y_1 \rhd y_1, Y_2 \rhd y_2] & (\mathsf{f}_4) \\ & & [\, mal(Y_1, Y_2) \rhd mal(y_1, y_2) \mid Y_1 \rhd y_1, Y_2 \rhd y_2] & (\mathsf{f}_5) \end{array}$$

Saturation. The main part of our procedure consists in saturating the knowledge base $\mathrm{Init}(\varphi)$ by means of the transformation rules described in Figure 1. The rule Narrowing is designed to apply a rewriting step on an existing deduction fact. Intuitively, this rule allows us to get rid of the equational theory and nevertheless ensure that the generation of deducible terms is complete. The rule F-Solving is used to instantiate an unsolved side condition of an existing deduction fact. Unifying and E-Solving add equational facts which remember when different recipes for a same term exist.

Note that this procedure may not terminate and that the fixed point may not be unique. We write $\Longrightarrow^*$ for the reflexive and transitive closure of $\Longrightarrow$.

Narrowing

$$\frac{\mathsf{f} = [M \rhd C[t] \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k] \in \mathsf{F},\ l \to r \in \mathcal{R}_\mathcal{E} \text{ with } t \notin \mathcal{X},\ \sigma = \mathrm{mgu}(l,t) \text{ and } \mathrm{var}(\mathsf{f}) \cap \mathrm{var}(l) = \emptyset.}{(\mathsf{F},\mathsf{E}) \Longrightarrow (\mathsf{F},\mathsf{E}) \oplus \mathsf{f}_0}$$

where $\mathsf{f}_0 = [M \rhd (C[r])\sigma \mid X_1 \rhd x_1\sigma, \ldots, X_k \rhd x_k\sigma]$.

F-Solving

$$\frac{\mathsf{f}_1 = [M \rhd t \mid X_0 \rhd t_0, \ldots, X_k \rhd t_k],\ \mathsf{f}_2 = [N \rhd s \mid Y_1 \rhd y_1, \ldots, Y_\ell \rhd y_\ell] \in \mathsf{F} \text{ with } t_0 \notin \mathcal{X},\ \sigma = \mathrm{mgu}(s,t_0) \text{ and } \mathrm{var}(\mathsf{f}_1) \cap \mathrm{var}(\mathsf{f}_2) = \emptyset.}{(\mathsf{F},\mathsf{E}) \Longrightarrow (\mathsf{F},\mathsf{E}) \oplus \mathsf{f}_0}$$

where $\mathsf{f}_0 = [M\{X_0 \mapsto N\} \rhd t\sigma \mid X_1 \rhd t_1\sigma, \ldots, X_k \rhd t_k\sigma, Y_1 \rhd y_1\sigma, \ldots, Y_\ell \rhd y_\ell\sigma]$.

Unifying

$$\frac{\mathsf{f}_1 = [M \rhd t \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k],\ \mathsf{f}_2 = [N \rhd s \mid Y_1 \rhd y_1, \ldots, Y_\ell \rhd y_\ell] \in \mathsf{F} \text{ with } \sigma = \mathrm{mgu}(s,t) \text{ and } \mathrm{var}(\mathsf{f}_1) \cap \mathrm{var}(\mathsf{f}_2) = \emptyset.}{(\mathsf{F},\mathsf{E}) \Longrightarrow (\mathsf{F},\mathsf{E} \cup \{\mathsf{f}_0\})}$$

where $\mathsf{f}_0 = [M \sim N \mid \{X_i \rhd x_i\sigma\}_{1 \leq i \leq k} \cup \{Y_i \rhd y_i\sigma\}_{1 \leq i \leq \ell}]$.

E-Solving

$$\frac{\mathsf{f}_1 = [U \sim V \mid Y \rhd s, X_1 \rhd t_1, \ldots, X_k \rhd t_k] \in \mathsf{E}, \mathsf{f}_2 = [M \rhd t \mid Y_1 \rhd y_1, \ldots, Y_\ell \rhd y_\ell\} \in \mathsf{F} \text{ with } s \notin \mathcal{X},\ \sigma = \mathrm{mgu}(s,t) \text{ and } \mathrm{var}(\mathsf{f}_1) \cap \mathrm{var}(\mathsf{f}_2) = \emptyset.}{(\mathsf{F},\mathsf{E}) \Longrightarrow (\mathsf{F},\mathsf{E} \cup \{\mathsf{f}_0\})}$$

where $\mathsf{f}_0 = [U\{Y \mapsto M\} \sim V\{Y \mapsto M\} \mid \{X_i \rhd t_i\sigma\}_{1 \leq i \leq k} \cup \{Y_i \rhd y_i\sigma\}_{1 \leq i \leq \ell}]$.

Fig. 1. Saturation rules

Example 4. Continuing Example 3, we illustrate the saturation procedure. We can apply the rule Narrowing on fact f_4 and rewrite rule $dec(enc(x,y),y) \to x$, as well as on fact f_5 and rewrite rule $mal(enc(x,y),z) \to enc(z,y)$ adding facts

$$[dec(Y_1,Y_2) \rhd x \mid Y_1 \rhd enc(x,y), Y_2 \rhd y] \qquad (\mathsf{f}_6)$$
$$[mal(Y_1,Y_2) \rhd enc(z,y) \mid Y_1 \rhd enc(x,y), Y_2 \rhd z] \qquad (\mathsf{f}_7)$$

The facts f_6 and f_7 are not solved and we can apply the rule F-Solving with f_1 adding the facts:

$$[dec(w_1,Y_2) \rhd b \mid Y_2 \rhd k] \ (\mathsf{f}_8) \qquad [mal(w_1,Y_2) \rhd enc(z,k) \mid Y_2 \rhd z] \ (\mathsf{f}_9)$$

Rule Unifying can be used on facts $\mathsf{f}_1/\mathsf{f}_3$, $\mathsf{f}_3/\mathsf{f}_9$ as well as $\mathsf{f}_1/\mathsf{f}_9$ to add equational facts. This third case allows one to obtain $\mathsf{f}_{10} = [w_1 \sim mal(w_1,Y_2) \mid Y_2 \rhd b]$ which can be solved (using E-Solving with f_2) to obtain $\mathsf{f}_{11} = [w_1 \sim mal(w_1,b)]$. Because of lack of space we do not detail the remaining rule applications. When reaching a fixed point the knowledge base contains the solved facts f_9 and f_{11} as well as those in $\mathrm{Init}(\varphi_2)$.

We now state the soundness and completeness of our transformation rules. The technical lemmas used to prove this result are detailed in Section 4.

Theorem 1 (soundness and completeness). *Let* φ *be a frame and* (F, E) *be a saturated knowledge base such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$*. Let* $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$ *and* $\mathsf{F}^+ = \mathsf{F} \cup \{[n \rhd n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$*. We have that:*

1. *For all* $M \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi))$ *such that* $\mathrm{fn}(M) \cap \mathrm{bn}(\varphi) = \emptyset$*, we have that*
$$M\varphi =_{\mathcal{E}} t \Leftrightarrow \exists N,\ \mathsf{E} \models M \sim N \text{ and } \mathsf{F}^+ \vdash^N t\!\downarrow_{\mathcal{R}_\mathcal{E}}$$
2. *For all* $M, N \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi))$ *such that* $\mathrm{fn}(M, N) \cap \mathrm{bn}(\varphi) = \emptyset$*, we have*
$$(M =_{\mathcal{E}} N)\varphi \ \Leftrightarrow\ \mathsf{E} \models M \sim N.$$

3.3 Application to deduction and static equivalence

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

1. Apply the saturation rules to obtain (if any) a saturated knowledge base (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. Let $\mathsf{F}^+ = \mathsf{F} \cup \{[n \rhd n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$.
2. Return *yes* if there exists N such that $\mathsf{F}^+ \vdash^N t\!\downarrow_{\mathcal{R}_\mathcal{E}}$ (that is, the $\mathcal{R}_\mathcal{E}$-normal form of t is generated by F with recipe N); otherwise return *no*.

Example 5. We continue our running example. Let (F, E) be the knowledge base obtained from $\mathrm{Init}(\varphi_2)$ described in Example 4. We show that $\varphi_2 \vdash enc(c, k)$ and $\varphi_2 \vdash b$. Indeed we have that $\mathsf{F} \cup \{[c \rhd c]\} \vdash^{mal(w_1,c)} enc(c, k)$ using facts f_9 and $[c \rhd c]$, and $\mathsf{F} \vdash^b b$ using fact f_2.

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

1. Apply the transformation rules to obtain (if possible) two saturated knowledge bases $(\mathsf{F}_i, \mathsf{E}_i)$, $i = 1, 2$ such that $\mathrm{Init}(\varphi_i) \Longrightarrow^* (\mathsf{F}_i, \mathsf{E}_i)$, $i = 1, 2$.
2. For $\{i, j\} = \{1, 2\}$, for every solved fact $[M \sim N \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k]$ in E_i, check if $(M\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\} =_{\mathcal{E}} N\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\})\varphi_j$.
3. If so return *yes*; otherwise return *no*.

Example 6. Consider again the frames φ_1 and φ_2 which are not statically equivalent (see Example 2). Our procedure answers *no* since $[mal(w_1, b) \sim w_1] \in \mathsf{E}_2$ whereas $(mal(w_1, b) \neq_{\mathcal{E}_{mal}} w_1)\varphi_1$.

4 Soundness and completeness

In this section we give the key results which are used to prove the two directions of Theorem 1. The soundness of our saturation procedure relies on Lemma 1 whereas its completeness is more involved: the key propositions are stated below.

Intuitively Lemma 1 states that any ground term which can be generated is indeed deducible. Similarly all equations which are consequences of the knowledge base are true equations in the initial frame. The soundness of our saturation procedure can be easily derived from this lemma.

Lemma 1 (soundness). *Let φ be a frame and (F, E) be a knowledge base such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. *Let $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$, $M, N \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi))$ such that* $\mathrm{fn}(M, N) \cap \mathrm{bn}(\varphi) = \emptyset$, *and* $\mathsf{F}^+ = \mathsf{F} \cup \{[n \rhd n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$. *We have that:*

1. $\mathsf{F}^+ \vdash^M t \ \Rightarrow \ M\varphi =_{\mathcal{E}} t$; *and*
2. $\mathsf{E} \models M \sim N \ \Rightarrow \ (M =_{\mathcal{E}} N)\varphi$.

We now give two propositions that are used to show the completeness of the saturation rules. The first one states that whenever there exist two recipes to generate a ground term from F then the equation on the two recipes is a consequence of E.

Proposition 1 (completeness, equation). *Let (F, E) be a saturated knowledge base, and M, N be two terms such that $\mathsf{F} \vdash^M t$ and $\mathsf{F} \vdash^N t$ for some ground term t. Then, we have that $\mathsf{E} \models M \sim N$.*

Next we show that whenever a ground term (not necessarily in normal form) can be generated then its normal form can also be generated and there exists an equation on the two recipes.

Proposition 2 (completeness, reduction). *Let (F, E) be a saturated knowledge base, M a term and t a ground term such that $\mathsf{F} \vdash^M t$ and $t{\downarrow_{\mathcal{R}_\mathcal{E}}} \neq t$. Then there exists M' and t' such that $\mathsf{F} \vdash^{M'} t'$ with $t \rightarrow^+_{\mathcal{R}_\mathcal{E}} t'$ and $\mathsf{E} \models M \sim M'$.*

Relying on these propositions, we can show completeness of our saturation procedure (i.e. $\Rightarrow$ of Theorem 1).

1. To prove item 1, we first observe that if t is deducible from φ modulo $\mathcal{E}$ then $\mathsf{F}^+ \vdash^{M'} t_0$ for some M' and t_0 such that $\mathsf{E} \models M \sim M'$ and $t_0 \rightarrow^* t{\downarrow_{\mathcal{R}_\mathcal{E}}}$. Actually M' differs from M by the fact that some public names that do not occur in the knowledge base are replaced by fresh variables. Then, we rely on Proposition 2 and we show the result by induction on t_0 equipped with the order $<$ induced by the rewriting relation ($t < t'$ iff $t \rightarrow^+ t'$).
2. Now, to prove item 2, we apply the result shown in item 1 on $M\varphi =_{\mathcal{E}} t$ and $N\varphi =_{\mathcal{E}} t$ where $t = M\varphi{\downarrow_{\mathcal{R}_\mathcal{E}}} = N\varphi{\downarrow_{\mathcal{R}_\mathcal{E}}}$. We deduce that there exist M' and N' such that $\mathsf{E} \models M \sim M'$, $\mathsf{F}^+ \vdash^{M'} t$, $\mathsf{E} \models N \sim N'$, and $\mathsf{F}^+ \vdash^{N'} t$. Then, Proposition 1 allows one to deduce that $\mathsf{E} \models M' \sim N'$, thus $\mathsf{E} \models M \sim N$.

5 Termination

As already announced the saturation process may not always terminate.

Example 7. Consider the convergent rewriting system consisting of the single rule $f(g(x)) \rightarrow g(h(x))$ and the frame $\phi = \nu a.\{w_1 \mapsto g(a)\}$. We have that

$$\mathrm{Init}(\varphi) \supseteq \{[w_1 \rhd g(a)],\ [f(X) \rhd f(x) \mid X \rhd x]\}.$$

By $\mathsf{Narrowing}$ we can add the fact $\mathsf{f}_1 = [f(X) \rhd g(h(x)) \mid X \rhd g(x)]$. Then we can apply $\mathsf{F\text{-}Solving}$ to solve its side condition $X \rhd g(x)$ with the fact $[w_1 \rhd g(a)]$

yielding the solved fact $[f(w_1) \rhd g(h(a))]$. Now, applying iteratively F-Solving on f_1 and the newly generated fact, we generate an infinity of solved facts of the form $[f(\ldots f(w_1)\ldots) \rhd g(h(\ldots h(a)\ldots))]$. Intuitively, this happens because our symbolic representation is unable to express that the function h can be nested an unbounded number of times when it occurs under an application of g.

The same kind of limitation already exists in the procedure implemented in YAPA [9]. However, our symbolic representation, that manipulates terms that are not necessarily ground and facts with side conditions, allows us to go beyond YAPA. We are able for instance to treat equational theories such as malleable encryption and trapdoor commitment.

5.1 Generic method for proving termination

We provide a generic method for proving termination, which we instantiate in the following section on several examples.

In order to prove that the saturation algorithm terminates, we require that the update function $\oplus$ be *uniform*: i.e., the same recipe R' be used for all useless solved deduction facts that have the same canonical form. Note that the soundness and completeness of the algorithm does not depend on the choice of the recipe R' when updating the knowledge base with a useless fact (*cf.* Definition 5).

Definition 6 (projection). *We define the* projection *of a deduction fact* $\mathsf{f} = [R \rhd t \mid X_1 \rhd t_1, \ldots, X_n \rhd t_n]$ *as* $\hat{\mathsf{f}} = [t \mid \{t_1, \ldots, t_n\}]$. *We extend the projection to sets of facts* F *and define* $\hat{\mathsf{F}} = \{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}\}$.

We identify projections which are equal up to bijective renaming of variables and we sometimes omit braces for the side conditions.

Proposition 3 (generic termination). *The saturation algorithm terminates if* $\oplus$ *is uniform and there exist some functions* $\mathcal{Q}$, $\mathsf{m_f}$, $\mathsf{m_e}$ *and some well-founded orders* $<_{\mathsf{f}}$ *and* $<_{\mathsf{e}}$ *such that for all frame* φ, *and for all* (F, E) *such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$, *we have that:*

1. $\{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}$ *and* f *is a solved deduction fact*$\} \subseteq \mathcal{Q}(\varphi)$ *and* $\mathcal{Q}(\varphi)$ *is finite;*
2. $\mathsf{m_f}(\mathsf{f}_0) <_{\mathsf{f}} \mathsf{m_f}(\mathsf{f}_1)$ *where* f_0, f_1 *are defined as in rule F-Solving;*
3. $\mathsf{m_e}(\mathsf{f}_0) <_{\mathsf{e}} \mathsf{m_e}(\mathsf{f}_1)$ *where* f_0, f_1 *are defined as in rule E-Solving.*

5.2 Applications

We now give several examples for which the saturation procedure indeed terminates. For each of these theories the definition of the function $\mathcal{Q}$ relies on the following notion of *extended subterm.*

Definition 7 (extended subterm). *Let t be a term, its set of* extended subterms $\mathrm{st}_{\mathcal{R}_\mathcal{E}}(t)$ *(w.r.t. $\mathcal{E}$), is the smallest set such that:*

1. $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(t)$,
2. $f(t_1, \ldots, t_k) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(t)$ *implies* $t_1, \ldots, t_k \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(t)$,
3. $t' \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(t)$ *and* $t' \to_{\mathcal{R}_\mathcal{E}} t''$ *implies* $t'' \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(t)$.

