Multiple Congruence Relations, First-Order Theories on Terms, and the Frames of the Applied Pi-Calculus

Florent Jacquemard, Etienne Lozes, Ralf Treinen, Jules Villard

Multiple Congruence Relations, First-Order Theories on Terms, and the Frames of the Applied Pi-Calculus

Florent Jacquemard[1], Étienne Lozes[1,3⋆], Ralf Treinen[2], and Jules Villard[1,4⋆]

[1] LSV, ENS Cachan, CNRS UMR 8643 and INRIA, France
[2] PPS, Université Paris Diderot, CNRS UMR 7126, France
[3] MOVES, RWTH Aachen, Germany
[4] Queen Mary University of London, UK

Abstract. We investigate the problem of deciding first-order theories of finite trees with several distinguished congruence relations, each of them given by some equational axioms. We give an automata-based solution for the case where the different equational axiom systems are linear and variable-disjoint (this includes the case where all axioms are ground), and where the logic does not permit to express tree relations $x = f(y, z)$. We show that the problem is undecidable when these restrictions are relaxed. As motivation and application, we show how to translate the model-checking problem of $A\pi\mathcal{L}$, a spatial equational logic for the applied pi-calculus, to the validity of first-order formulas in term algebras with multiple congruence relations.

1 Introduction

Term algebras play a crucial role in the symbolic modeling of cryptographic protocols. In the applied π-calculus [2], a variant of the π-calculus tailored to the study of security protocols, the history of communications at some point of a protocol can be represented by a *frame*, consisting of a set of terms, each representing a message that has been sent, together with a set of *names* that are assumed to be secret at the beginning of the communication. For instance, the encryption of a secret s using someone's public key $pub(k)$ (with the equational axiom $dec(enc(x, pub(k)), k) = x$) can lead to the frame $F_0 := (\{k, s\}, \{u_0 = pub(k), u_1 = enc(s, u_0)\})$ where the first element of the pair is the set of *secret* (or *hidden*) names (here k and s) of the frame. Analyzing frames is crucial to discover potential flaws in security protocols.

Usually, one checks the properties of frames against two particular queries: the deducibility of a term from a given frame, and the static equivalence of two given frames. Assuming passive attackers who can observe messages exchanged on all public channels, deducibility corresponds to what they may infer from these observations, while static equivalence asserts *indistinguishability* between two protocols. These two properties are decidable for a fairly large (at least from a practical perspective) class of underlying equational theories, as shown by Abadi and Cortier [1]. However, many other properties, more tailored to a particular protocol, are imaginable. For instance, in the frame F above, one may ask whether the owner of the private key k will be able to

⋆ Authors partially supported by the french ANR project PANDA.

uncover s. To provide a more general decision procedure that would also apply to these properties, one may wish to use a logic for which the model-checking problem is decidable. Since first-order logics over a term algebra cannot easily express the properties above, other formalisms need be considered.

In this paper, we study the decidability of the model-checking of $A\pi\mathcal{L}$ [18, 17], a spatial logic for the applied π-calculus, and more precisely of a fragment $\mathcal{FSL}$ of it we call *frame spatial logic*, that is dedicated to frames. This fragment exposes two of the main ingredients of $A\pi\mathcal{L}$, hidden name revelation and spatial conjunction, which we believe to be generally useful in naturally expressing security properties of frames. For instance, the hidden name revelation can be used to capture the subtler property mentioned above using the formula $\mathsf{H}k.\, u_0 = pub(k) \wedge (\exists x.\, \mathsf{H}s.\, x = s)$, which reads informally as follows: by revealing k, whose public key is published on u_0, one may craft a term x, independent of s but which may depend on k (given the position of the existential quantifier in the formula), such that x is equal to s (here $x = dec(u_2, k)$ would be a valid witness). Spatial conjunction $*$ between two properties expresses the fact that the current frame can be decomposed into two subframes that do not share any hidden name such that each subframe satisfies one of the subformulas. For instance, the formula $1 := \neg\mathbf{0} \wedge \neg(\neg\mathbf{0} * \neg\mathbf{0})$ describes precisely the non-empty frames that may not be decomposed into two non-empty frames. Using this formula, one may express a property Φ about a part of a frame that represents a single session of a protocol (supposing that each session is distinguished from the others by the use of a unique hidden name in each message) with $(1 \wedge \Phi) * \mathsf{true}$. Decomposing frames spatially may also help expose which parts of the frame are responsible for the leak of a secret: the formula $(\exists x.\, \mathsf{H}n.\, x = n) \wedge \neg(\exists x.\, \mathsf{H}n.\, (\Phi_1 * x = n))$ means that a secret name is leaked, but that the messages in the part of the frame described by Φ_1 are necessary to obtain this secret. The frame spatial logic $\mathcal{FSL}$ is also rich enough to express that a given term is deducible from a frame and to characterise a particular frame.

Reducing the model-checking problem of the logic $\mathcal{FSL}$ to a purely equational logic with no spatial connectives gives rise to formulas where *multiple* congruence relations may appear, which come from the various (fragments of) frames $\{u_i = t_i\}_{i\in I}$ under consideration, each introducing additional axioms $u_i = t_i$ to the term algebra. Another, more restricted case of multiple congruence relations can be found in the logic of frames $\mathcal{LF}$ of Hüttel and Pedersen [14], in which one can compare terms either syntactically ($t_1 = t_2$) or according to the underlying equational theory $\mathcal{E}$ ($t_1 =_{\mathcal{E}} t_2$).