This notation is extended to frames in the usual way.

All the examples in this section rely on the same measures $\mathsf{m_f}$ and $\mathsf{m_e}$. Let $\{X_1 \rhd t_1, \ldots, X_n \rhd t_n\}$ be the set of side conditions of a fact f. We define $\mathsf{m_f}(\mathsf{f}) = (\#\,\mathrm{var}(t_1, \ldots, t_n), \sum_{1 \leq i \leq n} |t_i|)$ and $<_\mathsf{f}$ is the lexicographical order on ordered pairs of integers. The measure $\mathsf{m_e}$ and the order $<_\mathsf{e}$ are defined in the same way.

We now present the class of subterm convergent equational theories as well as the theories for malleable encryption and trap-door commitment. The detailed proofs are given in Appendix B.

Subterm convergent equational theories. Abadi and Cortier [1] have shown that deduction and static equivalence are decidable for *subterm convergent* equational theories in polynomial time. We retrieve the same results with our algorithm. An equational theory $\mathcal{E}$ is subterm convergent if $\mathcal{R}_\mathcal{E}$ is convergent and for every rule $l \to r \in \mathcal{R}_\mathcal{E}$, we have that either r is a strict subterm of l, or r is a ground term in $\mathcal{R}_\mathcal{E}$-normal form.

The termination proof for this class relies on the function $\mathcal{Q}$ where $\mathcal{Q}(\varphi)$ is defined as the smallest that contains

1. $[t \mid \emptyset]$, where $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$;
2. $[f(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$, where $ar(f) = k$.

Malleable encryption. We obtain also termination for the equational theory $\mathcal{E}_{mal}$ described in Example 1. This is a toy example that does not fall in the class studied in [1]. Indeed, this theory is not *locally stable*: the set of terms in normal form deducible from a frame φ cannot always be obtained by applying public contexts over a finite set (called $sat(\varphi)$ in [1]) of ground terms.

As a witness consider the frame $\varphi_2 = \nu a, k.\{w_1 \mapsto enc(b, k\}$ introduced in Example 2. Among the terms that are deducible from φ_2, we have those of the form $enc(t, k)$ where t represents any term deducible from φ_2. From this observation, it is easy to see that $\mathcal{E}_{mal}$ is not locally stable.

Our procedure does not have this limitation. A prerequisite for termination is that the set of terms in normal form deducible from a frame is exactly the set of terms obtained by nesting in all possible ways a finite set of contexts. The theory $\mathcal{E}_{mal}$ falls in this class. In particular, for the frame φ_2, our procedure produces the fact $\mathsf{f}_9 = [mal(w_1, Y_2) \rhd enc(z, k) \mid Y_2 \rhd z]$ allowing us to capture all the terms of the form $enc(t, k)$ by the means of a single deduction fact.

The termination proof relies on the function $\mathcal{Q}$ where $\mathcal{Q}(\varphi)$ is defined as the smallest set that contains:

1. $[t \mid \emptyset]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$;
2. $[f(x_1, x_2) \mid x_1, x_2]$, where $f \in \{enc, dec, mal\}$;
3. $[enc(x, t) \mid x]$, if there exists t' such that $enc(t', t) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$.

Trap-door commitment. The following convergent equational theory $\mathcal{E}_{td}$ is a model for trap-door commitment:

$$\begin{array}{ll} open(td(x,y,z),y) = x & td(x_2, f(x_1,y,z,x_2), z) = td(x_1,y,z) \\ open(td(x_1,y,z), f(x_1,y,z,x_2)) = x_2 & f(x_2, f(x_1,y,z,x_2), z, x_3) = f(x_1,y,z,x_3) \end{array}$$

As said in introduction, we encountered this equational theory when studying electronic voting protocols. The term $td(m,r,td)$ models the commitment of the message m under the key r using an additional trap-door td. Such a commitment scheme allows a voter who has performed a commitment to open it in different ways using its trap-door. Hence, trap-door bit commitment $td(v,r,td)$ does not bind the voter to the vote v. This is useful to ensure privacy-type properties in e-voting and in particular receipt-freeness [18]. With such a scheme, even if a coercer requires the voter to reveal his commitment, this does not give any useful information to the coercer as the commitment can be viewed as the commitment of any vote (depending on the key that will be used to open it).

For the same reason as $\mathcal{E}_{mal}$, the theory of trap-door commitment described below cannot be handle by the algorithms described in [1, 9]. Our termination proof relies on the function $\mathcal{Q}$ where $\mathcal{Q}(\varphi)$ is the smallest set that contains:

1. $[t \mid \emptyset]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$;
2. $[td(t_1, r, tp) \mid \emptyset]$ such that $f(t_1, r, tp, t_2) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some t_2;
3. $[g(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$, where $g \in \{open, td, f\}$ and $ar(g) = k$;
4. $[f(t_1, r, tp, x) \mid x]$, such that $f(t_1, r, tp, t_2) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some t_2.

Termination of our procedure is also ensured for theories such as blind signature and addition as defined in [1].

5.3 Going beyond with fair strategies

In [1] decidability is also shown for an equational theory modeling homomorphic encryption. For our procedure to terminate on this theory we use a particular saturation strategy.

Homomorphic encryption. We consider the theory $\mathcal{E}_{\mathsf{hom}}$ of homomorphic encryption that has been studied in [1, 9].

$$\begin{gathered} fst(pair(x,y)) = x \qquad snd(pair(x,y)) = y \qquad dec(enc(x,y),y) = x \\ enc(pair(x,y),z) = pair(enc(x,z), enc(y,z)) \\ dec(pair(x,y),z) = pair(dec(x,z), dec(y,z)) \end{gathered}$$

In general, our algorithm does not terminate under this equational theory. Consider for instance the frame $\phi = \nu a, b.\{w_1 \mapsto pair(a,b)\}$. We have that:

$$\mathrm{Init}(\varphi) \supseteq \{[w_1 \rhd pair(a,b)],\ [enc(X,Y) \rhd enc(x,y) \ \mid \ X \rhd x,\, Y \rhd y]\}.$$

As in Example 7 we can obtain an unbounded number of solved facts whose projections are of the form:

$$[pair(enc(\dots enc(a, z_1)\dots, z_n), enc(\dots enc(b, z_1)\dots, z_n)) \mid z_1, \dots, z_n].$$

However, we can guarantee termination by using a *fair* saturation strategy. We say that a saturation strategy is fair if whenever a rule instance is enabled it will eventually be taken. Indeed in the above example using a fair strategy we will eventually add the facts $[fst(w_1) \rhd a]$ and $[snd(w_1) \rhd b]$. Now the "problematic" facts described above become useless and are not added to the knowledge base anymore. One may note that a fair strategy does not guarantee termination in Example 7 (intuitively, because the function g is one-way and a is not deducible in that example).

The proof of termination will as for the previous theories define functions $\mathcal{Q}$, $\mathsf{m_f}$ and $\mathsf{m_e}$. The main argument of the proof is the observation that due to fairness only a finite number of solved fact not in $\mathcal{Q}(\varphi)$ can be added. More details are given in Appendix B.

6 Implementation

A C++ implementation of the procedures described in this paper is provided in the KiSs (Knowledge In Security protocolS) tool [11].

The tool implements a fair saturation strategy and a uniform $\oplus$. Moreover the tool implements several optimizations. First, as the order of solving side conditions is not important we always solve the first (unsolved) side condition rather than considering all the combinations. In our implementation, we use a DAG representation of terms and specialized F-Solving and E-Solving rules when a ground term is solved. Indeed, by checking whether the side condition is generated or not we know whether solving it will eventually produce a solved fact. Note that checking generation can be done in polynomial time. This makes the procedure terminate in polynomial time for subterm convergent equational theories, and the theories $\mathcal{E}_{blind}$, $\mathcal{E}_{mal}$ and $\mathcal{E}_{td}$.

The performances of the tool are comparable to the YAPA tool [8, 9] and on most examples the tool terminates in less than a second. In [9] a family of contrived examples is presented to diminish the performance of YAPA exploiting the fact that YAPA does not implement DAG representations of terms and recipes, as opposed to KiSs. As expected KiSs indeed performs better on these examples.

Regarding termination, our procedure terminates on all examples of equational theories presented in [9]. In addition, our tool terminates on the theories $\mathcal{E}_{mal}$ and $\mathcal{E}_{td}$ whereas YAPA does not. In [9] a class of equational theories for which YAPA terminates is identified and it is not known whether our procedure terminates. YAPA may also terminate on examples outside this class. Hence the question whether termination of our procedures encompasses termination of YAPA is still open.

References

1. M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 387(1-2):2–32, 2006.
2. M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. 28th ACM Symposium on Principles of Programming Languages (POPL'01)*. ACM, 2001.
3. S. Anantharaman, P. Narendran, and M. Rusinowitch. Intruders with caps. In *Proc. 18th International Conference on Term Rewriting and Applications (RTA'07)*, volume 4533 of *LNCS*. Springer, 2007.
4. A. Armando et al. The AVISPA Tool for the automated validation of internet security protocols and applications. In *Proc. 17th Int. Conference on Computer Aided Verification (CAV'05)*, volume 3576 of *LNCS*, pages 281–285. Springer, 2005.
5. M. Backes, C. Hritcu, and M. Maffei. Automated verification of remote electronic voting protocols in the applied pi-calculus. In *Proc. 21st IEEE Computer Security Foundations Symposium (CSF'08)*, 2008.
6. M. Backes, M. Maffei, and D. Unruh. Zero-knowledge in the applied pi-calculus and automated verification of the direct anonymous attestation protocol. In *IEEE Symposium on Security and Privacy (S&P'08)*. IEEE Comp. Soc. Press, 2008.
7. M. Baudet. Deciding security of protocols against off-line guessing attacks. In *12th ACM Conference on Computer and Communications Security (CCS'05)*, 2005.
8. M. Baudet. YAPA (Yet Another Protocol Analyzer), 2008. http://www.lsv.ens-cachan.fr/~baudet/yapa/index.html.
9. M. Baudet, V. Cortier, and S. Delaune. YAPA: A generic tool for computing intruder knowledge. Research Report LSV-09-03, Laboratoire Spécification et Vérification, ENS Cachan, France, Feb. 2009. 26 pages.
10. Y. Chevalier. *Résolution de problèmes d' accessibilité pour la compilation et la validation de protocoles cryptographiques*. PhD thesis, Université Henri Poincaré, Nancy (France), 2003.
11. Ş. Ciobâcă. KiSs, 2009. http://www.lsv.ens-cachan.fr/~ciobaca/kiss.
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)*, ENTCS, 2004.
13. V. Cortier and S. Delaune. Deciding knowledge in security protocols for monoidal equational theories. In *Proc. 14th Int. Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07)*, LNAI. 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, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 2008. To appear.
16. P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of Abelian groups with distributive encryption. *Information and Computation*, 205(4):581–623, 2007.
17. J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *Proc. 8th ACM Conference on Computer and Communications Security (CCS'01)*, 2001.
18. T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In *Proc. 5th Int. Security Protocols Workshop*, volume 1361. Springer, 1997.
19. M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions and composed keys is NP-complete. *Theoretical Computer Science*, 299:451–475, 2003.

A Proofs of Section 4

We now define when a fact makes a valid statement about a given frame φ. We say that the fact *holds* in φ.

Definition 8 (f holds in φ). *Let φ be a frame and $\mathsf{f} = [R \rhd t \mid \Delta]$ (respectively $[U \sim V \mid \Delta]$) be a fact with $\Delta = \{X_1 \rhd t_1, \dots, X_k \rhd t_k\}$. We say that* f holds *in φ if for any substitution τ grounding for $t_1, \dots, t_k$ such that $\varphi \vdash_{\mathcal{E}} t_i\tau$ with recipe R_i for $1 \leq i \leq n$, we have that $\varphi \vdash_{\mathcal{E}} t\tau$ with recipe $R\{X_i \mapsto R_i\}_{1 \leq i \leq k}$ (respectively $(U\{X_i \mapsto R_i\}_{1 \leq i \leq k} =_{\mathcal{E}} V\{X_i \mapsto R_i\}_{1 \leq i \leq k})\varphi$).*

A.1 Soundness

Lemma 4. *Let φ be a frame and (F, E) be a knowledge base such that every fact in (F, E) (deduction or equational) holds in φ. Let f_0 be a fact that holds in φ, then every fact in $(\mathsf{F}, \mathsf{E}) \oplus \mathsf{f}_0$ holds in φ.*

Lemma 5. *Let φ be a frame and (F, E) be a knowledge base such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. Then every $\mathsf{f} \in \mathsf{F} \cup \mathsf{E}$ holds in φ.*

Proof. By induction on the derivation $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$.

Base case: We have that $(\mathsf{F}, \mathsf{E}) = \mathrm{Init}(\varphi)$. To conclude, we have to show that the facts and the equations we put in the initial knowledge base hold in φ.

There are three kind of deduction facts that can be added in the knowledge base: the facts that come from φ, those of the form $[n \rhd n]$ for $n \in \mathrm{fn}(\varphi)$, and those of the form:

$$[f(X_1, \dots, X_k) \rhd f(x_1, \dots, x_k) \mid X_1 \rhd x_1, \dots, X_k \rhd x_k].$$

It is easy to see that all these facts hold in φ and we can conclude by Lemma 4.

Induction step: In such a case, we have $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}', \mathsf{E}') \Longrightarrow (\mathsf{F}, \mathsf{E})$. We perform a case analysis on the inference rule used in $(\mathsf{F}', \mathsf{E}') \Longrightarrow (\mathsf{F}, \mathsf{E})$. For each rule, we show that the resulting fact f_0 holds in φ and we conclude by relying on Lemma 4.

Rule Narrowing: Let $\mathsf{f} = [M \rhd C[t] \mid X_1 \rhd x_1, \dots, X_k \rhd x_k]$ be the deduction fact, $l \to r \in \mathcal{R}_{\mathcal{E}}$ be the rewrite rule and $\sigma = \mathrm{mgu}(l, t)$ be the substitution involved in this step. Let $\mathsf{f}_0 = [M \rhd (C[r])\sigma \mid X_1 \rhd x_1\sigma, \dots, X_k \rhd x_k\sigma]$ be the resulting deduction fact.

We show that f_0 holds in φ. Let τ be a substitution such that $\varphi \vdash_{\mathcal{E}} x_i\sigma\tau$ with recipe M_i ($1 \leq i \leq k$). Since f holds in φ, we have that $\varphi \vdash_{\mathcal{E}} (C[t])\sigma\tau$ with recipe $M' = M\{X_1 \mapsto M_1, \dots, X_k \mapsto M_k\}$. It is easy to see that the following equalities are satisfied:

$$(C[t])\sigma\tau = (C[l])\sigma\tau =_{\mathcal{E}} (C[r])\sigma\tau$$

Therefore $\varphi \vdash_{\mathcal{E}} (C[r])\sigma\tau$ by recipe M', and thus f_0 holds in φ.

Rule F-Solving: Let $\mathsf{f}_1 = [M \rhd t \mid X_0 \rhd t_0, \ldots, X_k \rhd t_k]$ with $t_0 \notin \mathcal{X}$ and $\mathsf{f}_2 = [N \rhd s \mid Y_1 \rhd y_1, \ldots, Y_\ell \rhd y_\ell]$ be the two deduction facts and $\sigma = \mathrm{mgu}(s, t_0)$ be the substitution involved in this step. Let f_0 be the resulting deduction fact:

$$\mathsf{f}_0 = [M\{X_0 \mapsto N\} \rhd t\sigma \mid X_1 \rhd t_1\sigma, \ldots, X_k \rhd t_k\sigma, Y_1 \rhd y_1\sigma, \ldots, Y_\ell \rhd y_\ell\sigma].$$

We show that f_0 holds in φ. Let τ be a substitution such that $\varphi \vdash_\mathcal{E} t_i\sigma\tau$ with recipe M_i $(1 \leq i \leq k)$ and $\varphi \vdash_\mathcal{E} y_j\sigma\tau$ with recipes N_j $(1 \leq j \leq \ell)$. Since f_2 holds in φ, we have that $\varphi \vdash_\mathcal{E} s\sigma\tau$ with recipe $N' = N\{Y_1 \mapsto N_1, \ldots, Y_\ell \mapsto N_\ell\}$. Since f_1 holds in φ and $s\sigma\tau = t_0\sigma\tau$, we deduce that $\varphi \vdash_\mathcal{E} t\sigma\tau$ with recipe

$$\begin{aligned}&M\{X_0 \mapsto N', X_1 \mapsto M_1, \ldots, X_k \mapsto M_k\}\\ &= (M\{X_0 \mapsto N\})\{X_1 \mapsto M_1, \ldots, X_k \mapsto M_k, Y_1 \mapsto N_1, \ldots, Y_\ell \mapsto N_\ell\}.\end{aligned}$$

This allows us to conclude that f_0 holds in φ.

Rule Unifying: Let $\mathsf{f}_1 = [M \rhd t \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k]$ and $\mathsf{f}_2 = [N \rhd s \mid Y_1 \rhd y_1, \ldots, Y_\ell \rhd y_\ell]$ be the two solved deduction facts and $\sigma = \mathrm{mgu}(s, t)$ be the substitution involved in this step. Let f_0 be the resulting equational fact:

$$\mathsf{f}_0 = [M \sim N \mid X_1 \rhd x_1\sigma, \ldots, X_k \rhd x_k\sigma, Y_1 \rhd y_1\sigma, \ldots, Y_\ell \rhd y_\ell\sigma].$$

We show that f_0 holds in φ. Let τ be a substitution such that $\varphi \vdash_\mathcal{E} x_i\sigma\tau$ with recipe M_i $(1 \leq i \leq k)$ and $\varphi \vdash_\mathcal{E} y_j\sigma\tau$ with recipes N_j $(1 \leq j \leq \ell)$. Since f_1 and f_2 holds in φ and $s\sigma\tau = t\sigma\tau$, we deduce that $\varphi \vdash_\mathcal{E} t\sigma\tau$ with recipe $M\{X_1 \mapsto M_1, \ldots, X_k \mapsto M_k\}$ and $N\{Y_1 \mapsto N_1, \ldots, Y_k \mapsto N_\ell\}$. This allows us to conclude that f_0 holds in φ.

Rule E-Solving: Let $\mathsf{f}_1 = [U \sim V \mid Y \rhd s, X_1 \rhd t_1, \ldots, X_k \rhd t_k]$ be the equational fact and $\mathsf{f}_2 = [N \rhd t \mid Y_1 \rhd y_1, \ldots, Y_\ell \rhd y_\ell]$ be the solved deduction fact, and $\sigma = \mathrm{mgu}(s, t)$ be the substitution involved in this step. Let f_0 be the resulting equational fact:

$$\mathsf{f}_0 = [U\{Y \mapsto N\} \sim V\{Y \mapsto N\} \mid X_1 \rhd t_1\sigma, \ldots, X_k \rhd t_k\sigma, Y_1 \rhd y_1\sigma, \ldots, Y_\ell \rhd y_\ell\sigma].$$

We show that f_0 holds in φ. Let τ be a substitution such that $\varphi \vdash_\mathcal{E} t_i\sigma\tau$ with recipe M_i $(1 \leq i \leq k)$ and $\varphi \vdash_\mathcal{E} y_j\sigma\tau$ with recipe N_j $(1 \leq j \leq \ell)$. Since f_2 holds in φ, we deduce that $\varphi \vdash_\mathcal{E} t\sigma\tau$ with recipe $N' = N[Y_1 \mapsto N_1, \ldots, Y_\ell \mapsto N_\ell]$. Since $s\sigma\tau = t\sigma\tau$, we deduce that $\varphi \vdash_\mathcal{E} s\sigma\tau$ with recipe N', and by using the fact that f_1 holds in φ we deduce that

$$(U\{Y \mapsto N', X_1 \mapsto M_1, \ldots, X_k \mapsto M_k\} =_\mathcal{E} V\{Y \mapsto N', X_1 \mapsto M_1, \ldots, X_k \mapsto M_k\})\varphi.$$

Thus, f_0 holds in φ. ☐

Lemma 1 (soundness). *Let φ be a frame and (F, E) be a knowledge base such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. Let $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$, $M, N \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi))$ such that $\mathrm{fn}(M, N) \cap \mathrm{bn}(\varphi) = \emptyset$, and $\mathsf{F}^+ = \mathsf{F} \cup \{[n \rhd n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$. We have that:*

1. $\mathsf{F}^+ \vdash^M t \Rightarrow M\varphi =_\mathcal{E} t$; *and*
2. $\mathsf{E} \models M \sim N \Rightarrow (M =_\mathcal{E} N)\varphi$.

Proof. By Lemma 15 and because every $\mathsf{f} \in \{[n \rhd n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$ holds in φ, we have that all facts in F^+ hold in φ. To conclude, we show the points 1 and 2 stated in the Lemma.

1. Let M and t be such that $\mathsf{F}^+ \vdash^M t$. By definition of $\vdash$, as t is ground, there exists a solved deduction fact $\mathsf{f}_0 = [M_0 \rhd t_0 \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k] \in \mathsf{F}^+$ such that $t = t_0\sigma$ for some substitution σ and $\mathsf{F}^+ \vdash^{M_i} x_i\sigma$ for some M_i $(1 \leq i \leq k)$ and $M = M_0\{X_1 \mapsto M_1, \ldots, X_k \mapsto M_k\}$. We show the result by induction on $|t|$.
   Base case: $|t| = 1$. In such a case t is either a name or a constant. We have that $k = 0$, $t_0 = t$ and $M = M_0$. Since f_0 holds in φ, we deduce that $\varphi \vdash_{\mathcal{E}} t$ with recipe M_0, i.e. $M_0\varphi =_{\mathcal{E}} t$. This allows us to conclude.

   Induction step. Note that $|x_i\sigma| < |t|$ and $\mathsf{F}^+ \vdash^{M_i} x_i\sigma$, thus we can apply our induction hypothesis on $x_i\sigma$. We deduce that $M_i\varphi =_{\mathcal{E}} x_i\sigma$ and thus $M\varphi =_{\mathcal{E}} t_0\sigma = t$ since f_0 holds in φ.
2. Let M and N be such that $\mathrm{fn}(M, N) \cap \mathrm{bn}(\varphi) = \emptyset$ and $\mathsf{E} \models M \sim N$. To show that $(M =_{\mathcal{E}} N)\varphi$, it is sufficient to establish that

   $$(M'\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\} =_{\mathcal{E}} N'\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\})\varphi$$

   for every solved equational fact $[M' \sim N' \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k] \in \mathsf{E}$. This follows easily from Lemma 15. $\square$

A.2 Completeness

Lemma 2. *Let (F, E) be a saturated knowledge base and $\mathsf{f} = [U \sim V \mid X_1 \rhd t_1, \ldots, X_k \rhd t_k]$ be an equational fact in E. For any substitution σ grounding for $\{t_1, \ldots, t_k\}$ such that $\mathsf{F} \vdash t_i\sigma$ $(1 \leq i \leq k)$, we have that $\mathsf{F} \vdash^{R_i} t_i\sigma$ for some R_i $(1 \leq i \leq k)$ and $\mathsf{E} \models U\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\} \sim V\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\}$.*

Proof. We show this result by induction on $\sum_{i=1}^{k} |t_i\sigma|$. We distinguish two cases:

1. f *is a solved equational fact*, i.e. $t_1, \ldots, t_k$ are variables (not necessarily distinct), say $x_1, \ldots, x_k$. In such a case, we have that

   $$\mathsf{E} \models U\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\} \sim V\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\}.$$

   We choose each R_i arbitrarily such that $x_i = x_j$ implies $R_i = R_j$. Then, it is easy to conclude.
2. f *is an unsolved equational fact.* In such a case, there exists t_j such that $t_j \notin \mathcal{X}$. Let us assume w.l.o.g. that $j = 1$. As $\mathsf{F} \vdash t_1\sigma$, we know that there exist a solved deduction fact $\mathsf{f}^1 = [R^1 \rhd t^1 \mid X_1^1 \rhd x_1^1, \ldots, X_\ell^1 \rhd x_\ell^1]$ in F and a substitution τ such that $t^1\tau = t_1\sigma$ and $\mathsf{F} \vdash^{R_i'} x_i^1\tau$ $(1 \leq i \leq \ell)$.
   Let $\rho = \mathrm{mgu}(t_1, t^1)$. We have that the following fact f_2 is in E since (F, E) is saturated:

   $$[U\{X_1 \mapsto R^1\} \sim V\{X_1 \mapsto R^1\} \mid X_1^1 \rhd x_1^1\rho, \ldots, X_\ell^1 \rhd x_\ell^1\rho, X_2 \rhd t_2\rho, \ldots, X_k \rhd t_k\rho].$$

Let σ' be the substitution such that $\sigma \cup \tau = \rho \circ \sigma'$. As the fact f^1 is solved, $x_1^1\rho\sigma', \dots, x_\ell^1\rho\sigma'$ are strict subterms of $t^1\rho\sigma' = t^1\tau$ and $\sum_{i=1}^{\ell} |x_i^1\rho\sigma'| < |t^1\tau| = |t_1\sigma|$. Thus we can apply our induction hypothesis on the equational fact f_2 with the substitution σ'. This allows us to obtain that there exist $M_1^1, \dots, M_\ell^1, M_2, \dots, M_k$ such that $\mathsf{F} \vdash^{M_i} t_i\rho\sigma' = t_i\sigma$ $(2 \leq i \leq k)$ and $\mathsf{F} \vdash^{M_i^1} x_i^1\rho\sigma' = x^1\sigma$ $(1 \leq i \leq \ell)$ and the following equation $(\star)$

$$\begin{array}{c} \mathsf{E} \models (U\{X_1 \mapsto R^1\})\{X_1^1 \mapsto M_1^1, \dots, X_\ell^1 \mapsto M_\ell^1, X_2 \mapsto M_2, \dots, X_k \mapsto M_k\} \\ \sim \\ (V\{X_1 \mapsto R^1\})\{X_1^1 \mapsto M_1^1, \dots, X_\ell^1 \mapsto M_\ell^1, X_2 \mapsto M_2, \dots, X_k \mapsto M_k\} \end{array}$$

We choose $R_1 = R^1\{X_1^1 \mapsto M_1^1, \dots, X_\ell^1 \mapsto M_\ell^1\}$ and $R_2 = M_2, \dots, R_k = M_k$. Thus, the equation $(\star)$ can be rewritten as follows:

$$\mathsf{E} \models U\{X_1 \mapsto R_1, \dots, X_k \mapsto R_k\} \sim V\{X_1 \mapsto R_1, \dots, X_k \mapsto R_k\}.$$

This allows us to conclude. □

Proposition 1 (completeness, equation). *Let (F, E) be a saturated knowledge base, and M, N be two terms such that $\mathsf{F} \vdash^M t$ and $\mathsf{F} \vdash^N t$ for some ground term t. Then, we have that $\mathsf{E} \models M \sim N$.*

Proof. By definition of $\mathsf{F} \vdash^M t$ we know that there exist a substitution σ_1 and a deduction fact $\mathsf{f}_1 = [M_0 \rhd u_0 \mid X_1 \rhd x_1, \dots, X_k \rhd x_k]$ in F such that $u_0\sigma_1 = t$, $\mathsf{F} \vdash^{M_i} x_i\sigma_1$ $(1 \leq i \leq k)$ and $M_0\{X_i \mapsto M_i\}_{1 \leq i \leq k} = M$. Similarly, by definition of $\mathsf{F} \vdash^N t$ we know that there exist a substitution σ_2 and a deduction fact $\mathsf{f}_2 = [N_0 \rhd v_0 \mid Y_1 \rhd y_1, \dots, Y_\ell \rhd y_\ell]$ in F such that $v_0\sigma_2 = t$, $\mathsf{F} \vdash^{N_j} y_j\sigma_2$ $(1 \leq j \leq \ell)$ and $N_0\{Y_j \mapsto N_j\}_{1 \leq i \leq \ell} = N$.

We prove the result by induction on $|t|$. As our knowledge base (F, E) is saturated, rule $\mathsf{Unifying}$ must have been applied to the facts f_1 and f_2. Therefore, we have that there exists an equational fact $\mathsf{f}_3 \in \mathsf{E}$ such that:

$$\mathsf{f}_3 = [M_0 \sim N_0 \mid X_1 \rhd x_1\sigma, \dots, X_k \rhd x_k\sigma, Y_1 \rhd y_1\sigma, \dots, Y_\ell \rhd y_\ell\sigma].$$

where $\sigma = mgu(u_0, v_0)$.

Let σ' be a substitution such that $\sigma_1 \cup \sigma_2 = \sigma \circ \sigma'$. We can now apply Lemma 2 on f_3 with substitution σ'. We obtain that there exist $R_1, \dots, R_k$ and $W_1, \dots, W_\ell$ such that $\mathsf{F} \vdash^{R_i} x_i\sigma\sigma'$ $(1 \leq i \leq k)$ and $\mathsf{F} \vdash^{W_j} y_j\sigma\sigma'$ $(1 \leq j \leq \ell)$ and such that

$$\mathsf{E} \models M_0\delta \sim N_0\delta \tag{1}$$

where $\delta = \{X_1 \mapsto R_1, \dots, X_k \mapsto R_k, Y_1 \mapsto W_1, \dots, Y_\ell \mapsto W_\ell\}$.

As M_i and R_i $(1 \leq i \leq k)$ are such that $\mathsf{F} \vdash^{M_i} x_i\sigma_1$ and $\mathsf{F} \vdash^{R_i} x_i\sigma\sigma'$, and as $x_1\sigma\sigma' = x_1\sigma_1$ is a strict subterm of $u_0\sigma_1 = t$, we can apply the induction hypothesis to obtain that $\mathsf{E} \models M_i \sim R_i$. In a similar way, we also deduce that $\mathsf{E} \models N_j \sim W_j$ $(1 \leq j \leq \ell)$. By replacing W_j by M_j and R_i by N_i in equation (1), we obtain our conclusion. □

Lemma 6. *Let* (F,E) *be a knowledge base and* t *be a term in* $\mathcal{T}(\mathcal{F},\mathcal{N}\cup\mathcal{X})$. *Let* σ *be a grounding substitution for* t. *If* $\mathsf{F}\vdash^{W} t$ *and* $\mathsf{F}\vdash^{R_x} x\sigma$ *for every* $x\in \mathrm{var}(t)$, *then* $\mathsf{F}\vdash^{W'} t\sigma$ *where* $W' = W\{x\mapsto R_x\}_{x\in\mathrm{var}(t)}$.

Proof. We show this result by induction on $|t|$.
Base case: $|t| = 0$*, i.e.* t *is a variable, say* x. As $\mathsf{F}\vdash^{W} t$, it follows that $W = t = x$. By hypothesis, there exists R such that $\mathsf{F}\vdash^{R} x\sigma = t\sigma$. This allows us to conclude.

Induction case: $|t| > 0$. As $\mathsf{F}\vdash^{W} t$, it follows that there exist a fact $\mathsf{f}\in\mathsf{F}$ and a substitution τ such that:

- $\mathsf{f} = [R \rhd u \mid X_1 \rhd x_1,\ldots,X_k\rhd x_k]$;
- $t = u\tau$;
- $\mathsf{F}\vdash^{R_i} x_i\tau$ for every $1\le i\le k$ and $W = R\{X_1\mapsto R_1,\ldots,X_k\mapsto R_k\}$.

We have that $\mathrm{var}(u) = \{x_1,\ldots,x_k\}$ and thus, $x_i\tau$ is a strict subterm of $u\tau$ $(1\le i\le k)$. Therefore, we can apply our induction hypothesis on each term $x_i\tau$ with the substitution σ. For each i such that $1\le i\le k$, we obtain that:

$$\mathsf{F}\vdash^{W_i} x_i\tau\sigma \text{ where } W_i = R_i\{x\mapsto R_x\}_{x\in\mathrm{var}(x_i\tau)}.$$

Note that since $t = u\tau$ and $\mathrm{var}(u) = \{x_1,\ldots,x_k\}$, we have that $\mathrm{var}(t) = \mathrm{var}(\{x_1\tau,\ldots,x_k\tau\})$. By using the fact f, we get that $\mathsf{F}\vdash^{W''} u\tau\sigma$ where

$$\begin{aligned} W'' &= R\{X_1\mapsto R_1\{x\mapsto R_x\}_{x\in\mathrm{var}(t)},\ldots,X_k\mapsto R_k\{x\mapsto R_x\}_{x\in\mathrm{var}(t)}\} \\ &= (R\{X_1\mapsto R_1,\ldots,X_k\mapsto R_k\})\{x\mapsto R_x\}_{x\in\mathrm{var}(t)} \\ &= W\{x\mapsto R_x\}_{x\in\mathrm{var}(t)} \end{aligned}$$

Let $W' = W\{x\mapsto R_x\}_{x\in\mathrm{var}(t)}$, we have that $\mathsf{F}\vdash^{W'} u\tau\sigma$ and since $u\tau\sigma = t\sigma$ we easily conclude. ☐

Lemma 7. *Let* $\mathsf{f} = [R\rhd t \mid X_1\rhd x_1,\ldots,X_k\rhd x_k]$ *be a solved fact and* (F,E) *be a knowledge base such that* $(\mathsf{F},\mathsf{E})\oplus\mathsf{f} = (\mathsf{F},\mathsf{E})$. *Let* σ *be a substitution grounding for* $\{x_1,\ldots,x_k\}$ *such that* $\mathsf{F}\vdash x_i\sigma$ *$(1\le i\le k)$. Then there exist* W *and* R_i *$(1\le i\le k)$ such that:*

- $\mathsf{F}\vdash^{W} t\sigma$*, and* $\mathsf{F}\vdash^{R_i} x_i\sigma$ *for every* $1\le i\le k$*;*
- $\mathsf{E}\models W\sim R\{X_1\mapsto R_1,\ldots,X_k\mapsto R_k\}$.