In this paper, we introduce the general framework of first-order constraints systems with *multiple* congruence relations. There exist a number of decidability results for the first-order theory of term algebras, or equivalently finite trees, and more generally for the first-order theory of the quotient of a term algebra by some congruence. Most of these decidability results were obtained by quantifier elimination. One of the key observation for quantifier elimination procedures is that the rule

$$\exists x.\, (x = t \wedge \phi) \quad \rightsquigarrow \quad \phi[x{\leftarrow}t] \quad \text{if } x \notin \mathit{Vars}(t)$$

where ϕ is an arbitrary conjunction of literals, and $\phi[x{\leftarrow}t]$ denotes the formula obtained by replacing every occurrence of the variable x by the term t, requires $=$ to be a congruence relation with respect to all functions and predicates of the structure. However,

when faced with several congruence relations, the observation above cannot be naively used as a basis for quantifier elimination. The reason is that, faced with a formula like $\exists x_1, x_2.\, (x_1 =_1 t_1 \wedge x_2 =_2 t_2 \wedge \phi)$ where $=_1$ and $=_2$ are two different congruence relations of our structure, one cannot simply eliminate x_1 or x_2 as before. Indeed $=_1$ would not necessarily be a congruence with respect to $=_2$, and vice versa, since in general the equational axioms used for defining these equivalence relations would be independent. One might however hope that there is a solution to this problem. If $\{\theta_1, \ldots, \theta_n\}$ is a complete set of unifiers of $x =_1 t_1$, that is for the equational theory $=_1$, then the above formula would be equivalent to $\exists x_2, \bar{y}_1.\, (x_2 =_2 t_2 \wedge \phi)\theta_1 \vee \ldots \vee \exists x_2, \bar{y}_n.\, (x_2 =_2 t_2 \wedge \phi)\theta_n$ where $\bar{y}_i$ is the set of extra variables introduced by the unifier θ_i. The question is whether a similar combination result can be achieved for the full first-order theory.

Results In this paper, we show the decidability of the first-order theory of term algebras with several congruence relations. The predicates of our structure are of the form $x =_i y$, where each $=_i$ is given by a set of linear and variable-disjoint equational axioms. The structure does *not* contain function symbols, and hence does not allow to express relations of the form $x = f(y, z)$. This restriction makes the structure accessible to automata-theoretic techniques, which is a key to our decidability result. We show that decidability no longer holds when we allow term relations like $x = f(y, z)$, or when one generalizes to flat axiom systems. However, our decidability result can be extended to the quotient of the term algebra under a certain class of rewrite systems (which represent underlying equational theories on terms) for which a completion procedure terminates. We show that it is the case for rewrite rules of the form $g \to x$ where g is a *jack* (see page 9) and all $=_i$ are axiomatized by ground equations. We also show that undecidability is reached as soon as one of the $=_i$ is the tree equality.

From a security point of view, as we will show, this means that deducibility and static equivalence, as well as the model-checking problem of $\mathcal{FSL}$, are all decidable when the underlying equational theory can be expressed as a rewrite system such that the completion procedure mentioned above terminates. This is the case in particular for the theory of pairs and of symmetric and asymmetric encryption with *fixed* keys, but not for the theory of signed messages for instance.

Related work This paper is the result of two lines of research: decidability results for first-order theories on the one side, and the study of process algebras for security protocols on the other side.

The decidability of the first-order theory of finite trees over a finite signature, with syntactic equality as the only predicate, was first shown by Malc'ev [20], this result was later rediscovered and extended independently by Maher [19] and Comon and Lescanne [10]. Encouraged by this result, several researchers started in the late 80s the program to show decidability of the first-order theory of term algebras with different predicates than just syntactic equality. Research basically went into several directions: one direction was to add relations other than equality to the theory, in particular ordering relations that were useful for ordered rewrite calculi [6, 15], or for typing of programming languages [22, 16]. Another direction was the addition of predicates that can be recognized by various classes of tree automata [5, 8]. A third direction was to replace the syntactic equality relation in the original result by an equality relation modulo a set

of equational axioms. The initial optimism was fueled by the fact that for quantifier-free positive constraints, so-called unification systems, the extension of syntactic unification to unification modulo equational theories has led to a rich theory and many useful results (see, for instance, [3] for a survey). The probably strongest result in this direction is the decidability of the theory of term algebras modulo so-called *shallow* equational theories [9]. However, it also turned out that the limits of decidability are met much earlier with first-order theories than with unification problems, and undecidability of the theory of term algebras modulo some important equational theories were shown, among them AC [23, 21].

From the perspective of symbolic cryptography, our work can be compared with the one of Abadi and Cortier [1] in which they show that term deduction and static equivalence are decidable for many equational theories. Most of the classes they consider are out of the reach of the techniques presented here; however, our work takes a different approach than theirs: we consider the decision of any property that can be expressed in $\mathcal{FSL}$, for instance the mere existence of a leaked secret name (which amounts to quantifying over the terms that can be deduced from a frame), or more generally of any property expressible in a first-order theory with multiple congruence relations and a background term rewrite system. This makes both results incomparable.

Outline Section 2 collects the necessary background on term algebras, tree automata, and term rewriting. In Section 3, we establish the decidability of the first-order theory of term algebras with multiple congruence relations, and the undecidability under small relaxations of our hypothesis. In Section 4, we show how to extend the decidability result to a certain class of "background" rewrite systems. Finally, Section 5 introduces the application to the study of the frames of the applied π-calculus.

2 Preliminaries

We assume the usual notions of rewriting. A *signature* Σ is a set of function symbols with arity. The subset of function symbols of Σ of arity n is denoted by Σ_n. A signature Σ is called *monadic* if when it contains only unary and constant function symbols ($\Sigma = \Sigma_0 \cup \Sigma_1$). The set of variables is V; given a signature Σ, we denote by $T(\Sigma, V)$ the set of terms over Σ, and by $T(\Sigma)$ the set of *ground* terms (terms without variables). A term $t \in T(\Sigma, V)$ can be conveniently seen as a function from its set of positions $Pos(t)$ (non-empty set of sequences of positive integers that is closed under prefix and left brother) into $\Sigma \cup V$. Let *Vars*(t) denote the set of variables of t, *depth*(t) its depth, $t|_p$ the subterm of t at position p, and $t[s]_p$ the replacement in t of the subterm at position p by s. The term t is called *linear* if every variable of *Vars*(t) occurs exactly once in t.

Equations are considered non-oriented, that is $\ell = r$ is identified with $r = \ell$. We call an equation $\ell = r$ *ground* when *Vars*(ℓ) = *Vars*$(r) = \emptyset$, *variable-disjoint* when *Vars*(ℓ) is disjoint with *Vars*(r), *flat* when *depth*(ℓ), *depth*$(r) \leq 1$ and *shallow* when every variable of *Vars*$(\ell) \cap$ *Vars*(r) occurs at depth at most 1 in ℓ and r. A set of equations is variable-disjoint (resp. ground, flat, shallow) when each of its equations is. Any flat equation is shallow, and any ground equation is both shallow and variable-disjoint, while in general flat or shallow equations are not necessarily variable-disjoint.

Let R be a rewrite system, and E a set of equational axioms. We write $s \xrightarrow[R]{} t$ when s rewrites to t in one step by R, and $s \xleftrightarrow[E]{} t$ when s transforms to t in one equational proof step by E. The relations $\xrightarrow[R]{*}$ and $=_E$ are the reflexive and transitive closures of respectively $\xrightarrow[R]{}$ and $\xleftrightarrow[E]{}$, that is, in the latter case, $s =_E t$ when s and t are equal modulo the set E of equations. We write $=_{E,R}$ for the reflexive, symmetric and transitive closure of $\xleftrightarrow[E]{} \cup \xrightarrow[R]{}$.

Given a finite signature Σ, a (bottom-up) *tree automaton* A is given by (Q, F, Δ) where Q is a finite set of *states*, $F \subseteq Q$ is called the set of *accepting states*, Δ is a set of rewrite rules $f(q_1, \ldots, q_n) \to q$ with $f \in \Sigma_n$, $q_1, \ldots, q_n, q \in Q$. The automaton A *accepts* a tree t iff $t \xrightarrow{*} q \in F$ by the transition rules Δ. The *language* L_A is the set of all trees accepted by A. Tree automata enjoy (almost) all the nice properties of word automata, in particular closure under Boolean operations, decidability of the emptiness problem, determinization, minimization [7].

The *convolution* operation defined below allows to code n-tuples of trees as trees over a signature of n-tuples. Let Σ be a signature with $\Box \notin \Sigma$. We define the signature $\Sigma^{[n]}$, for $n \geq 1$, as

$$\Sigma^{[n]} = \{[f_1, \ldots, f_n] \mid f_i \in \Sigma \cup \{\Box\}, f_i \neq \Box \text{ for at least one } i\}.$$

The arity of $[f_1 \ldots, f_n]$ in $\Sigma^{[n]}$ is the maximum of the arities of those f_i that are in Σ. For $t_1, \ldots, t_n \in T(\Sigma)$, the convolution $t_1 \otimes \ldots \otimes t_n$ is the tree $t \in T\big(\Sigma^{[n]}\big)$ defined by $Pos(t) = Pos(t_1) \cup \ldots \cup Pos(t_n)$, and for all $\pi \in Pos(t)$, $t(\pi) = [f_1, \ldots, f_n]$ where $f_i = t_i(\pi)$ if $\pi \in Pos(t_i)$, and $f_i = \Box$ otherwise. Projection is defined by $\pi_i(t_1 \otimes \ldots \otimes t_n) = t_i$.

For example, let $\Sigma = \{h, f, a\}$, where a is a constant, f unary, and h binary. Then we have that $f(a) \otimes h(a, f(a)) = [f, h]([a, a], [\Box, f]([\Box, a]))$.

Now, one can define *tree-automatic representations* and *tree-automatic structures* analogously to the definition given in [4] for automata over finite words. This definition applies only to so-called *relational* structures, that is structures that have only predicates in their logical language and no constants or function symbols. This is not a restriction as constants or functions can always be expressed by predicates. Let $\mathfrak{A}$ be a structure over a relational signature with relation symbols $R_1, \ldots, R_n$. A *tree-automatic representation* of $\mathfrak{A}$ is given by

1. a finite signature Σ,
2. a recognizable tree language $L_\delta \subseteq T(\Sigma)$,
3. an onto function $\nu\colon L_\delta \to |\mathfrak{A}|$ ($|\mathfrak{A}|$ denotes the universe of $\mathfrak{A}$),
4. a recognizable tree language $L_R \subseteq T(\Sigma^{[n]})$ for each relation symbol R of the signature of $\mathfrak{A}$, such that for all $t_1, \ldots, t_n \in L_\delta$, $t_1 \otimes \ldots \otimes t_n \in L_R$ if and only if $(\nu(t_1), \ldots, \nu(t_n)) \in R^{\mathfrak{A}}$ –we say that the relation $R^{\mathfrak{A}}$ is *recognizable*.

A structure is *tree-automatic* if it has a tree-automatic representation. The first-order theory of any tree-automatic structure is decidable.

Ground Tree Transducers (GTT) have been introduced in [11]. A GTT is defined by two tree automata A_1 and A_2 over the same signature Σ, and possibly with shared states. The GTT defined by A_1 and A_2 recognizes the pair $(t, t') \in T(\Sigma)^2$ iff there exists a context C, terms $t_i, t'_i \in T(\Sigma)$, and states q_i for $1 \leq i \leq n$, such that $t =$

$C[t_1, \ldots, t_n]$, $t' = C[t'_1, \ldots, t'_n]$, $t_i \xrightarrow{*} q_i$ by A_1 and $t'_i \xrightarrow{*} q_i$ by A_2. Any relation defined by a GTT is recognizable, and the set of GTT-definable relations is closed under iteration (Kleene star) [12].

3 The Case of Several Congruence Relations

Definition 1. *Let Σ be a countable signature with an upper bound on the arities of the function symbols, $(E_i)_{i\in I}$ be a finite family of finite sets of equations over Σ, and $(L_j)_{j\in J}$ a finite family of recognizable tree languages over finite subsets of the signature Σ. The first-order structure $\mathfrak{A}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J})$ is defined as follows: the universe is the set of all ground Σ-terms, there are no constant or function symbols, for every $i \in I$ we have a binary relation $=_i$, interpreted as $t_1 =_i t_2$ iff $t_1 =_{E_i} t_2$, for every $j \in J$ we have a unary relation L_j, interpreted as $L_j(t)$ iff $t \in L_j$. The structure $\mathfrak{H}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J})$ contains in addition to $\mathfrak{A}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J})$ all symbols from Σ as function symbols, interpreted as free constructor symbols.*

Note that first order logic with equality comes as a particular case, when $E_i = \emptyset$ for some i. In this case, we can write $=$ for $=_i$. This definition allows to consider a structure in which every ground term $t \in T(\Sigma)$ exists as a syntactic constant. This would be represented by having in the family of recognizable tree languages, for every $t \in T(\Sigma)$, the language consisting of the single term t only (each such language is of course recognizable). Also, note that the logical language of $\mathfrak{H}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J})$ allows to express unification problems like $x = f(y, z)$; however this is not possible in $\mathfrak{A}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J})$.