Proof. Let f' be the canonical form of f. We first show that $\mathsf{F}\cup\{\mathsf{f}'\} = \mathsf{F}$ implies $\mathsf{F}\vdash t$. This is easily shown by induction on the number of steps to compute the canonical form.

Base case: If f is already in canonical form we have that $\mathsf{f} = \mathsf{f}'$ and hence $\mathsf{F}\vdash t$.
Inductive case: The two rules are of the form

$$\frac{[R\rhd t \mid X_1\rhd x_1,\ldots,X_k\rhd x_k]}{\mathsf{f}_0 = [R'\rhd t\mid X_1\rhd x_1,\ldots,X_{i-1}\rhd x_{i-1},X_{i+1}\rhd x_{i+1},\ldots,X_k\rhd x_k]}$$

Let f_0' be the canonical form of f_0. By induction hypothesis we have $\mathsf{F}\cup\{\mathsf{f}_0'\} = \mathsf{F}$ implies $\mathsf{F}\vdash t$. As $\mathsf{f}' = \mathsf{f}_0'$ we conclude.

To prove the lemma we consider both cases where f is either useful or useless.

$\mathsf{Useful\ fact}$: If f is useful we have that $\mathsf{F} \vdash t$. By what we have just shown, $\mathsf{F} \cup \{\mathsf{f}'\} \neq \mathsf{F}$ which contradicts that $(\mathsf{F}, \mathsf{E}) \oplus \mathsf{f} = (\mathsf{F}, \mathsf{E})$. Hence, this case is impossible.

$\mathsf{Useless\ fact}$: Since $(\mathsf{F}, \mathsf{E}) \oplus \mathsf{f} = (\mathsf{F}, \mathsf{E})$, it follows that there exists W' such that $\mathsf{F} \vdash^{W'} t$ and $\mathsf{E} \models W' \sim R\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\}$. We choose R_i arbitrarily such that $\mathsf{F} \vdash^{R_i} x_i\sigma$. Let $W'' = W'\{x_1 \mapsto R_1, \ldots, x_k \mapsto R_k\}$. Thanks to Lemma 6, we deduce that $\mathsf{F} \vdash^{W''} t\sigma$ and we also have that

$$\mathsf{E} \models (W' \sim R\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\})\{x_1 \mapsto R_1, \ldots, x_k \mapsto R_k\},$$

i.e. $\mathsf{E} \models W'' \sim R\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\}$.

Let $W = W''$. We have that $\mathsf{F} \vdash^{W} t\sigma$, and $\mathsf{F} \vdash^{R_i} x_i\sigma$ for every $1 \leq i \leq k$. Lastly, we have that $\mathsf{E} \models W \sim R\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\}$. $\square$

Lemma 3. *Let (F, E) be a saturated knowledge base. Let $\mathsf{f} = [R \rhd t \mid X_1 \rhd t_1, \ldots, X_k \rhd t_k]$ be a deduction fact such that $(\mathsf{F}, \mathsf{E}) \oplus \mathsf{f} = (\mathsf{F}, \mathsf{E})$. For any substitution σ grounding for $\{t_1, \ldots, t_k\}$ such that $\mathsf{F} \vdash t_i\sigma$ $(1 \leq i \leq k)$, we have that there exist $R_1, \ldots, R_k$ and W such that*

- *$\mathsf{F} \vdash^{W} t\sigma$, and $\mathsf{F} \vdash^{R_i} t_i\sigma$ for $1 \leq i \leq k$;*
- *$\mathsf{E} \models W \sim R\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\}$.*

Proof. We show the result by induction on $\sum_{i=1}^{k} |t_i\sigma|$. We distinguish two cases. If f is solved then we easily conclude by applying Lemma 7.

If f is not solved, there exists j such that $t_j \notin \mathcal{X}$. We assume w.l.o.g. that $j = 1$. Since $\mathsf{F} \vdash t_1\sigma$, there exist a solved deduction fact $\mathsf{f}' \in \mathsf{F}$, some terms $R'_i (1 \leq i \leq \ell)$ and a substitution τ such that:

- $\mathsf{f}' = [R' \rhd t' \mid Y_1 \rhd y_1, \ldots, Y_\ell \rhd y_\ell]$;
- $t'\tau = t_1\sigma$;
- $\mathsf{F} \vdash^{R'_i} y_i\tau$ for every $1 \leq i \leq \ell$.

By application of the $\mathsf{F\text{-}Solving}$ rule to the deduction facts f and f', we obtain the following fact f_0:

$$\mathsf{f}_0 = [R\{X_1 \mapsto R'\} \rhd t\rho \mid X_2 \mapsto t_2\rho, \ldots, X_k \mapsto t_k\rho, Y_1 \mapsto y_1\rho, \ldots, Y_\ell \mapsto y_\ell\rho]$$

where $\rho = mgu(t', t_1)$.

As (F, E) is saturated, $(\mathsf{F}, \mathsf{E}) \oplus \mathsf{f}_0 = (\mathsf{F}, \mathsf{E})$. Let σ' be the substitution such that $\sigma \cup \tau = \rho \circ \sigma'$. As $y_i\rho\sigma' = y_i(\sigma \cup \tau) = y_i\tau$ are strict disjoint subterms of $t'\tau = t_1\sigma$, it follows that we can apply our induction hypothesis on f_0 and the substitution σ'. Therefore, there exist $R'_2, \ldots, R'_k, R^y_1, \ldots, R^y_\ell$ and W' such that:

- $\mathsf{F} \vdash^{W'} t\rho\sigma'$,

– $\mathsf{F} \vdash^{R'_i} t_i\rho\sigma'$ for every $2 \le i \le k$;
– $\mathsf{F} \vdash^{R^y_j} y_j\rho\sigma'$ for every $1 \le j \le \ell$;
– $\mathsf{E} \models W' \sim (R\{X_1 \mapsto R'\})\{X_2 \mapsto R'_2, \ldots, X_k \mapsto R'_k, Y_1 \mapsto R^y_1, \ldots, Y_\ell \mapsto R^y_\ell\}$.

Let $W = W'$, $R_1 = R'\{Y_1 \mapsto R^y_1, \ldots, Y_\ell \mapsto R^y_\ell\}$, $R_j = R'_j$ for every $2 \le j \le k$. It immediately follows that $\mathsf{E} \models W \sim R\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\}$, $\mathsf{F} \vdash^W t\sigma$, and $\mathsf{F} \vdash^{R_i} t_i\sigma$ for $1 \le i \le k$. This allows us to conclude. □

Proposition 2 (completeness, reduction). *Let (F, E) be a saturated knowledge base, M a term and t a ground term such that $\mathsf{F} \vdash^M t$ and $t\downarrow_{\mathcal{R}_\mathcal{E}} \ne t$. Then there exists M' and t' such that $\mathsf{F} \vdash^{M'} t'$ with $t \to^+_{\mathcal{R}_\mathcal{E}} t'$ and $\mathsf{E} \models M \sim M'$.*

Proof. We show this result by induction on $|t|$. By definition of $\mathsf{F} \vdash^M t$ we know that there exist $\mathsf{f}_0 = \{M_0 \rhd u_0 \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k\}$ in F and a substitution σ such that $u_0\sigma = t$ and $\mathsf{F} \vdash^{M_i} x_i\sigma$ $(1 \le i \le k)$ and $M_0\{X_i \mapsto M_i\}_{1 \le i \le k} = M$ for some M_i $(1 \le i \le k)$. We distinguish two cases:

Case 1: there exists $1 \le j \le k$ such that $x_j\sigma\downarrow_{\mathcal{R}_\mathcal{E}} \ne x_j\sigma$. Let us assume w.l.o.g. that $j = 1$. Since $x_1\sigma$ is a strict subterm of t, we can apply our induction hypothesis on $x_1\sigma$. We obtain that there exist M'_1 and u'_1 such that $\mathsf{F} \vdash^{M'_1} u'_1$ with $x_1\sigma \to^+_{\mathcal{R}} u'_1$ and $\mathsf{E} \models M_1 \sim M'_1$. Now, let σ' be the substitution defined as follows:

$$x\sigma' = \begin{cases} x\sigma \text{ for } x \ne x_1 \\ u'_1 \text{ otherwise} \end{cases}$$

Let $t' = u_0\sigma'$ and $M' = M_0\{X_1 \mapsto M'_1, X_2 \mapsto M_2, \ldots, X_k \mapsto M_k\}$. Since $x_1 \in \mathrm{var}(u_0)$, it is easy to see that $t = u_0\sigma \to^+_{\mathcal{R}} u_0\sigma' = t'$. Furthermore, it is also easy to see that $\mathsf{F} \vdash^{M'} t'$. Lastly, since $\mathsf{E} \models M_1 \sim M'_1$, we have that $\mathsf{E} \models M \sim M'$.

Case 2: $x_j\sigma\downarrow_{\mathcal{R}_\mathcal{E}} = x_j\sigma$ for every $1 \le j \le k$. In such a case, we have that $u_0 = C[u'_0]$ for some context C and some term $u'_0 \notin \mathcal{X}$ such that $u'_0\sigma = l\tau$ where $l \to r \in \mathcal{R}$ and τ is a substitution. As the knowledge base (F, E) is saturated, the rule $\mathsf{Narrowing}$ must have been applied. Therefore there exists f_1 such that:

– $(\mathsf{F}, \mathsf{E}) \oplus \mathsf{f}_1 = (\mathsf{F}, \mathsf{E})$, and
– $\mathsf{f}_1 = [M_0 \rhd (C[r])\rho \mid X_1 \rhd x_1\rho, \ldots, X_k \rhd x_k\rho]$

where $\rho = \mathrm{mgu}(u'_0, l)$. Let ρ' be the substitution with $\mathrm{dom}(\rho') = \mathrm{var}(\{x_1\rho, \ldots, x_k\rho\})$ and $\sigma \cup \tau = \rho \circ \rho'$. Now, we apply Lemma 3 on the fact f_1 and the substitution ρ'. We deduce that there exists $R_1, \ldots, R_k$ and W such that

– $\mathsf{F} \vdash^W (C[r])\rho\rho'$, and $\mathsf{F} \vdash^{R_i} x_i\rho\rho'$ for $1 \le i \le k$; and
– $\mathsf{E} \models W \sim M_0\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\}$.

Let $t' = (C[r])\rho\rho'$ and $M' = W$. We have that $\mathsf{F} \vdash^{M'} t'$. Moreover, since $\mathsf{F} \vdash^{R_i} x_i\rho\rho'$, $\mathsf{F} \vdash^{M_i} x_i\sigma$ and $x_i\rho\rho' = x_i\sigma$, we can apply Lemma 1 in order to deduce that $\mathsf{E} \models R_1 \sim M_i$ for $1 \le i \le k$. Thus, we have that $\mathsf{E} \models M \sim M'$. In order to conclude, it remains to show that $t \to^+_{\mathcal{R}_\mathcal{E}} t'$. Indeed, we have that $t = u_0\sigma = (C[u'_0])\sigma \to^+_{\mathcal{R}_\mathcal{E}} (C[r])\rho\rho' = t'$. □

A.3 Proof of Theorem 1

Theorem 1 (soundness and completeness). *Let φ be a frame and (F, E) be a saturated knowledge base such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. *Let $t \in \mathcal{T}(\mathcal{F}, \mathcal{N})$ and* $\mathsf{F}^+ = \mathsf{F} \cup \{[n \rhd n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$. *We have that:*

1. *For all $M \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi))$ such that $\mathrm{fn}(M) \cap \mathrm{bn}(\varphi) = \emptyset$, we have that*
$$M\varphi =_{\mathcal{E}} t \Leftrightarrow \exists N,\ \mathsf{E} \models M \sim N \text{ and } \mathsf{F}^+ \vdash^N t{\downarrow_{\mathcal{R}_\mathcal{E}}}$$
2. *For all $M, N \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi))$ such that $\mathrm{fn}(M, N) \cap \mathrm{bn}(\varphi) = \emptyset$, we have*
$$(M =_{\mathcal{E}} N)\varphi \ \Leftrightarrow\ \mathsf{E} \models M \sim N.$$

Proof. Let φ be a frame and (F, E) be a saturated knowledge base such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$.

1.($\Leftarrow$) Let M, N and t be such that $\mathsf{E} \models M \sim N$ and $\mathsf{F}^+ \vdash^N t{\downarrow_{\mathcal{R}_\mathcal{E}}}$. Thanks to Lemma 1, we have that $M\varphi =_{\mathcal{E}} N\varphi =_{\mathcal{E}} t$.

($\Rightarrow$) Let M and t be such that $M\varphi =_{\mathcal{E}} t$.

Let $\mathsf{F}^{++} = \mathsf{F} \cup \{[n \rhd n] \mid n \in \mathrm{fn}(M)\}$. We have that $\mathsf{F}^{++} \vdash^M t_0$ and $t_0 \to^* t{\downarrow_{\mathcal{R}_\mathcal{E}}}$ with $t_0 = M\varphi$.

Let $\{n_1, \ldots, n_\ell\} = \mathrm{fn}(M) \smallsetminus \mathrm{fn}(\varphi \cup \{t\})$. Let $y_1, \ldots, y_\ell$ be fresh variables and $\delta = \{n_1 \mapsto y_1, \ldots, n_\ell \mapsto y_\ell\}$. Let $M' = M\delta$. We have that $\mathsf{F}^{++} \vdash^{M'} t'_0$ and $t'_0 \to^* t{\downarrow_{\mathcal{R}_\mathcal{E}}}$ with $t'_0 = M'\varphi$.

Now, let $\mathsf{E}^{++} = \mathsf{E} \cup \{[n \sim n] \mid n \in \mathrm{fn}(M)\}$. As (F, E) is a saturated knowledge base, we have that $(\mathsf{F}^{++}, \mathsf{E}^{++})$ is a saturated knowledge base as well. Now thanks to Proposition 1, we deduce that $\mathsf{E}^{++} \models M \sim M'$, thus $\mathsf{E} \models M \sim M'$ as well.

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: $\mathsf{F}^+ \vdash^{M'} t_0 = t{\downarrow_{\mathcal{R}_\mathcal{E}}}$. Let $N = M'$, we have $\mathsf{E} \models M \sim N$ and $\mathsf{F} \vdash^N t{\downarrow_{\mathcal{R}_\mathcal{E}}}$.

Induction case: $\mathsf{F}^+ \vdash^{M'} t_0$ *with* $t_0 \neq t{\downarrow_{\mathcal{R}_\mathcal{E}}}$. Let $\mathsf{E}^+ = \mathsf{E} \cup \{[n \sim n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$. We easily see that as (F, E) is a saturated knowledge base we have that $(\mathsf{F}^+, \mathsf{E}^+)$ is a saturated knowledge base as well. Hence we can apply Proposition 2 and deduce that there exist N' and t' such that $\mathsf{F}^+ \vdash^{N'} t'$, $t \to^+_{\mathcal{R}_\mathcal{E}} t'$, and $\mathsf{E}^+ \models M' \sim N'$. It is easy to see that $\mathsf{E} \models M' \sim N'$ as well. We have that $\mathsf{F}^+ \vdash^{N'} t' \to^* t{\downarrow_{\mathcal{R}_\mathcal{E}}}$ and $t' < t_0$. Thus, we can apply our induction hypothesis and we obtain that there exists N such that $\mathsf{E} \models N' \sim N$ and $\mathsf{F}^+ \vdash^N t{\downarrow_{\mathcal{R}_\mathcal{E}}}$.