We will show that one can effectively construct, given as input a finite family $(E_i)_{i\in I}$ of linear and variable-disjoint equation systems and a finite family $(L_j)_{j\in J}$ of recognizable tree languages, a tree-automatic representation of $\mathfrak{A}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J})$. The first step is to define the encoding of the algebra as trees over a finite signature, the (minor) difficulty here being that the algebra contains trees over a possibly infinite alphabet but with a bounded arity. We elude the details.

The languages L_j, $j \in J$, are recognizable by definition. In order to show that every $=_i$, $i \in I$, is recognizable we construct a Ground Tree Transducer as follows: Given the linear and variable-disjoint equational theory $E = \{s_1 = t_1, \ldots, s_n = t_n\}$, let A_1 be the tree automaton that recognizes the set of instances of s_i in state q_i, for any i, and the set of instances of t_i in state p_i, for any i. Symmetrically, let A_2 be the tree automaton that recognizes the set of instances of s_i in state p_i, for any i, and the set of instances of t_i in state q_i, for any i. These automata can be constructed exactly because each equational axiom is linear. Since the axioms are variable-disjoint, the GTT defined by A_1 and A_2 recognizes a pair of terms (t, t') iff t is obtained from t' by a parallel equational replacement with respect to E. The transitive closure of this relation is exactly the equality relation modulo E, which is again a GTT [12], and hence recognizable. Hence:

Theorem 1. *Let Σ be an arity-bounded countable signature. The following problem is decidable: given a finite family $(E_i)_{i\in I}$ of finite sets of linear variable-disjoint equations over Σ, a finite family $(L_j)_{j\in J}$ of recognizable tree languages over Σ, and a first-order formula ϕ, does $\mathfrak{A}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J}) \models \phi$ hold?*

Thm. 1 no longer holds if generalized to the structure $\mathfrak{H}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J})$, that is if one also allows relations like $x = f(y, z)$.

Theorem 2. *It is undecidable whether a given existential closed first order formula holds in a given structure $\mathfrak{H}(\Sigma, (E_i)_{1\leq i\leq 3}, (L_j)_{1\leq j\leq 3})$ with Σ finite, E_1 and E_2 finite sets of ground equations, and $E_3 = \emptyset$.*

Proof *(sketch)* We encode the problem of acceptance of the empty tape for Turing machines. A configuration of a Turing machine M is represented as a right-comb $c_i = g(c_{i,1}, g(c_{i,2}, \ldots, g(c_{i,k}, \flat)\ldots))$ where g is a binary symbol and the constant symbols $c_{i,j}$ are either letter of the input alphabet of M, or a state of M, used to indicate the position of its head. A computation $c_0, \ldots, c_n$ of M (sequence of successive configurations) is also encoded as a right comb $f(c_0, \ldots, f(c_n, \flat))$. We consider the closed formula ϕ defined as follows:

$$\exists y, y_1, y_2, x.\, L_{sp}(y) \wedge y =_{E_1} y_1 \wedge L_c(y_1) \wedge y =_{E_2} y_2 \wedge L_c(y_2) \wedge L_0(x) \wedge y_1 = f(x, y_2)$$

where L_0 and L_c are the languages of term representations of respectively the initial configurations of M (there are several such representations because we use padding), and sequences of configurations (possibly not successive) of M, ending with a final configuration. The regular language L_{sp} contains roughly the term representation of sequences of convolution products of pairs of successive configurations (roughly, terms of the form $f(c_0 \otimes d_1, \ldots, f(c_{n-1} \otimes d_n, f(c_n \otimes \flat, \flat)))$ where the configuration d_{i+1} is obtained from c_i using a transition of M).

Moreover, E_1 and E_2 define respectively the left and right projections over the signatures of pairs. Hence ϕ holds in $\mathfrak{H}(\Sigma, (E_i)_{i\in 1,2}, (L_{sp}, L_c, L_0))$ iff M admits a successful computation (y_1) starting with an initial configuration. □

Note that the above problem is decidable for arbitrary first-order formula and structures $\mathfrak{H}(\Sigma, (E_1), \emptyset)$ where E_1 is a shallow equational system [9]. However, Thm. 1 no longer holds when one replaces variable-disjoint equational systems by flat equational systems. The signature considered in the next theorem is monadic, hence the results holds already when considering a domain of words.

Theorem 3. *It is undecidable whether a given existential closed first order formula holds in a given structure $\mathfrak{A}(\Sigma, (E_i)_{1\leq i\leq 3}, (L_j)_{1\leq j\leq 2})$ with Σ finite and monadic, E_1 and E_2 finite sets of flat equations, and $E_3 = \emptyset$.*

Proof *(sketch)* We reduce from the Post correspondence problem (PCP). Let $\mathcal{P} = \{(u_i, v_i) \mid u_i, v_i \in \{a, b\}^+, 1 \leq i \leq N\}$ be an instance of PCP and let $L := \max(|u_i|, |v_i| \mid i \leq N)$. We consider a monadic signature containing a constant symbol $\flat$ and unary function symbols a, b and $P_{i,j}$ for all $1 \leq i \leq N$ and $1 \leq j \leq L$. The purpose of the symbols $P_{i,j}$ is to represent a "skeleton" of solution of $\mathcal{P}$, *i.e.* a sequence of indexes that will be replaced by letters of the u_i's or v_i's using two sets of flat equations E_1 and E_2. In E_1, we have equations like $P_{i,j}(x) = u_{i,j}(x)$ if $1 \leq i \leq N$ and $1 \leq j \leq |u_i|$ ($u_{i,j}$ is the j^{th} letter of u_i) and $P_{i,j}(x) = x$ if $|u_i| < j$, and similarly for v_i in E_2.

Moreover, we have two tree automata: L_α recognizing $\{a, b\}^+\flat$, and L_P recognizing $\{P_{i,1} \cdots P_{i,L} \mid 1 \leq i \leq N\}^* \flat$. Finally, the closed formula $\phi := \exists x, u, v.\, L_P(x) \wedge x =_{E_1} u \wedge x =_{E_2} v \wedge L_\alpha(u) \wedge L_\alpha(v) \wedge u = v$ holds in $\mathfrak{A}\big(\Sigma, (E_i)_{1\leq i\leq 3}, (L_\alpha, L_P)\big)$ iff $\mathcal{P}$ has a solution. □

4 Adding a Background Term Rewrite System

In this section we show that Thm. 1 can be extended to the case where all equations are taken modulo an additional term rewrite system with some particular properties. The first property is that the system is *canonical*, that is normalizing and confluent, such that each term has a unique normal form. This allows us to restrict the universe of the logic structure to contain only terms in normal form, and each ground term would be interpreted in that structure as its normal form.