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

($\Rightarrow$) Let M and N such that $M\varphi =_{\mathcal{E}} N\varphi$. This means that there exists t such that $M\varphi =_{\mathcal{E}} t$ and $N\varphi =_{\mathcal{E}} t$. Let $\mathsf{F}^+ = \mathsf{F} \cup \{[n \rhd n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$ and $\mathsf{E}^+ = \mathsf{E} \cup \{[n \sim n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$. By applying 1, we deduce that there exists M', N' such that $\mathsf{E} \models M \sim M'$, $\mathsf{F}^+ \vdash^{M'} t{\downarrow_{\mathcal{R}_\mathcal{E}}}$, $\mathsf{E} \models N \sim N'$ and $\mathsf{F}^+ \vdash^{N'} t{\downarrow_{\mathcal{R}_\mathcal{E}}}$. It is easy to see that $\mathsf{E}^+ \models M \sim M'$ and $\mathsf{E}^+ \models N \sim N'$ as well. Because $(\mathsf{F}^+, \mathsf{E}^+)$ is a saturated knowledge base we apply Proposition 1 and deduce that $\mathsf{E}^+ \models M' \sim N'$, and thus $\mathsf{E}^+ \models M \sim N$, which easily implies $\mathsf{E} \models M \sim N$. $\square$

A.4 Application to deduction and static equivalence

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

1. Apply the saturation rules to obtain (if any) a saturated knowledge base (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. Let $\mathsf{F}^+ = \mathsf{F} \cup \{[n \rhd n] \mid n \in \mathrm{fn}(t) \smallsetminus \mathrm{bn}(\varphi)\}$.
2. Return *yes* if there exists N such that $\mathsf{F}^+ \vdash^N t{\downarrow}_{\mathcal{R}_\mathcal{E}}$ (that is, the $\mathcal{R}_\mathcal{E}$-normal form of t is generated by F with recipe N); otherwise return *no*.

Proof. If the algorithm returns *yes*, there exists N such that $\mathsf{F}^+ \vdash^N t{\downarrow}_{\mathcal{R}_\mathcal{E}}$. As $\mathsf{E} \models N \sim N$, by Theorem 1 we have that $N\varphi =_{\mathcal{E}} t{\downarrow}_{\mathcal{R}_\mathcal{E}}$, *i.e.*, $\varphi \vdash_{\mathcal{E}} t$. Conversely, if t is deducible from φ, then there exists M such that $M\varphi =_{\mathcal{E}} t$. By Theorem 1, there exists N such that $\mathsf{F}^+ \vdash^N t{\downarrow}_{\mathcal{R}_\mathcal{E}}$. Hence, the algorithm returns *yes*. $\square$

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

1. Apply the transformation rules to obtain (if possible) two saturated knowledge bases $(\mathsf{F}_i, \mathsf{E}_i)$, $i = 1, 2$ such that $\mathrm{Init}(\varphi_i) \Longrightarrow^* (\mathsf{F}_i, \mathsf{E}_i)$, $i = 1, 2$.
2. For $\{i, j\} = \{1, 2\}$, for every solved fact $[M \sim N \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k]$ in E_i, check if $(M\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\} =_{\mathcal{E}} N\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\})\varphi_j$.
3. If so return *yes*; otherwise return *no*.

Proof. If the algorithm returns *yes*, this means that ($\star$): for every solved equational fact $[M \sim N \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k]$ in E_1, we have that:

$$(M\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\} =_{\mathcal{E}} N\{X_1 \mapsto x_1, \ldots X_k \mapsto x_k\})\varphi_2.$$

Let $M, N \in \mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathrm{dom}(\varphi))$ such that $\mathrm{fn}(M, N) \cap \tilde{n} = \emptyset$ and $(M =_{\mathcal{E}} N)\varphi_1$. Thanks to Theorem 1, we have that $\mathsf{E}_1 \models M \sim N$. Thanks to ($\star$), we deduce that $(M =_{\mathcal{E}} N)\varphi_2$. The other direction is proved in the same way.

Conversely, assume now that $\varphi_1 \approx_{\mathcal{E}} \varphi_2$. Let $[M \sim N \mid X_1 \rhd x_1, \ldots, X_k \rhd x_k]$ be a solved equational fact in E_1 and let us show that $(\tilde{M} =_{\mathcal{E}} \tilde{N})\varphi_2$ where

- $\tilde{M} = M\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\}$, and
- $\tilde{N} = N\{X_1 \mapsto x_1, \ldots, X_k \mapsto x_k\}$.

(The other case is done in a similar way, and we will conclude that the algorithm returns *yes*.) Let $\{y_1, \ldots, y_\ell\} = \mathrm{var}(M, N)$ and $n_1, \ldots, n_\ell$ be ℓ fresh names that occur neither in $\tilde{n} \cup \mathrm{fn}(M, N)$, nor in φ. Let $\delta = \{y_1 \mapsto n_1, \ldots, y_\ell \mapsto n_\ell\}$. Since $\mathsf{E}_1 \models \tilde{M} \sim \tilde{N}$, we have also that $\mathsf{E}_1 \models \tilde{M}\delta \sim \tilde{N}\delta$. Clearly, we have that $\mathrm{fn}(\tilde{M}\delta, \tilde{N}\delta) \cap \tilde{n} = \emptyset$, thus by Theorem 1, we have that $(\tilde{M}\delta =_{\mathcal{E}} \tilde{N}\delta)\varphi_1$. As $\varphi_1 \approx_{\mathcal{E}} \varphi_2$, we have also that $(\tilde{M}\delta =_{\mathcal{E}} \tilde{N}\delta)\varphi_2$, and thus $(\tilde{M} =_{\mathcal{E}} \tilde{N})\varphi_2$. This allows us to conclude. $\square$

B Proofs of Section 5

B.1 Generic method for proving termination

Proposition 3 (generic termination). *The saturation algorithm terminates if $\oplus$ is uniform and there exist some functions $\mathcal{Q}$, $\mathsf{m_f}$, $\mathsf{m_e}$ and some well-founded orders $<_\mathsf{f}$ and $<_\mathsf{e}$ such that for all frame φ, and for all (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$, we have that:*

1. $\{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}$ *and* f *is a solved deduction fact*$\} \subseteq \mathcal{Q}(\varphi)$ *and* $\mathcal{Q}(\varphi)$ *is finite;*
2. $\mathsf{m_f}(\mathsf{f}_0) <_\mathsf{f} \mathsf{m_f}(\mathsf{f}_1)$ *where* f_0, f_1 *are defined as in rule F-Solving;*
3. $\mathsf{m_e}(\mathsf{f}_0) <_\mathsf{e} \mathsf{m_e}(\mathsf{f}_1)$ *where* f_0, f_1 *are defined as in rule E-Solving.*

Proof. A *solved deduction fact* f is only added to F if there is no $\mathsf{f}' \in \mathsf{F}$ such that $\hat{\mathsf{f}} = \hat{\mathsf{f}}'$. Indeed, if $\hat{\mathsf{f}} = \hat{\mathsf{f}}'$ then $\hat{\mathsf{f}}$ is useless and an equational fact will be added instead. As $\{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}$ and f is a solved deduction fact$\} \subseteq \mathcal{Q}(\varphi)$ and $\mathcal{Q}(\varphi)$ is finite we conclude that only a finite number of solved deduction facts can be added.

An *unsolved deduction fact* f can be added in two ways.

- f can be added by the rule Narrowing. Since the number of solved deduction facts and the number of rewriting rules are finite the number of facts added by the rule Narrowing is bounded.
- f can be added by the rule F-Solving. The number of facts added by the rule F-Solving is bounded by the measure $\mathsf{m_f}$ which is strictly decreasing for a well-founded order.

An *equational fact* f can be added in three ways.

- f can be added when the knowledge base is updated with a useless deduction fact. However, since $\oplus$ is uniform only a finite number of such facts is added.
- f can be added by the rule Unifying. Since the number of solved deduction facts is finite, the number of facts added by Unifying is bounded.
- f can be added by the rule E-Solving. The number of facts added by rule E-Solving is bounded by the measure $\mathsf{m_e}$ which is strictly decreasing for a well-founded order.

Altogether, this allows us to conclude. □

B.2 Subterm convergent equational theories

Lemma 8. *Let $\mathcal{E}$ be a subterm convergent equational theory and $\mathcal{R}_\mathcal{E}$ be its associated rewrite system. For any frame φ, and any (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow (\mathsf{F}, \mathsf{E})$, we have that:*

1. $\{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}$ *and* f *is a solved deduction fact*$\} \subseteq \mathcal{Q}(\varphi)$ *and* $\mathcal{Q}(\varphi)$ *is finite;*

2. $\mathsf{m_f}(\mathsf{f}_0) <_\mathsf{f} \mathsf{m_f}(\mathsf{f}_1)$ *where* f_0, f_1 *are defined as in rule* F-Solving;
3. $\mathsf{m_e}(\mathsf{f}_0) <_\mathsf{e} \mathsf{m_e}(\mathsf{f}_1)$ *where* f_0, f_1 *are defined as in rule* E-Solving

where $\mathcal{Q}$, $\mathsf{m_f}$, $\mathsf{m_e}$, $<_\mathsf{f}$, *and* $<_\mathsf{e}$ *are defined w.r.t. the rewrite system* $\mathcal{R}_\mathcal{E}$ *as described in Section 5.2.*

Proof. The proof of item 1 is done by induction on the number of saturation steps needed to reach (F, E). To ease the induction we strengthen the induction hypothesis and prove a slightly stronger statement. We define $\mathcal{Q}'(\varphi, \mathsf{F})$ as the smallest set such that

1. $[t \mid \emptyset] \in \mathcal{Q}'(\varphi, \mathsf{F})$, where $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
2. $[f(x_1, \ldots, x_k) \mid x_1, \ldots, x_k] \in \mathcal{Q}'(\varphi, \mathsf{F})$, where $ar(f) = k$
3. $[r\sigma \mid t_1, \ldots, t_k] \in \mathcal{Q}'(\varphi, \mathsf{f})$, where:
   - $l \to r \in \mathcal{R}_\mathcal{E}$
   - $\sigma : \mathrm{var}(l) \to \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ is a partial function
   - $l\sigma = C[t_1, \ldots, t_k]$ for some context C
   - $r\sigma \in \mathrm{st}(D[t_1, \ldots, t_k, u_1, \ldots, u_n])$ for some public context D and some terms u_i such that $[u_i \mid \emptyset] \in \hat{\mathsf{F}}$
   - $\exists i : t_i \notin \mathcal{X}$

In the following when a projection $\hat{\mathsf{f}}$ corresponds to one of the above 3 cases, we say that f is of type i ($1 \leq i \leq 3$). Note that a solved deduction fact is either of type 1 or 2. We prove that for any (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$ we have that $\hat{\mathsf{F}} \subseteq \mathcal{Q}'(\varphi, \mathsf{F})$. We have that $\{\hat{\mathsf{f}} \mid \hat{\mathsf{f}} \in \mathcal{Q}'(\varphi, \mathsf{F}) \text{ and } \hat{\mathsf{f}} \text{ is solved}\} \subseteq \mathcal{Q}(\varphi)$ and this allows us to conclude. We prove the result by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$.

Base case. It is clear that for all deduction facts $\mathsf{f} \in \mathrm{Init}(\varphi)$ we have that $\hat{\mathsf{f}}$ is either of type 1 or type 2.

Inductive case. We assume that the result holds for (F, E), i.e. $\hat{\mathsf{F}} \subseteq \mathcal{Q}'(\varphi, \mathsf{F})$, and show that any possible application of a saturation rule preserves the result.

1. Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 1, i.e. $\hat{\mathsf{f}} = [t \mid \emptyset]$. By applying rule Narrowing to it, we obtain a fact f' such that $\hat{\mathsf{f}'} = [t' \mid \emptyset]$ with $t \to_{\mathcal{R}_\mathcal{E}} t'$. As $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$, we have that $t' \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ and therefore f' is of type 1.
2. Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 2, i.e. $\hat{\mathsf{f}} = [f(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$. As all positions of the term $f(x_1, \ldots, x_k)$, except the head are variables, rule Narrowing can only be applied at this position. Let $l \to r \in \mathcal{R}_\mathcal{E}$ be the rewrite rule involved in this step. We obtain a fact f' such that $\hat{\mathsf{f}'} = [r\tau \mid x_1\tau, \ldots, x_k\tau]$ where $\tau = \mathrm{mgu}(f(x_1, \ldots, x_k), l)$. We distinguish two cases:
   - *Case 1: l is a variable, say x.* In such a case, $\hat{\mathsf{f}'} = [r\tau \mid x_1, \ldots, x_k]$ and $r \in \mathcal{T}(\mathcal{F}, \emptyset)$. Therefore, the resulting fact f' is useless.
   - *Case 2: l is not a variable.* In such a case, we have that $l = f(l_1, \ldots, l_k)$ and $\hat{\mathsf{f}'} = [r \mid l_1, \ldots, l_k]$. Let σ be such that $\mathrm{dom}(\sigma) = \emptyset$, $C = f(\_, \ldots, \_)$. It is clear that $\hat{\mathsf{f}'}$ satisfies the three first conditions of a fact of type 3. Now, either $r \in \mathcal{T}(\mathcal{F}, \emptyset)$, i.e. r is a public ground term and in such a case

it is clear that the fact is useless. Otherwise, we have that r is a strict subterm of l, i.e $r \in \mathrm{st}(l_j)$ for some $1 \leq j \leq k$. Therefore the fourth condition also holds. Now, assume that all the l_i are variables (i.e. f' is solved), we show it is useless and it is not added to the knowledge base. Indeed, in such a situation, we necessarily have that r is a variable (remember that $r \in \mathrm{st}(l_j)$) and therefore the fact f' is useless.

3. Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 3. Let $\hat{\mathsf{f}} = [r\sigma \mid t_1, \ldots, t_k]$. In such a case, there exist a rewrite rule $l \to r$, a partial function $\sigma : \mathrm{var}(l) \to \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$, a context C such that $l\sigma = C[t_1, \ldots, t_k]$ and we have that $r\sigma \in \mathrm{st}(D[t_1, \ldots, t_k, u_1, \ldots, u_n])$ for some public context D and some terms u_i such that $[u_i \mid \emptyset] \in \hat{\mathsf{F}}$. Assume that one of the side conditions of f is being solved by rule F-Solving with a solved fact $\mathsf{f}' \in \mathsf{F}$. We assume w.l.o.g. that t_1 is being solved. We distinguish two cases depending on the type of f'.
   - *Case 1:* $\hat{\mathsf{f}}' = [u_0 \mid \emptyset]$. Let $\tau = \mathrm{mgu}(u_0, t_1)$. The fact resulting from the F-Solving rule is $\mathsf{f}'' = [r\sigma\tau \mid t_2\tau, \ldots, t_k\tau]$. We consider $\sigma' = \tau \cup \sigma$, $C' = C[u_0, \ldots, \_]$ and $D' = D$. We can show that the first four conditions hold. If the last condition does not hold, and because the fourth holds, the resulting fact must be either of type 1 or useless and therefore not added to the knowledge base.
   - *Case 2:* $\hat{\mathsf{f}}' = [f(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$. Let $\tau = \mathrm{mgu}(f(x_1, \ldots, x_k), t_1)$. As t_1 is not a variable, we have that $t_1 = f(s_1, \ldots, s_\ell)$. The fact resulting from the application of the rule F-Solving is $\mathsf{f}'' = [r\sigma \mid s_1, \ldots, s_\ell, t_2, \ldots, t_k]$. We can show that the first four conditions hold. If the last condition does not hold, and because the fourth holds, the resulting fact must be either of type 1 or useless and therefore not added to the knowledge base.

To show items 2 and 3 it remains to be proven that $\mathsf{m_f}$ and $\mathsf{m_e}$ strictly decrease after a side condition of an unsolved fact is solved. As a side condition can only be solved by facts of type 1 or 2 this is easily shown by a case analysis. We detail the proof for $\mathsf{m_f}$. The case of $\mathsf{m_e}$ can be done in a similar way.
Let $\mathsf{f}_1 = [R \rhd t \mid X_1 \rhd t_1, \ldots X_n \rhd t_n]$.

- Suppose f_1 is solved by a solved fact f_2 of type 1. Let $\hat{\mathsf{f}}_2 = [u \mid \emptyset]$ where $u \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ and $\sigma = \mathrm{mgu}(u, t_1)$. There are two possible cases. Either $u = t_1$. As $u \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ we have that u is ground and $\mathrm{dom}(\sigma) = \emptyset$. In this case $\#\,\mathrm{var}(t_2, \ldots, t_n) = \#\,\mathrm{var}(t_1, \ldots, t_n)$ but as $t_1 \notin \mathcal{X}$ we have that $\sum_{2 \leq i \leq n} |t_i| < \sum_{1 \leq i \leq n} |t_i|$. Or $u \neq t_1$ and $\#\,\mathrm{var}(t_2, \ldots t_n) < \#\,\mathrm{var}(t_1, \ldots t_n)$.
- Suppose f_1 is solved by a solved fact f_2 of type 2. Let $\hat{\mathsf{f}}_2 = [f(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$ and $\sigma = \mathrm{mgu}(u, t_1)$. As $t_1 \notin \mathcal{X}$ we have that $t_1 = f(s_1, \ldots, s_k)$. We have that $\sigma = \{x_1 \mapsto s_1, \ldots, x_k \mapsto s_k\}$ and the resulting fact f_0 is such that
$$\hat{\mathsf{f}}_0 = [t\sigma \mid \Delta] = [t\sigma \mid s_1, \ldots, s_k, t_2, \ldots, t_n].$$

  Thus, we have that $\#\,\mathrm{var}(\Delta) = \#\,\mathrm{var}(t_1, \ldots, t_n)$ and $\sum_{u \in \Delta} |u| < \sum_{1 \leq i \leq n} |t_i|$.