Definition 2. *Let Σ, $(E_i)_{i\in I}$, $(L_j)_{j\in J}$ be as in Def. 1, and R be a canonical, left-linear rewrite system. The first-order structure $\mathfrak{A}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J}, R)$ is defined as $\mathfrak{A}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J})$ in Def. 1 except that the universe is restricted to R-normal forms and that $t_1 =_i t_2$ is interpreted as $t_1 =_{E_i,R} t_2$.*

Note that the term rewrite system may indeed intervene even when the structure contains only terms in normal form, and when all equational systems are normalized with respect to the rewrite system. Take, for example, a rewrite system R consisting of the rule $\mathit{left}(\mathit{pair}(x, y)) \to x$ and the equational system $E = \{c = \mathit{pair}(a, b)\}$. The system E is normalized w.r.t. R, and so are the terms a and $\mathit{left}(c)$. However, $\mathit{left}(c) = a$ is a consequence of $E \cup R$ but not of E alone.

We say that there is a *critical pair* (CP) between two rewrite rules $\ell \to r$ and $g \to d$ if there exists a substitution σ and a non-variable position p of g such that $g\sigma \mid_p = l\sigma$, in that case the critical pair is the equation $g\sigma[r\sigma]_p = d\sigma$.

For the decidability result below we require in addition the rewrite system to be *orthogonal*, that is left-linear and without critical pairs. The set of terms in normal forms is then recognizable as a consequence of left-linearity [7]; absence of critical pairs will be useful in the proof of Thm. 4. Orthogonality implies confluence [13].

The idea is to "complete" any of the given equational systems E_i w.r.t. R, by adding the CP (which are equations) between equations and rules of R. If this process terminates for each of these systems E_i then we can conclude. Given an equation $l = r$ and a rewrite rule $g \to d$, we consider the following two cases of critical pairs:

- cp_1) There is a substitution σ and a non-variable position p of g such that $g\sigma \mid_p = l\sigma$, in that case the critical pair is $g\sigma[r\sigma]_p = d\sigma$.
- cp_2) There is a substitution σ and a non-variable position p of $l\sigma$ such that $g\sigma = l\sigma \mid_p$, in that case the critical pair is $r\sigma = l\sigma[d\sigma]_p$.

We say that E' is the *completion* of E by R when E' is the smallest set containing E and that contains all its own critical pairs with R. If this set is finite then it can be calculated from E by successive addition of critical pairs.

Lemma 1. *If R is orthogonal and E' is the completion of E by R then $s =_{E,R} t$ iff $s =_{E'} t$ for all terms s, t in R-normal form.*

Proof Any E' proof step can be simulated by several E, R proof steps, so the back direction is obvious. For the other direction, first note that when $s =_{E,R} t$ then $s =_{E',R} t$ since $E \subseteq E'$. Any proof of $s =_{E',R} t$ can be transformed into a proof such that any R-rewrite step is either preceded by an R rewrite-step, or by an E-step such that

the redex of the rewrite step has a non-trivial overlap with the previous equational step. This is a consequence of the orthogonality of R and the fact that s and t are in R-normal form, since a rewrite step can be commuted with a non-overlapping equational step. If the shortest such proof used an R-step then we could replace the preceding equational step and that rewrite step by one single equational step (their critical pair), which would yield a contradiction. □

In order to meet the hypotheses of Thm. 1, we have to assure that the critical pair is again linear and variable-disjoint. Linearity may be violated only by a non-linearity of d (since all other terms are linear), and variable disjointness may be violated in case cp_1 when $g\sigma[\bullet]_p$ is not ground. We obtain together with Lemma 1 and Thm. 1:

Theorem 4. *Let Σ be an arity-bounded countable signature, and R an orthogonal and terminating term rewrite system. There exists a decision procedure for the following problem: given a finite family $(E_i)_{i\in I}$ of finite sets of linear variable-disjoint equations over Σ, such that each E_i has a finite completion by R that is linear and variable-disjoint, given a finite family $(L_j)_{j\in J}$ of recognizable tree languages over Σ, and a first-order formula ϕ, does $\mathfrak{A}(\Sigma, (E_i)_{i\in I}, (L_j)_{j\in J}, R) \models \phi$ hold?*

Example. Let R be the term rewrite system with rules $\mathit{left}(\mathit{pair}(x, y)) \to x$, $\mathit{right}(\mathit{pair}(x, y)) \to y$ and let E be the following equational theory: $E = \{\mathit{pair}(a, \mathit{pair}(b, c)) = d\}$. Completion terminates successfully with the following equational system: $E = \{\mathit{pair}(a, \mathit{pair}(b, c)) = d, a = \mathit{left}(d),\ \mathit{pair}(b, c) = \mathit{right}(d), b = \mathit{left}(\mathit{right}(d)), c = \mathit{right}(\mathit{right}(d))\}$.

We can characterize a simple case in which completion always succeeds: we call a term a *jack* when it is either shallow and linear, or $f(t_1, \ldots, t_i, \ldots, t_n)$ such that some t_i is shallow and linear, and each t_j with $j \neq i$ is a constant.