This allows us to conclude the proof. □

B.3 Malleable encryption

Lemma 9. *For any frame φ, and any (F, E) such that* $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$ *w.r.t.* $\mathcal{R}_{\mathcal{E}_{mal}}$*, we have that:*

1. $\{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}$ *and* f *is a solved deduction fact*$\} \subseteq \mathcal{Q}(\varphi)$ *and* $\mathcal{Q}(\varphi)$ *is finite;*
2. $\mathsf{m_f}(\mathsf{f}_0) <_{\mathsf{f}} \mathsf{m_f}(\mathsf{f}_1)$ *where* f_0, f_1 *are defined as in rule F-Solving;*
3. $\mathsf{m_e}(\mathsf{f}_0) <_{\mathsf{e}} \mathsf{m_e}(\mathsf{f}_1)$ *where* f_0, f_1 *are defined as in rule E-Solving*

where $\mathcal{Q}$, $\mathsf{m_f}$, $\mathsf{m_e}$, $<_{\mathsf{f}}$, *and* $<_{\mathsf{e}}$ *are defined w.r.t. to the rewrite system* $\mathcal{R}_{\mathcal{E}_{mal}}$ *as described in Section 5.2.*

Proof. Let $\mathcal{E} = \mathcal{E}_{mal}$. The proof of item 1 is done by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. To ease the induction we strengthen the induction hypothesis and prove a slightly stronger statement. We define $\mathcal{Q}'(\varphi)$ as the smallest set such that:

1. $[t \mid \emptyset] \in \mathcal{Q}'(\varphi)$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
2. $[f(x_1, x_2) \mid x_1, x_2] \in \mathcal{Q}'(\varphi)$, where $f \in \{enc, dec, mal\}$
3. $[enc(x, t) \mid x] \in \mathcal{Q}'(\varphi)$, if there exists t' such that $enc(t', t) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
4. $[x \mid enc(x, y), y] \in \mathcal{Q}'(\varphi)$
5. $[enc(z, y) \mid enc(x, y), z] \in \mathcal{Q}'(\varphi)$
6. $[t \mid t_1, \ldots, t_k] \in \mathcal{Q}'(\varphi)$, if $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ and $C[t_1, \ldots, t_k] \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some context C
7. $[x \mid x, t_1, \ldots, t_k]$, where $C[t_1, \ldots, t_k] \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some context C

In the following when a projection $\hat{\mathsf{f}}$ corresponds to one of the above 7 cases, we say that f is of type i ($1 \leq i \leq 7$). We prove that for any (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$ we have that $\hat{\mathsf{F}} \subseteq \mathcal{Q}'(\varphi)$. It is easy to see that $\{\hat{\mathsf{f}} \mid \hat{\mathsf{f}} \in \mathcal{Q}'(\varphi)$ and $\hat{\mathsf{f}}$ is solved$\} \subseteq \mathcal{Q}(\varphi)$, this will indeed allows us to conclude. We prove the result by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$.

Base case. It is clear that for all deduction facts $\mathsf{f} \in \mathrm{Init}(\varphi)$ we have that $\hat{\mathsf{f}}$ is either of type 1 or type 2.

Inductive case. We assume that the result holds for (F, E) and show that any possible application of a saturation rule preserves the result.

- Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 1, i.e. $\hat{\mathsf{f}} = [t \mid \emptyset]$ with $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$. By applying rule Narrowing, we obtain a fact f' such that $\hat{\mathsf{f}'} = [t' \mid \emptyset]$, and $t \rightarrow_{\mathcal{R}_\mathcal{E}} t'$. As $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$, it follows that $t' \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ and therefore f' is a fact of type 1.
- Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 2 such that $\hat{\mathsf{f}} = [f(x_1, x_2) \mid x_1, x_2]$. By applying the rule Narrowing we obtain a fact of type 4, or 5.
- Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 3, then $\hat{\mathsf{f}} = [enc(x, t) \mid x]$ and the rule Narrowing can only be applied on a position in t. Therefore, Narrowing will produce another fact $\hat{\mathsf{f}'} = [enc(x, u) \mid x]$, where $t \rightarrow u$. As there exists t' such that $enc(t', t) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ by definition of $\mathrm{st}_{\mathcal{R}_\mathcal{E}}$, $enc(t', u) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ yielding again a fact of type 3.

– Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 4, then its unsolved side condition can be solved using a fact of type 1, 2 or 3. In the first case, we obtain a fact of type 6. In the second case, we obtain an useless fact. In the third case, we obtain a fact of type 7.
– Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 5, its unsolved side condition can be solved using a fact of type 1, 2 or 3. In the first case, we obtain a fact of type 3. In the second and third case, we obtain an useless fact.
– Consider a fact $\mathsf{f} \in \mathsf{F}$ of type 6 or 7, its unsolved side conditions can be solved using a fact of type 1, 2 or 3. Let f' be the new fact obtained by applying the F-Solving rule. If f' is unsolved, it has the same type as f. If f' is solved, it is either of type 1 if f is of type 6 or it is useless if f is of type 7.

To show items 2 and 3 it remains to be proven that $\mathsf{m_f}$ and $\mathsf{m_e}$ strictly decrease after a side condition of an unsolved fact is solved. As side conditions can only be solved by facts of type 1-3 this is easily shown by a case analysis. We detail the proof for $\mathsf{m_f}$. The case of $\mathsf{m_e}$ can be done in a similar way.
Let $\mathsf{f}_1 = [R \rhd t \mid X_1 \rhd t_1, \ldots X_n \rhd t_n]$. The case where f_1 is solved by a fact f_2 of type 1 (resp. type 2) is similar to the proof done in Lemma 8. It remains the case where f_2 is of type 3.

Let $\hat{\mathsf{f}}_2 = [enc(x, u) \mid x]$ and $\sigma = \mathrm{mgu}(enc(x, u), t_1)$. As there exists u' such that $enc(u', u) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ we have that u is ground. As $t_1 \notin \mathcal{X}$ we have that $t_1 = enc(t'_1, t''_1)$. The projection of the resulting fact f_0 is $\hat{\mathsf{f}}_0 = [t\sigma \mid x\sigma, t_2\sigma, \ldots, t_n\sigma]$. We distinguish two cases. Either $\sigma = \{x \mapsto t'_1\}$ and $\hat{\mathsf{f}}_0 = [t \mid t'_1, t_2, \ldots, t_n]$. In such a case $\#\,\mathrm{var}(t_2, \ldots, t_n) \leq \#\,\mathrm{var}(t_1, \ldots, t_n)$ and $\sum_{2 \leq i \leq n} |t_i| < \sum_{1 \leq i \leq n} |t_i|$. Otherwise, we have that $\#\,\mathrm{var}(t_2, \ldots, t_n) < \#\,\mathrm{var}(t_1, \ldots, t_n)$. ☐

B.4 Trap-door commitment

The following convergent equational theory $\mathcal{E}_{td}$ is a model for trap-door commitment:

1. $open(td(x, y, z), y) = x$
2. $td(x_2, f(x_1, y, z, x_2), z) = td(x_1, y, z)$
3. $open(td(x_1, y, z), f(x_1, y, z, x_2)) = x_2$
4. $f(x_2, f(x_1, y, z, x_2), z, x_3) = f(x_1, y, z, x_3)$

We will refer below to the four corresponding rewrite rules as R1, R2, R3 and R4.

Lemma 10. *For any frame φ, and any (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$, we have that:*

1. *$\{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}$ and f is a solved deduction fact$\} \subseteq \mathcal{Q}(\varphi)$ and $\mathcal{Q}(\varphi)$ is finite;*
2. *$\mathsf{m_f}(\mathsf{f}_0) <_\mathsf{f} \mathsf{m_f}(\mathsf{f}_1)$ where f_0, f_1 are defined as in rule F-Solving;*
3. *$\mathsf{m_e}(\mathsf{f}_0) <_\mathsf{e} \mathsf{m_e}(\mathsf{f}_1)$ where f_0, f_1 are defined as in rule E-Solving*

where $\mathcal{Q}(\varphi)$ is defined as the smallest set that contains:

1. *$[t \mid \emptyset]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$*

2. $[td(t_1, r, tp) \mid \emptyset]$ *such that* $f(t_1, r, tp, t_2) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ *for some* t_2
3. $[g(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$*, where* $g \in \{open, td, f\}$ *and* $ar(g) = k$
4. $[f(t_1, r, tp, x) \mid x]$*, such that* $f(t_1, r, tp, t_2) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ *for some* t_2

and $\mathsf{m_f}$*,* $\mathsf{m_e}$*,* $<_\mathsf{f}$*, and* $<_\mathsf{e}$ *are defined with* $\mathcal{E} = \mathcal{E}_{td}$ *as described in Section 5.2.*

Proof. Let $\mathcal{E} = \mathcal{E}_{td}$. The proof of item 1 is done by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. To ease the induction we strengthen the induction hypothesis and prove a slightly stronger statement. We define $\mathcal{Q}'(\varphi)$ as the smallest set that contains:

1. $[t \mid \emptyset]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
2. $[td(t_1, r, tp) \mid \emptyset]$ such that $f(t_1, r, tp, t_2) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some t_2
3. $[g(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$, where $g \in \{open, td, f\}$ and $ar(g) = k$
4. $[f(t_1, r, tp, x) \mid x]$, such that $f(t_1, r, tp, t_2) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some t_2
5. $[x \mid td(x, y, z), y]$
6. $[td(x_1, y, z) \mid x_2, f(x_1, y, z, x_2), z]$
7. $[x_2 \mid td(x_1, y, z), f(x_1, y, z, x_2)]$
8. $[f(x_1, y, z, x_3) \mid x_2, f(x_1, y, z, x_2), z, x_3]$
9. $[x_2 \mid x_1, y, z, f(x_1, y, z, x_2)]$
10. $[x_2 \mid td(x, y, z), x, y, z, x_2]$
11. $[x \mid f(t_1, r, tp, x)]$ for every $t_1, r, tp \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
12. $[x \mid td(t, r, tp), x]$ for every $t, r, tp \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
13. $[x \mid x, t_1, \ldots, t_k]$ for every $t_1, \ldots, t_k \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
14. $[t \mid td(t_1, r, tp)]$ for every $t, t_1, r, tp \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
15. $[t \mid t_1, \ldots, t_k]$ for every $t, t_1, \ldots, t_k \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$, $k \geq 1$
16. $[td(t, r, tp) \mid t_1, \ldots, t_k]$, $\exists t'\ f(t, r, tp, t') \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi), t_1, \ldots, t_k \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi), k \geq 1$
17. $[td(t, r, tp) \mid x, t_1, \ldots, t_k]$, $\exists t'\ f(t, r, tp, t') \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi), t_1, \ldots, t_k \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi), k \geq 1$
18. $[f(t, r, tp, x) \mid x, t_1, \ldots, t_k]$, $\exists t'\ f(t, r, tp, t') \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$, $t_1, \ldots, t_k \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
19. $[f(t, r, tp, x) \mid x, x', t_1, \ldots, t_k]$, $\exists t'\ f(t, r, tp, t') \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi), t_1, \ldots, t_k \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$

In the following when a projection $\hat{\mathsf{f}}$ corresponds to one of the above 19 cases, we say that f is of type i ($1 \leq i \leq 19$). We prove that for any (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$ we have that $\hat{\mathsf{F}} \subseteq \mathcal{Q}'(\varphi)$. It is easy to see that $\{\hat{\mathsf{f}} \mid \hat{\mathsf{f}} \in \mathcal{Q}'(\varphi)$ and $\hat{\mathsf{f}}$ is solved$\} \subseteq \mathcal{Q}(\varphi)$, this will indeed allows us to conclude. We prove the result by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$.

Base case. It is clear that all deduction facts $\mathsf{f} \in \mathrm{Init}(\varphi)$ are either of type 1 or type 3.

Inductive case. We assume that the result holds for (F, E) and show that any possible application of a saturation rule preserves the result. We summarize case analysis in the following two matrices.

Narrowing	R1	R2	R3	R4
type 1	1	1	1	1
type 2	2	2	2	2
type 3	5	6	7	8
type 4	4	4	4	4

F-Solving	type 1	type 2	type 3	type 4
type 5	15	15	useless	impossible
type 6	16	impossible	useless	17
type 7	11 or 14	11	9 or 10	12
type 8	18	impossible	useless	19
type 9	15	impossible	useless	13
type 10	13	13	useless	impossible
type 11	1	impossible	13	useless
type 12	useless	useless	13	impossible
type 13	13 or useless	13 or useless	13	13
type 14	1	1	15	impossible
type 15	15 or 1	15 or 1	15	15
type 16	16 or 2	16 or 2	16	16
type 17	17 or 2	17 or 2	17	17
type 18	18 or 4	18 or 4	18	18
type 19	19 or 4	19 or 4	19	19

Items 2 and 3 are shown as in Lemma 9. □

B.5 Blind signature

The following convergent equational theory $\mathcal{E}_{blind}$ is a model for blind signatures:

1. $unblind(blind(x, y), y) = x$
2. $unblind(sign(blind(x, y), z), y) = sign(x, z)$
3. $checksign(sign(x, y), pk(y)) = x$

We will refer below to the three corresponding rewrite rules as $\mathsf{R1}$, $\mathsf{R2}$ and $\mathsf{R3}$.

Lemma 11. *For any frame φ, and any (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$, we have that:*

1. *$\{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}$ and f is a solved deduction fact$\} \subseteq \mathcal{Q}(\varphi)$ and $\mathcal{Q}(\varphi)$ is finite;*
2. *$\mathsf{m_f}(\mathsf{f}_0) <_\mathsf{f} \mathsf{m_f}(\mathsf{f}_1)$ where f_0, f_1 are defined as in rule F-Solving;*
3. *$\mathsf{m_e}(\mathsf{f}_0) <_\mathsf{e} \mathsf{m_e}(\mathsf{f}_1)$ where f_0, f_1 are defined as in rule E-Solving*

where $\mathcal{Q}(\varphi)$ is defined as the smallest set that contains:

1. *$[t \mid \emptyset]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$*
2. *$[f(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$, where $f \in \mathcal{F}$ and $ar(f) = k$*
3. *$[sign(t, x) \mid x]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$*
4. *$[sign(t, t') \mid \emptyset]$, for every $t, t' \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$*

and $\mathsf{m_f}$, $\mathsf{m_e}$, $<_\mathsf{f}$, and $<_\mathsf{e}$ are defined with $\mathcal{E} = \mathcal{E}_{blind}$ as described in Section 5.2.

Proof. Let $\mathcal{E} = \mathcal{E}_{blind}$. The proof of item 1 is done by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. To ease the induction we strengthen the induction hypothesis and prove a slightly stronger statement. We define $\mathcal{Q}'(\varphi)$ as the smallest set that contains:

1. $[t \mid \emptyset]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
2. $[f(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$, where $f \in \mathcal{F}$ and $ar(f) = k$
3. $[sign(t, x) \mid x]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
4. $[sign(t, t') \mid \emptyset]$, for every $t, t' \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
5. $[x \mid blind(x, y), y]$
6. $[sign(x, z) \mid sign(blind(x, y), z), y]$
7. $[x \mid sign(x, y), pk(y)]$
8. $[sign(x, z) \mid blind(x, y), z, y]$
9. $[x \mid sign(x, y), y]$
10. $[x \mid x, y, pk(y)]$
11. $[t \mid t_1, \ldots, t_k]$ if $C[t_1, \ldots, t_k] \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some context C and $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
12. $[sign(t, t') \mid t_1, \ldots, t_k]$ if $C[t_1, \ldots, t_k] \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some context C, $k \geq 1$, and $t, t' \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
13. $[t \mid pk(t')]$, for every $t, t' \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
14. $[x \mid sign(x, t)]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
15. $[t \mid y, pk(y)]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
16. $[sign(t, z) \mid z, t_1, \ldots, t_k]$ if $C[t_1, \ldots, t_k] \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some context C, $k \geq 1$, and $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
17. $[x \mid x, t_1, \ldots, t_k]$ if $C[t_1, \ldots, t_k] \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for some context C

In the following when a projection $\hat{\mathsf{f}}$ corresponds to one of the above 17 cases, we say that f is of type i ($1 \leq i \leq 17$). We prove that for any (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$ we have that $\hat{\mathsf{F}} \subseteq \mathcal{Q}'(\varphi)$. It is easy to see that $\{\hat{\mathsf{f}} \mid \hat{\mathsf{f}} \in \mathcal{Q}'(\varphi)$ and $\hat{\mathsf{f}}$ is solved$\} \subseteq \mathcal{Q}(\varphi)$, this will indeed allows us to conclude. We prove the result by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$.

Base case. It is clear that all deduction facts $\mathsf{f} \in \mathrm{Init}(\varphi)$ are either of type 1 or type 2.

Inductive case. We assume that the result holds for (F, E) and show that any possible application of a saturation rule preserves the result. We summarize the case analysis in the following two matrices.

Narrowing	R1	R2	R3
type 1	1	1	1
type 2	5	6	7
type 3	3	3	3
type 4	4	4	4

F-Solving	type 1	type 2	type 3	type 4
type 5	11	useless	impossible	impossible
type 6	12	8	16	12
type 7	13 or 14	9 or 10	15	13
type 8	16	useless	impossible	impossible
type 9	11	useless	1	11
type 10	17	useless	impossible	impossible
type 11	11 or 1	11	11	11 or 1
type 12	12 or 4	12	12	12 or 4
type 13	1	11	impossible	impossible
type 14	1	17	11	1
type 15	11	1	impossible	impossible
type 16	16 or 3	16	16	16 or 3
type 17	17 or useless	17	17	17 or useless

Items 2 and 3 are shown as in Lemma 9. □

B.6 Addition

The following convergent equational theory $\mathcal{E}_{add}$ is a simple model of addition introduced in [1]:

1. $plus(x, s(y)) = plus(s(x), y)$
2. $plus(x, 0) = x$
3. $pred(s(x)) = x$

We will refer below to the three corresponding rewrite rules as $\mathsf{R1}$, $\mathsf{R2}$ and $\mathsf{R3}$.

Lemma 12. *For any frame φ, and any (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$, we have that:*

1. *$\{\hat{\mathsf{f}} \mid \mathsf{f} \in \mathsf{F}$ and f is a solved deduction fact$\} \subseteq \mathcal{Q}(\varphi)$ and $\mathcal{Q}(\varphi)$ is finite;*
2. *$\mathsf{m_f}(\mathsf{f}_0) <_\mathsf{f} \mathsf{m_f}(\mathsf{f}_1)$ where f_0, f_1 are defined as in rule F-Solving;*
3. *$\mathsf{m_e}(\mathsf{f}_0) <_\mathsf{e} \mathsf{m_e}(\mathsf{f}_1)$ where f_0, f_1 are defined as in rule E-Solving*

where $\mathcal{Q}(\varphi)$ is defined as the smallest set that contains:

1. *$[t \mid \emptyset]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$*
2. *$[f(x_1, \ldots, x_k) \mid x_1, \ldots, x_k]$, where $f \in \{s, plus, pred, 0\}$ and $ar(f) = k$*
3. *$[plus(s^n(x), t) \mid x]$, if $s^n(t) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for $n \geq 0$*

and $\mathsf{m_f}$, $\mathsf{m_e}$, $<_\mathsf{f}$, and $<_\mathsf{e}$ are defined with $\mathcal{E} = \mathcal{E}_{add}$ as described in Section 5.2.

Proof. Let $\mathcal{E} = \mathcal{E}_{add}$. The proof of item 1 is done by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. To ease the induction we strengthen the induction hypothesis and prove a slightly stronger statement. We define $\mathcal{Q}'(\varphi)$ as the smallest set that contains:

1. $[t \mid \emptyset]$, for every $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$
2. $[f(x_1,\dots,x_k) \mid x_1,\dots,x_k]$, where $f \in \mathcal{F}$ and $ar(f) = k$
3. $[plus(s^n(x),t) \mid x]$, if $s^n(t) \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ for $n \geq 0$
4. $[x \mid x, 0]$
5. $[plus(s(x),y) \mid x, s(y)]$
6. $[x \mid s(x)]$

In the following when a projection $\hat{\mathsf{f}}$ corresponds to one of the above 6 cases, we say that f is of type i ($1 \leq i \leq 6$). We prove that for any (F,E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F},\mathsf{E})$ we have that $\hat{\mathsf{F}} \subseteq \mathcal{Q}'(\varphi)$. It is easy to see that $\{\hat{\mathsf{f}} \mid \hat{\mathsf{f}} \in \mathcal{Q}'(\varphi)$ and $\hat{\mathsf{f}}$ is solved$\} \subseteq \mathcal{Q}(\varphi)$, this will indeed allows us to conclude. We prove the result by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F},\mathsf{E})$.

Base case. It is clear that all deduction facts $\mathsf{f} \in \mathrm{Init}(\varphi)$ are either of type 1 or type 2.

Inductive case. We assume that the result holds for (F,E) and show that any possible application of a saturation rule preserves the result. We summarize the case analysis in the following two matrices.

Narrowing	R1	R2	R3
type 1	1	1	1
type 2	5	4	6
type 3	3	useless or 3	3

F-Solving	type 1	type 2	type 3
type 4	useless	useless	impossible
type 5	3	useless	impossible
type 6	1	useless	impossible

To show item 2 and 3, it remains to be proven that $\mathsf{m_f}$ and $\mathsf{m_e}$ strictly decrease after a side condition of an unsolved fact is solved. A side condition can only be solved by facts of type 1, 2 or 3. We show the result by a case analysis.
Let $\mathsf{f}_1 = [R \rhd t \mid X_1 \rhd t_1, \dots, X_n \rhd t_n]$.

- If the solved fact is of type 1 or 2, the proof is similar to the reasoning done in Lemma 8.
- It is easy to see that a solved fact of type 3 cannot be used to solved a side condition of an unsolved fact (types 4-6). Indeed, the side conditions which are are not variables, are either 0 or a term of the form $s(x)$ and hence unification is impossible.

Let $\mathsf{f} = [U \sim V \mid X_1 \rhd t_1, \dots, X_n \rhd t_n]$

- If the solved fact is of type 1 or 2, the proof is similar to the reasoning done in Lemma 8.
- A solved fact of type 3 can be used to solve a side condition of the form $X \rhd t$ when t is headed with the symbol *plus*. It is easy to see (since we already know the form of the deduction facts) that the only terms t occurring in a side condition of an equational fact and headed with *plus* are ground. This allows us to conclude that the measure $\mathsf{m_e}$ decreases also in this case. $\square$

B.7 Homomorphic encryption

Lemma 13. *If the saturation strategy is fair the saturation process terminates for the equational theory $\mathcal{E}_{\mathsf{hom}}$.*

Proof. In the following let $\mathcal{E} = \mathcal{E}_{\mathsf{hom}}$. Orienting the five equations in $\mathcal{E}_{\mathsf{hom}}$ we obtain the following rewriting rules:

R1 $\mathit{fst}(\mathit{pair}(x, y)) \to x$
R2 $\mathit{snd}(\mathit{pair}(x, y)) \to y$
R3 $\mathit{dec}(\mathit{enc}(x, y), y) \to x$
R4 $\mathit{enc}(\mathit{pair}(x, y), z) \to \mathit{pair}(\mathit{enc}(x, z), \mathit{enc}(y, z))$
R5 $\mathit{dec}(\mathit{pair}(x, y), z) \to \mathit{pair}(\mathit{dec}(x, z), \mathit{dec}(y, z))$

For the purpose of this proof we extend the notion of extended subterm and define $\mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t)$ to be the smallest set such that:

1. $t \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t)$,
2. $f(t_1, \ldots, t_k) \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t)$ implies $t_1, \ldots, t_k \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t)$,
3. $t' \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t)$ and $t' \to_{\mathcal{R}_\mathcal{E}} t''$ implies $t'' \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t)$.
4. $\mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(f(t_1, \ldots, t_k)) \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t)$ implies $\mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(f(s_1, \ldots, s_k)) \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t)$ for every $s_i \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(t_i)$ and for every $f \in \mathcal{F}$ of arity k.

Let φ be the frame being saturated. We first show that for all knowledge bases (F, E) such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$ we have that each $\hat{\mathsf{f}} \in \hat{\mathsf{F}}$ has one of the following forms:

1. $[t \mid \emptyset]$, for some $t \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(\varphi)$
2. $[\mathit{fst}(x) \mid x]$
3. $[\mathit{snd}(x) \mid x]$
4. $[\mathit{enc}(x, y) \mid x, y]$
5. $[\mathit{dec}(x, y) \mid x, y]$
6. $[\mathit{pair}(x, y) \mid x, y]$
7. $[C[t_1, \ldots, t_k] \mid \mathrm{var}(C)]$ where:
   - C is obtained by arbitrarily nesting the following (classes of) contexts: $C_1 = \mathit{enc}(\_, z_i)$, $C_2 = \mathit{dec}(\_, z_i)$ and $C_3 = \mathit{pair}(\_, \_)$, where z_i are variables.
   - C contains at least one variable.
   - $C'[t_1, \ldots, t_k] \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(\phi)$, where C' is obtain from C by replacing $\mathit{enc}(\_, z_i)$ and $\mathit{dec}(\_, z_i)$ with $\_$.
8. $[x \mid \mathit{pair}(x, y)]$
9. $[y \mid \mathit{pair}(x, y)]$
10. $[x \mid \mathit{enc}(x, y), y]$
11. $[\mathit{pair}(\mathit{enc}(x, z), \mathit{enc}(y, z)) \mid \mathit{pair}(x, y), z]$
12. $[\mathit{pair}(\mathit{dec}(x, z), \mathit{dec}(y, z)) \mid \mathit{pair}(x, y), z]$
13. $[t \mid t_1, \ldots, t_k]$, for some $t, t_1, \ldots, t_k \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(\varphi)$
14. $[C[t_1, \ldots, t_k] \mid s_1, \ldots, s_l, \mathrm{var}(C)]$ where:

- C is obtained by arbitrarily nesting the following (classes of) contexts: $C_1 = enc(\_, z_i)$, $C_2 = dec(\_, z_i)$, and $C_3 = pair(\_, \_)$, where z_i are variables.
- $C'[t_1, \ldots, t_k] \in \mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(\phi)$, where C' is obtain from C by replacing $enc(\_, z_i)$ and $dec(\_, z_i)$ with $\_$.
- s_i are ground terms

We show this by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. In the following when a projection $\hat{\mathsf{f}}$ corresponds to one of the above 14 cases, we say that f is of type i $(1 \leq i \leq 14)$.
Base case. It is easy to see that all $\mathsf{f} \in \mathrm{Init}(\varphi)$ are indeed of type $1-6$.
Inductive case. We assume that the result holds for (F, E) and show that any possible application of a saturation rule preserves the result. We summarize case analysis in the following two matrices.

Narrowing	R1	R2	R3	R4	R5
type 1	1	1	1	1	1
type 2	8	impossible	impossible	impossible	impossible
type 3	impossible	9	impossible	impossible	impossible
type 4	impossible	impossible	impossible	11	impossible
type 5	impossible	impossible	10	impossible	12
type 6	impossible	impossible	impossible	impossible	impossible
type 7	7	7	$1, 7, 13, 14$	7	7

F-Solving	type 1	type 2	type 3	type 4	type 5	type 6	type 7
type 8	1	imp.	imp.	imp.	imp.	useless	$7, 1$
type 9	1	imp.	imp.	imp.	imp.	useless	$7, 1$
type 10	13	imp.	imp.	imp.	useless	imp.	$7, 1$
type 11	7	imp.	imp.	imp.	imp.	useless	7
type 12	7	imp.	imp.	imp.	imp.	useless	7
type 13	$1, 13$	13	13	13	13	13	13
type 14	$7, 14$	14	14	14	14	14	14

We next show that because the strategy is fair at a given saturation step, no more facts of type 7 are added.

Lemma 14. *Suppose that the saturation strategy is fair and let*

$$\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}_0, \mathsf{E}_0) \Longrightarrow \ldots \Longrightarrow (\mathsf{F}_i, \mathsf{E}_i) \Longrightarrow \ldots$$

be a sequence of saturation steps. If $\hat{\mathsf{f}} = [C[t_1, \ldots, t_k] \mid s_1, \ldots, s_l, \mathrm{var}(C)] \in \hat{\mathsf{F}}_0$ *is of type 7 or type 14 and* $\mathsf{F}_0 \vdash s_j$ *for all* j*, then there exists* n *such that* $\mathsf{F}_n \vdash t_i$ *for all* i*.*

Proof. The proof is done by induction on the number of saturation steps of $\mathrm{Init}(\varphi) \Rightarrow^* (\mathsf{F}_0, \mathsf{E}_0)$.
Base case. As $\mathrm{Init}(\varphi)$ does not contain any facts of type 7 or 14 we conclude.
Inductive case. We suppose that the result holds for $(\mathsf{F}_0, \mathsf{E}_0)$ and verify that it is maintained by any possible rules that add a fact of type 7 or 14.

- Suppose we add a fact of type 7 by using rule Narrowing on a fact of type 7 in F_0 and R1 or R2. The rewriting must occur at a position in one of the t_i which is rewritten to t_i'. By induction hypothesis we have that there exists n, such that $\mathsf{F}_n \vdash t_i$. We can adapt the proof of Proposition 2 to show that because of fairness (rather than saturation) narrowing must be applied such that there exists n' such that $\mathsf{F}_{n'} \vdash t_i'$.
- Suppose we add a fact of type 7 by using rule Narrowing on a fact of type 7 in F_0 and R3. If narrowing is applied on one of the t_i the case is similar to the previous one. If narrowing is applied inside the context such that the t_i do not change we conclude by induction hypothesis.
- Suppose we add a fact of type 14 by using rule Narrowing on a fact of type 7 in F_0 and R3. Narrowing must have changed both the context and one of the t_i. Suppose w.l.o.g. $i = 1$. It must be that be that $t_1 = enc(t_1', t_1'')$. We have to show that there exists n such that if $\mathsf{F}_n \vdash t_1''$ then $\mathsf{F}_n \vdash t_1'$ and $\mathsf{F}_n \vdash t_i$ for $2 \leq i \leq k$. $\mathsf{F}_n \vdash t_i$ is obtained by induction hypothesis. If $\mathsf{F}_n \vdash t_1''$ and because $\mathsf{F}_n \vdash enc(t_1', t_1'')$ we can apply Narrowing such that $\mathsf{F}_{n'} \vdash t_1'$ for some n'.
- Suppose we add a fact of type 7 by using rule Narrowing on a fact of type 7 in F_0 and R4. If narrowing is applied on one of the t_i the case is similar to previous cases. If narrowing is applied inside the context such that the t_i do not change we conclude by induction hypothesis. Suppose both the context and one of the t_i change. We suppose w.l.o.g. that $i = 1$. It must be that $t_1 = pair(t_1', t_1'')$. By induction hypothesis we have that there exists n such that $\mathsf{F}_n \vdash t_i$ for $2 \leq i \leq k$. We need to show that there exists F_n. As $\mathsf{F}_n \vdash pair(t_1', t_1'')$ we also have that $\mathsf{F}_n \vdash fst(pair(t_1', t_1''))$ and $\mathsf{F}_n \vdash snd(pair(t_1', t_1''))$. Because of fairness Narrowing can be applied such that $\mathsf{F}_{n'} \vdash t_1'$ and $\mathsf{F}_{n'} \vdash t_1''$ for some n''.
- Suppose we add a fact of type 7 by using rule F-Solving on facts of type 11 and 1 in F_0. Let $pair(t_1, t_2)$ be the fact of type 1. As the strategy is fair we will add facts $[x|pair(x, y)]$ and $[y|pair(x, y)]$ by applying rule Narrowing on type 2/R1 and type 3/R2. Again by fairness we will apply solving on $pair(t_1, t_2)$ and $[x|pair(x, y)]$ as well as $[y|pair(x, y)]$. Therefore t_1 and t_2 will be generated.
- Suppose we add a fact of type 7 by using rule F-Solving on facts of type 12 and 1 in F_0. This case is similar to the previous one.
- Suppose we add a fact of type 7 by applying rule F-Solving on facts of type 8-12 with a fact of type 7 in F_0. The resulting fact is a context on the same (or a subset of the) terms t_i $(1 \leq i \leq k)$ as the initial type 7 fact. We conclude by induction hypothesis.