Lemma 2. *When R is a non-overlapping rewrite system of rules $g \to x$ where each g is a jack, $x \in \mathit{Vars}(g)$, and E a ground equational system such that no constant occurring on a left-hand side of R is a side of E, then completion of any variable-disjoint and linear equation system is finite.*

Proof The rewrite system is, as an easy consequence of the hypotheses, terminating and orthogonal. Since any right-hand side is subterm of a left-hand-side, which in turn is linear, all terms involved and hence all CP are linear. If $l = r$ is an equation and $g\sigma_p = l\sigma$ an overlap, then due to the definition of jacks and the third condition in the lemma, $g\sigma[\bullet]_p$ is ground, and hence the CP is variable-disjoint. We elude the termination proof of completion. □

Here is an example of a term rewrite system that satisfies the conditions of Lem. 2. This system describes the cryptographic operators of pairing and projection, and asymmetric encryption and decryption for *fixed* keys.

$$\begin{array}{lll} \mathit{left}(\mathit{pair}(x, y)) \to x & \mathit{dec}(\mathit{enc}(x, \mathit{pub}(a)), a) \to x & \mathit{enc}(\mathit{dec}(x, \mathit{pub}(a)), a) \to x \\ \mathit{right}(\mathit{pair}(x, y)) \to y & \mathit{dec}(\mathit{enc}(x, b), \mathit{pub}(b)) \to x & \mathit{enc}(\mathit{dec}(x, b), \mathit{pub}(b)) \to x \end{array}$$

In this case, equational axioms may not contain a or b (the ground subterms of the left-hand sides of R). The generalization of these axioms to arbitrary keys represented by

a variable, *i.e.* $dec(enc(x, pub(y)), y) \to x$ would lead to a left-hand side that is not a jack. Thm. 4 does not hold when the completion is no longer variable-disjoint.

Theorem 5. *It is undecidable whether a given existential closed first order formula holds in a given structure $\mathfrak{A}(\Sigma, (E_i)_{1\leq i\leq 3}(L_j)_{1\leq j\leq 2}, R)$ with Σ finite, R containing rules of the form $f(x, c) \to x$ for $f \in \Sigma_2$, $c \in \Sigma_0$ and $x \in V$, E_1, E_2 finite sets of ground equations over Σ, $E_3 = \emptyset$.*

Proof Similarly to the proof of Thm. 3, we reduce from PCP. The main difference is that we use binary terms of the form $f(\alpha_1, \dots f(\alpha_n, \flat) \dots)$ instead of unary ones (words). The letters of the PCP alphabet and the auxiliary symbols $P_{i,j}$ are now constant symbols, and the equations of E_1 have the form $P_{i,j} = u_{i,j}$ if $1 \leq j \leq |u_i|$ or $P_{i,j} = \Box$ if $|u_i| < j \leq L$ (and similarly for v_i with E_2). The TRS contains only one rule $f(\Box, x) \to x$. □

Note that in the case of the proof of Thm. 5, the completion of an equation $P_{i,j} = \Box$ by the rule $f(\Box, x) \to x$ yields the non variable-disjoint equation $f(P_{i,j}, x) = x$.

5 Application to the Spatial Logic for Frames

In this section, we recall the definitions of the frames of the applied π-calculus (Aπ for short) and the fragment $\mathcal{FSL}$ of the spatial equational logic $A\pi\mathcal{L}$. We then show how to reduce the model-checking problem of $\mathcal{FSL}$ to the satisfaction of a first-order constraint system with multiple congruence relations and a background equational theory, which allows us to apply the results of the previous section in the context of the study of cryptographic protocols.

5.1 Frames

A *frame* is a record of the current knowledge of the environment in the form of *active substitutions*, each accounting for a message that has been sent over the network. Frames act as snapshots of the history of communications during the reduction of Aπ processes. Their study is useful for the post-mortem analysis of the knowledge leaked by a process as well as for characterizing observationally equivalent processes.

Formally, we suppose given a signature Σ that contains the disjoint and countable sets $\mathcal{V}^\pi$ and $\mathcal{N}^\pi$ representing respectively Aπ variables (not to be confused with *term* variables: from the point of view of the signature, Aπ variables are *constants*) and names. V is the usual set of (first-order) variables, distinct from $\mathcal{V}^\pi$. A frame is a pair (H, S), where $H \subseteq \mathcal{N}^\pi$ is a finite set of hidden names and S is a finite set of ground equations of the form $u = r$, where $u \in \mathcal{V}^\pi$ and r is a *ground* term (which can contain aπ variables and names, but no term variables). Following the original definition of the applied π-calculus [2], we only consider frames $F = (H, \{u_1 = r_1, \dots, u_k = r_k\})$ where the u_i's are pairwise distinct and there is no cycle in the Aπ variables (*i.e.* there is an ordering $(i_1, \dots, i_k)$ of the indices such that u_{i_j} does not appear in $r_{i_{j'}}$ when $j \leq j'$). The u_i's (resp. r_i) form the *domain* (resp. *codomain*) of F, written $dom(F)$ (resp. $codom(F)$). We suppose fixed an equational theory $\mathcal{E}$, used to model cryptographic primitives (for instance defined as a rewrite system as in the previous section).

Notations We will use the letters h, n, m, s to refer to elements of $\mathcal{N}^\pi$, u for elements of $\mathcal{V}^\pi$, a for elements of $\mathcal{N}^\pi \cup \mathcal{V}^\pi$ and x, y for elements of V. We write t for arbitrary terms in $T(\Sigma, V)$, and r for ground terms in $T(\Sigma)$. The expressions $fn(t)$ and $fav(t)$ respectively denote the sets of names and Aπ variables of t, defined as usual, and $fnav(t) := fn(t) \cup fav(t)$. These notations are lifted to the sets of free names and Aπ variables of frames and formulas in the standard way, with $fn((H, S)) := fn(S) \setminus H$. The union of *disjoint* sets is denoted by $\uplus$.

Frames are considered up to the following structural congruence relation that accounts for α-equivalence over hidden names, for vacuous hidden names, and for the rewriting of terms using the equational theory:

Definition 3. *Structural congruence $\equiv$ is the smallest equivalence relation on frames satisfying the following assertions*[5]*:*

α-CONV	$(H, S) \equiv (H[n \leftarrow n'], S[n \leftarrow n'])$	*if* $n \in H$ *and* $n' \notin H \cup fn(S)$
NEW	$(H, S) \equiv (H', S)$	*if* $H \cap fn(S) = H' \cap fn(S)$
REWRITE	$(H, \{u_1 = r_1, \ldots, u_k = r_k\}) \equiv (H, \{u_1 = r'_1, \ldots, u_k = r'_k\})$	*if* $\forall i \in \{1, \ldots, k\}.\, r_i \xleftrightarrow[\mathcal{E}]{*} r'_i$

Let us now recall the two essential notions of deducibility and static equivalence for frames. Two ground terms r_1 and r_2 are equal in the frame F, written $F \vdash_\mathcal{E} r_1 = r_2$ (or $F \vdash r_1 = r_2$ if $\mathcal{E}$ is clear from context) when there exists a frame $(H', S') \equiv F$ such that $fn(r_1, r_2) \cap H' = \emptyset$ and $r_1 \xleftrightarrow[\mathcal{E} \cup S']{*} r_2$.

Definition 4. *A ground term r is* deducible *from the frame (H, S) if there exists a term r' such that $fn(r') \cap H = \emptyset$ and $(\emptyset, S) \vdash r = r'$.*

F and F' are statically equivalent*, written $F \approx_s F'$, when $dom(F) = dom(F')$ and, for all ground terms r, r', $F \vdash r = r'$ if and only if $F' \vdash r = r'$.*

Definition 5. *Two frames $F_1 = (H_1, S_1)$ and $F_2 = (H_2, S_2)$ are* orthogonal *if $H_1 \cap H_2 = \emptyset$, $dom(F_1) \cap dom(F_2) = \emptyset$, $fn(codom(F_1)) \cap H_2 = fn(codom(F_2)) \cap H_1 = \emptyset$, and $S_1 \uplus S_2$ is acyclic. The* composition *$F = F_1 * F_2$ of orthogonal frames F_1, F_2 is the frame $(H_1 \uplus H_2, S_1 \uplus S_2)$.*

As usual, we write $F_1 \equiv F_2 * F_3$ if there are F'_1, F'_2, F'_3 such that $F'_1 = F'_2 * F'_3$ and $F_i \equiv F'_i$. For instance, the following equality holds:

$$\begin{aligned} &(\{n\}, \{u_o = pub(n)\}) * (\{n\}, \{u_1 = enc(n, u_0)\}) \\ \equiv\ &(\{k, s\}, \{u_0 = pub(k), u_1 = enc(s, u_0)\}) \end{aligned}$$

The composition of two frames requires their rewriting so as to prevent clashes of their respective hidden names, hence $(\{k\}, \{u_o = pub(k)\})$ and $(\{k, s\}, \{u_1 = enc(s, pub(k)\}))$ can be composed into $(\{k, k', s\}, \{u_0 = pub(k), u_1 = enc(s, pub(k')\})\}$ but not into $(\{k, s\}, \{u_0 = pub(k), u_1 = enc(s, pub(k))\})$.

[5] We slightly deviate from the standard structural congruence defined by Abadi and Fournet [2], as we assume that substitutions of a frame are not taken into account when rewriting the terms of this frame (for instance, in our setting, $(H, \{u_1 = u_2, u_2 = r\}) \not\equiv (H, \{u_1 = r, u_2 = r\})$). This does not change the notions of deducibility and static equivalence.

$$
\begin{array}{lll}
F, v \vDash t_1 = t_2 & \Leftrightarrow & F \vdash_{\mathcal{E}} t_1 v = t_2 v \\
F, v \vDash \mathbf{0} & \Leftrightarrow & F \equiv (\emptyset, \emptyset) \\
F, v \vDash \copyright a & \Leftrightarrow & \forall F' \equiv F.\, a \in \mathit{fnav}(F') \\
F, v \vDash \neg \Phi & \Leftrightarrow & F, v \nvDash \Phi \\
F, v \vDash \Phi_1 \wedge \Phi_2 & \Leftrightarrow & F, v \vDash \Phi_1 \text{ and } F, v \vDash \Phi_2 \\
F, v \vDash \Phi_1 * \Phi_2 & \Leftrightarrow & \exists F_1, F_2.\, F \equiv F_1 * F_2,\ F_1, v \vDash \Phi_1 \text{ and } F_2, v \vDash \Phi_2 \\
F, v \vDash \exists x.\, \Phi & \Leftrightarrow & \exists r \in T(\Sigma).\, F, (v \cup \{x \rightarrow r\}) \vDash \Phi \\
F, v \vDash \mathit{И} a.\, \Phi & \Leftrightarrow & \exists a' \notin \mathit{fnav}(F, v, \Phi).\, F, v \vDash \Phi[a \leftarrow a'] \\
F, v \vDash \mathsf{H} n.\, \Phi & \Leftrightarrow & \exists n' \notin \mathit{fn}(F, v, \Phi).\, \exists (H', S').\, \begin{array}{l} F \equiv (\{n'\} \uplus H', S') \\ \text{and } (H', S'), v \vDash \Phi[n \leftarrow n'] \end{array} \\
F, v \vDash \Phi \oslash n & \Leftrightarrow & (\{n\} \cup H, S), v \vDash \Phi
\end{array}
$$

Fig. 1. Satisfaction relation of $\mathcal{FSL}$ for a frame $F = (H, S)$

5.2 The frame logic $\mathcal{FSL}$

Consider the fragment $\mathcal{FSL}$ of $A\pi\mathcal{L}$ formed by the formulas Φ of the following grammar, where $t_1, t_2 \in T(\Sigma, V)$, $a \in \mathcal{N}^\pi \uplus \mathcal{V}^\pi$, $x \in V$, and $n \in \mathcal{N}^\pi$.

$$\Phi ::= t_1 = t_2 \mid \mathbf{0} \mid \copyright a \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 * \Phi_2 \mid \exists x.\, \Phi \mid \mathit{И} a.\, \Phi \mid \mathsf{H} n.\, \Phi \mid \Phi \oslash a$$

The semantics of the logic is given by a satisfaction relation between a frame $F = (H, S)$, a valuation v mapping term variables of V to ground terms of $T(\Sigma)$, and a formula Φ. It is shown in Fig. 1, and is devised so as not to distinguish between structurally congruent frames. Intuitively, $t_1 = t_2$ is an equality test under the ambient equational theory $\mathcal{E}$ augmented by the equalities in F, $\mathbf{0}$ describes empty frames, $\copyright a$ is true whenever the name or Aπ variable a appears free in all the frames structurally congruent to F, $\neg$, $\wedge$ and $\exists$ is the classical first-order fragment, $\mathit{И} a$ is the Gabbay-Pitts quantifier over fresh names or Aπ variables (*i.e.* it quantifies over names–or Aπ variables–that do not appear free in neither the frame nor the remaining formula), $\mathsf{H} n$ is a quantifier over hidden names of the frame (intuitively, it reveals a secret name of the frame, which may be vacuous if it does not appear free in the set of equations S of F), $*$ is the spatial conjunction that decomposes F into two orthogonal subframes, and $\Phi \oslash n$ hides the name n in F and proceeds with Φ.