– Suppose we add a fact of type 7 by applying rule F-Solving on a fact of type 14 with a fact of type 1 in F_0. The type 14 fact has only one ground side condition s_1 which is solved by the type 1 fact. Hence $[s_1] \in \hat{\mathsf{F}}_0$ and $\mathsf{F}_0 \vdash s_1$. We can apply the induction hypothesis and conclude.
– Suppose we add a fact of type 14 by applying rule F-Solving on a fact of type 14 with a fact of type i ($1 \leq i \leq 14$) in F_0. We directly conclude by induction hypothesis. ☐

There are a finite number of solved facts other than of type 7. There exist only a finite number of t_i which can occur in facts of type 7 as they are in $\mathrm{st}^+_{\mathcal{R}_\mathcal{E}}(\varphi)$.

Hence it follows from Lemma 14 that for any fair saturation sequence, at some moment all new facts of type 7 become useless and therefore are not added to the knowledge base. Therefore any fair saturation sequence only contains a finite number of solved facts.

We know that after some number n of saturation steps, no more solved deduction facts are added to the knowledge base. We now show that a finite number of unsolved facts are added after this stage. Indeed, after n iterations, as no more solved facts are added to the knowledge base, the only types of facts potentially added are 13 and 14. The side conditions of these facts contain only ground terms or variables. By solving one of the ground side conditions the cardinality of the side condition decreases ensuring termination.

We now show that all equational facts are of the form $[M \sim N \mid X_1 \rhd t_1, \ldots, X_k \rhd t_k]$, for some M, N where either $t_i \in \mathcal{X}$ or $t_i = C[s_1, \ldots, s_l]$ for some ground terms s_j ($1 \leq j \leq l$) and for some context C obtained by arbitrary nesting of contexts $C_1 = enc(\_, z_n)$, $C_2 = dec(\_, z_n)$, $C_3 = pair(\_, \_)$ and $C_4 = \_$, where z_n are variables.

This is true for the equational facts obtained by rule Unifying. When applying rule E-Solving on a side condition of the above type we consider the following cases:

– if we solve $X_i \rhd t_i$ with a type 1 fact, we easily conclude;
– if we solve $X_i \rhd t_i$ with a fact of type 2, 3, 4, 5, 6, the result is immediate;
– if we solve $X_i \rhd t_i$ (where $t_i = C[s_1, \ldots, s_l]$) with a type 7 fact $[C'[u_1, \ldots, u_m] \mid \mathrm{var}(C')]$, we note that $\mathrm{mgu}(t_i, C'[u_1, \ldots, u_m])$ is such that variables are mapped to either variables or ground terms. Therefore the property holds.

Using again the measure

$$\mathsf{m_e}([M \sim N \mid X_1 \rhd t_1, \ldots, X_k \rhd t_k]) = (\#\,\mathrm{var}(t_1, \ldots, t_k), |t_1| + \ldots + |t_k|)$$

and the lexicographic order $<_\mathsf{e}$ on pairs, we obtain that $\mathsf{f}_0 <_\mathsf{e} \mathsf{f}_1$ for all f_0 and f_1 as in rule F-Solving.

C Implementation – Complexity

With certain optimizations described below, our saturation algorithm runs in polynomial time for subterm convergent equational theories, $\mathcal{E}_{mal}$, $\mathcal{E}_{blind}$, and $\mathcal{E}_{td}$.

C.1 Optimizations

Deciding generation in polynomial time ($\mathsf{F} \vdash t$). The recursive algorithm obtained immediately from the generation rules is not polynomial. However, by using memorization, its complexity becomes polynomial. Using the same trick, we can compute a recipe R such that $\mathsf{F} \vdash^R t$ in polynomial time, if we store R in DAG form.

Recipes in DAG form. Indeed, any recipe might grow to an exponential size if it is not stored in DAG form. Therefore, we require that the term R in $[R \rhd u \mid \Delta]$ and the terms U and V in $[U \sim V \mid \Delta]$ are stored in DAG form.

Optimisation to solve ground side conditions. Using different combinations of solved facts to solve ground side conditions is unnecessary work. Therefore we consider that the standard F-Solving and E-Solving rules are applied only when the side condition being solved contains at least one variable. To solve a side condition of the form $X \rhd t$ when t is ground, we use the two rules described below. Again, as for $\oplus$, we suppose that the choice of recipes N and M is uniform.

F-Solving'

$$\frac{\mathsf{f}_1 = [M \rhd t \mid X_0 \rhd t_0, \ldots, X_k \rhd t_k],\ \mathrm{var}(t_0) = \emptyset \quad \mathsf{F} \vdash^N t_0,\ \mathrm{var}(N) \cap \mathrm{var}(\mathsf{f}_1) = \emptyset}{(\mathsf{F}, \mathsf{E}) \Longrightarrow (\mathsf{F}, \mathsf{E}) \oplus \mathsf{f}_0}$$

where $\mathsf{f}_0 = [M[X_0 \mapsto N] \rhd t \mid X_1 \rhd t_1, \ldots, X_k \rhd t_k]$.

E-Solving'

$$\frac{\mathsf{f}_1 = [U \sim V \mid Y \rhd s, X_1 \rhd t_1, \ldots, X_k \rhd t_k] \in \mathsf{E},\ \mathrm{var}(s) = \emptyset \quad \mathsf{F} \vdash^M s,\ \mathrm{var}(M) \cap \mathrm{var}(\mathsf{f}_1) = \emptyset}{(\mathsf{F}, \mathsf{E}) \Longrightarrow (\mathsf{F}, \mathsf{E} \cup \{\mathsf{f}_0\})}$$

where $\mathsf{f}_0 = [U\{Y \mapsto M\} \sim V\{Y \mapsto M\} \mid \{X_i \rhd t_i\}_{1 \leq i \leq k}]$.

Fig. 2. Optimized saturation rules for solving ground side conditions

The soundness of this optimization is assured by Lemma 15 (whose proof is immediate) whereas completeness is shown by proving Lemma 2 and Lemma 3 in the context of the new saturation rules.

Lemma 15 (soundness of the two additional rules). *Let φ be a frame and (F, E) be a knowledge base such that every fact in (F, E) holds in φ. Let f_1 and f_0 be two facts as in rules F-Solving' (resp. E-Solving'). If f_1 holds in φ then f_0 holds in φ.*

Lemma 2. *Let* (F, E) *be a saturated knowledge base and* $\mathsf{f} = [U \sim V \mid X_1 \rhd t_1, \ldots, X_k \rhd t_k]$ *be an equational fact in* E. *For any substitution* σ *grounding for* $\{t_1, \ldots, t_k\}$ *such that* $\mathsf{F} \vdash t_i\sigma$ $(1 \le i \le k)$, *we have that* $\mathsf{F} \vdash^{R_i} t_i\sigma$ *for some* R_i $(1 \le i \le k)$ *and* $\mathsf{E} \models U\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\} \sim V\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\}$.

Proof. By induction on $\sum_{i=1}^{k} |t_i\sigma|$. We distinguish two cases:

1. f *is a solved equational fact.* The proof is as before.
2. f *is an unsolved equational fact.* In such a case, there exists t_j such that $t_j \notin \mathcal{X}$. Let us assume w.l.o.g. that $j = 1$. If t_1 is not ground, then the proof is as before. If t_1 is ground and because (F, E) is saturated,

$$\mathsf{f}_2 = [U\{X_1 \mapsto M\} \sim V\{X_1 \mapsto M\} \mid X_2 \rhd t_2, \ldots, X_k \rhd t_k]$$

must be in E by rule E-Solving', where M is such that $\mathsf{F} \vdash^{M} t_1$.
We can apply the induction hypothesis on the fact f_2 and the same substitution σ to obtain that there exist R_i $(i \ge 2)$ such that $\mathsf{F} \vdash^{R_i} t_i\sigma$ and:

$$\mathsf{E} \models (U \sim V)\{X_1 \mapsto M\}\{X_2 \mapsto R_2, \ldots, X_k \mapsto R_k\}$$

We chose R_1 and M and we immediately obtain the conclusion. $\square$

Lemma 3. *Let* (F, E) *be a saturated knowledge base. Let* $\mathsf{f} = [R \rhd t \mid X_1 \rhd t_1, \ldots, X_k \rhd t_k]$ *be a deduction fact such that* $(\mathsf{F}, \mathsf{E}) \oplus \mathsf{f} = (\mathsf{F}, \mathsf{E})$. *For any substitution* σ *grounding for* $\{t_1, \ldots, t_k\}$ *such that* $\mathsf{F} \vdash t_i\sigma$ $(1 \le i \le k)$, *we have that there exist* $R_1, \ldots, R_k$ *and* W *such that*

- $\mathsf{F} \vdash^{W} t\sigma$, *and* $\mathsf{F} \vdash^{R_i} t_i\sigma$ *for* $1 \le i \le k$;
- $\mathsf{E} \models W \sim R\{X_1 \mapsto R_1, \ldots, X_k \mapsto R_k\}$.

Proof. By induction on $\sum_{i=1}^{k} |t_i\sigma|$. We distinguish two cases. If f is solved, the proof is as before. If f is not solved, there exists j such that $t_j \notin \mathcal{X}$. We assume w.l.o.g. that $j = 1$. If t_1 contains at least one variable, the proof is as before. Otherwise, if t_1 is ground and because (F, E) is saturated, rule F-Solving' must have been applied and therefore we can apply the induction hypothesis on

$$\mathsf{f}_2 = [R\{X_1 \mapsto N\} \rhd t \mid X_2 \rhd t_2, \ldots, X_k \rhd t_k\}]$$

(where N is such that $F \vdash^{N} t_1$) and on the same substitution σ to obtain that there exist R_i $(i \ge 2)$ and W such that

- $\mathsf{F} \vdash^{W} t\sigma$ and $F \vdash^{R_i} t_i\sigma$, for $2 \le i \le k$
- $\mathsf{E} \models R\{X_1 \mapsto N\}\{X_2 \mapsto R_2, \ldots, X_k \mapsto R_k\} \sim W$

We choose $R_1 = N$ and we immediately obtain our conclusion. $\square$

C.2 Complexity

Theorem 2. *Using the optimizations described in Section C.1, and if φ is in normal form, the saturation algorithm terminates in polynomial time for any subterm convergent equational theory, for $\mathcal{E}_{td}$, for $\mathcal{E}_{mal}$ and for $\mathcal{E}_{blind}$.*

In the remaining, we consider an equational theory $\mathcal{E}$ that is either subterm convergent, or $\mathcal{E} \in \{\mathcal{E}_{mal}, \mathcal{E}_{blind}, \mathcal{E}_{td}\}$. We define the following set:

$$\mathcal{Q}(\varphi) = \{[r\sigma \mid t_1, \ldots, t_k]\}$$

for every rewrite rule $l \to r$, for every partial substitution $\sigma : \mathrm{var}(l) \to \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$ and for every set of incomparable positions $p_1, \ldots, p_k \in \mathrm{pos}(l)$ such that for every i ($1 \leq i \leq k$) we have that $t_i = (l|_{p_i})\sigma$.

In order to prove Theorem 2, we need an additional lemma.

Lemma 16. *Let φ be a frame and (F, E) be such that $\mathrm{Init}(\varphi) \Longrightarrow^* (\mathsf{F}, \mathsf{E})$. For any unsolved deduction fact $\mathsf{f} \in \mathsf{F}$ we have that $\hat{\mathsf{f}} \in \mathcal{Q}(\varphi)$.*

Proof. First, note that an unsolved deduction fact obtained by applying Narrowing on a solved fact satisfies this property. Now assume we have an unsolved deduction fact $\hat{\mathsf{f}} = [r\sigma \mid (l|_{p_1})\sigma, \ldots, (l|_{p_k})\sigma] \in \mathcal{Q}(\varphi)$ and assume one of its side conditions $(l|_{p_i})\sigma$ is being solved. Assume w.l.o.g. that $i = 1$.

- If $(l|_{p_1})\sigma$ is ground, rule F-Solving' must be applied. We therefore obtain a fact $\hat{\mathsf{f}}' = [r\sigma \mid (l|_{p_2})\sigma, \ldots, (l|_{p_k})\sigma]$.
- If $(l|_{p_1})\sigma$ is not ground, rule F-Solving is applied and $l|_{p_1}$ is necessarily not a variable (by the definition of σ, it maps variables only to ground terms). Therefore $l|_{p_1}$ is of the form $g(s_1, \ldots, s_l)$ for some function symbol $g \in \mathcal{F}$. We distinguish three cases:
  - If the side condition is solved using a deduction fact whose projection is of the form $[t \mid \emptyset]$ for some $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$, let $\sigma' = \mathrm{mgu}((l|_{p_1})\sigma, t)$ and consider $\tau = \sigma \circ \sigma'$. By rule F-Solving, the side condition $(l|_{p_1})\sigma$ will be replaced by side conditions $((l|_{p_1})|_{q_j})\tau$, for all $(l|_{p_1})|_{q_j} \in \mathcal{X}$ and therefore the fact resulting from the application of the rule satisfies the property.
  - If the side condition is solved using a fact whose projection is of the form $[g(x_1, \ldots, x_l) \mid x_1, \ldots, x_l]$, then the side condition $(l|_{p_1})\sigma$ will be replaced by side conditions $(l|_{p_1 \cdot j})\sigma$, for $1 \leq j \leq l$.
  - If the side conditions is solved using a "special" fact $[sign(t, x) \mid x]$ (with $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$), $[enc(x, t) \mid x]$ (with $t \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$), $[td(t_1, t_2, t_3)]$ (with $t_1, t_2, t_3 \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$) or $[f(t_1, t_2, t_3, x) \mid x]$ (with $t_1, t_2, t_3 \in \mathrm{st}_{\mathcal{R}_\mathcal{E}}(\varphi)$), we obtain by a case-by-case analysis that the property is satisfied by the resulting fact. □

Now, we are able to prove Theorem 2

Proof. (of Theorem 2)

We first show that any knowledge base contains a polynomial number of deduction facts. Indeed, there are a polynomial number of solved deduction facts. Applying rule $\mathsf{Narrowing}$ yields a polynomial number of unsolved deduction facts. We also know, thanks to Lemma 16, that for any frame φ (in normal form), for any (F, E) reachable from $\mathrm{Init}(\varphi)$, and for any unsolved fact $\mathsf{f} \in \mathsf{F}$, we have that $\hat{\mathsf{f}} \in \mathcal{Q}(\varphi)$.

We consider the two following orders:

– the order $<_p$ defined on sets of positions as follows:

$$\{p_0, \ldots, p_\ell\} <_p \{q_1, \ldots, q_k, p_1, \ldots, p_\ell\} \text{ iff } q_1, \ldots, q_k \text{ are incomparable positions and } p_0 \text{ is a prefix of } q_i \ (1 \leq i \leq k).$$

– the order $<_\mathsf{f}$ defined on deduction facts whose projection are in $\mathcal{Q}(\varphi)$:

$$\mathsf{f}_0 <_\mathsf{f} \mathsf{f}_1 \text{ iff either } \ell < k \text{ or } \ell = k \text{ and } \{p_1, \ldots, p_k\} <_p \{p'_1, \ldots, p'_\ell\}.$$

where $\mathsf{f}_0 = [R \rhd r\sigma \mid X_1 \rhd l|_{p_1}\sigma, \ldots, X_k \rhd l|_{p_k}]$, and
$\mathsf{f}_1 = [R' \rhd r\sigma' \mid X_1 \rhd l|_{p'_1}\sigma', \ldots, X_l \rhd l|_{p'_\ell}\sigma']$.

As $<_\mathsf{f}$ does not depend on the frame, all strictly decreasing sequences of deduction facts have at most a constant size. Also note that if f_1 and f_0 are as in rule $\mathsf{F\text{-}Solving}$ or $\mathsf{F\text{-}Solving}$', we have that $\mathsf{f}_0 <_\mathsf{f} \mathsf{f}_1$. There is at most a polynomial number of choices to be made when solving each deduction fact (which side condition, which solved deduction fact). As the resulting facts will be smaller (according to $<_\mathsf{f}$) than the initial fact, and as any such sequence has at most a constant length, an unsolved fact will generated at most a polynomial number of facts.

We now show that each deduction fact has at most a polynomial size if the recipes are stored in DAG form. This is obviously true of the initial facts. The other recipes are obtained from the initial recipes by applying a polynomial number of substitutions whose size is polynomially bounded. Therefore all recipes have polynomial size.

It remains to show that there are a polynomial number of equational facts. This is true of the (necessarily solved) equational facts added during application of $\mathsf{Narrowing}$ and $\mathsf{F\text{-}Solving}$ (via the $\oplus$ operation). The other possibility to generate equational facts is $\mathsf{Unifying}$, which generates a polynomial number of (possible unsolved) equational facts. All such unsolved equational facts have side conditions which are either ground or variables. Therefore, each such unsolved equational fact will lead to at most a polynomial number of other equational facts by applying rule $\mathsf{E\text{-}Solving}$'. $\square$