For instance, the deducibility of a secret name (without specifying which one) is expressed by $\exists x.\, \mathsf{H} k.\, x = k$: as the term quantification is placed first, the guessed term x cannot mention the revealed name k. The general deducibility problem is also expressible in this fragment, but the formula depends on the frame $F = (\{h_1, \ldots, h_l\}, \{u_1 = t_1, \ldots, u_k = t_k\})$ due to α-conversion issues:

$$\mathsf{deducible}(F, t) := \exists x.\, \mathsf{H} h_1, \ldots, h_l.\, (x = t \wedge u_1 = t_1 \wedge \ldots \wedge u_k = t_k)$$

Other security properties are expressible using spatial logics, for instance regarding the quantity of information leaked in a frame: $\exists x.\, \mathsf{H} k.\, x = k$ holds if there is at least one secret leaked by the frame, while $\exists x, y.\, \mathsf{H} k, k'.\, x = k \wedge y = k'$ asserts that two independent secrets are. The formulas presented in the introduction also fit our fragment.

5.3 From spatial to equational

In this section, we reduce the model-checking problem for $\mathcal{FSL}$ to the evaluation of an equational formula over a term algebra. We assume given a signature $\Sigma \supseteq \mathcal{N}^\pi \uplus \mathcal{V}^\pi$ and an equational theory $\mathcal{E}$ defined by an orthogonal, terminating term rewrite system $R_\mathcal{E}$. Moreover, we can assume that all the rewrite rules in $R_\mathcal{E}$ mention only variables, and no constants, as it is always the case in Aπ equational theories. For every finite set S of ground equations of the form $u = r$, $=_S$ denotes $\overset{*}{\underset{S \cup \mathcal{E}}{\leftrightarrow}}$. Consider the first-order logic $\mathcal{L}_{\text{eq}}$ defined by the following grammar (we omit its semantics for brevity):

$$\phi ::= t_1 =_S t_2 \mid n \in \mathit{fn}(t) \mid u \in \mathit{fav}(t) \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid \exists x.\, \phi \mid \mathit{\Nu} n.\, \phi$$

Let $\mathfrak{A} := \mathfrak{A}(\Sigma, (=_S)_S, (\mathcal{C}_a)_{a \in \mathcal{N}^\pi \uplus \mathcal{V}^\pi}, R_\mathcal{E})$ where $C_a := \{t \mid a \in \mathit{fnav}(t)\}$. We give below a translation $H, S, \Phi \mapsto (\!|H, S, \Phi|\!)$ that associates an equational formula in $\mathcal{L}_{\text{eq}}$ to a frame (H, S) and a spatial formula Φ, built by induction on Φ with the following inductive hypothesis:

Lemma 3. *For all v, H, S and Φ, $\mathfrak{A}, v \vDash (\!|H, S, \Phi|\!)$ if and only if $(H, S), v \vDash \Phi$.*

Notations We write $\boldsymbol{t} = \boldsymbol{t'}$ for $\bigwedge_{i=1}^n t_i = t'_i$ (and similarly for sets of terms) and $m \in \mathit{fn}(\boldsymbol{t})$ for $\bigvee_{i=1}^n m \in \mathit{fn}(t_i)$ (and similarly for $u \in \mathit{fav}(\boldsymbol{t})$). Arities are implicitly supposed to match: in $\exists \boldsymbol{t}.\, \boldsymbol{t} = \mathit{codom}(S)$, $\boldsymbol{t}$'s size is implicitly chosen to match the size of $\mathit{codom}(S)$. Finally, $\top$ (resp. $\bot$) is a formula that is always true (resp. always false), for instance $n = n$ for some n (resp. $\neg n = n$).

The translation of $\copyright a$ follows its semantics and thus is quite straightforward. It is defined as $\bot$ when $a \in H$, $\top$ when $a \in \mathit{dom}(S)$, and otherwise as

$$(\!|H, S, \copyright a|\!) := \forall \boldsymbol{x}.\, \boldsymbol{x} =_\emptyset \mathit{codom}(S) \Rightarrow a \in \mathit{fnav}(\boldsymbol{x})$$

Hiding a name consists merely of adding h to the set of hidden names, and term quantification is left as-is, since the semantics of $\exists x$ for $\mathcal{FSL}$ and $\mathcal{L}_{\text{eq}}$ are the same. As we know all the hidden names of the frame, we can treat name revelation as a disjunction over those names and a fresh name n', the latter accounting for the fact that one can reveal "fake" hidden names (using NEW):

$$(\!|H, S, \Phi \oslash n|\!) := (\!|H \cup \{n\}, S, \Phi|\!) \qquad (\!|H, S, \exists x.\, \Phi|\!) := \exists x.\, (\!|H, S, \Phi|\!)$$

$$(\!|H, S, \mathsf{H} n.\, \Phi|\!) := \mathit{\Nu} n'.\ \bigvee_{h \in H \uplus \{n'\}} (\!|H \setminus \{h\}, S, \Phi[n \leftarrow h]|\!)$$

To translate an equality $t_1 = t_2$ one has to take care of the hidden names of S, as $\mathcal{L}_{\text{eq}}$ only allows substitutions as parameters of equality tests, and not general frames. To overcome this, we simulate the behavior of hidden names by replacing the names of S that appear in H with fresh names H' such that $H' \cap \mathit{fn}(S, t_1, t_2) = \emptyset$. It is easy to check that these fresh names behave like hidden names for the equality test.

$$\begin{aligned}&(\!|\{h_1, \ldots, h_k\}, S, t_1 = t_2|\!) := \\ &\quad \mathit{\Nu} h'_1, \ldots, h'_k.\, t_1[h_1, \ldots, h_k \leftarrow h'_1, \ldots, h'_k] =_S t_2[h_1, \ldots, h_k \leftarrow h'_1, \ldots, h'_k]\end{aligned}$$

To translate $*$, we need to be able to state that the set of hidden names appearing in two subframes are disjoint one from another up to rewriting of terms using the equational theory. This is achieved by the operator $\boldsymbol{t}_1 \bot^H \boldsymbol{t}_2$ below which states that two sets of names $\boldsymbol{t}_1$ and $\boldsymbol{t}_2$ may be rewritten so as not to share names in H:

$$\boldsymbol{t}_1 \bot^H \boldsymbol{t}_2 := \exists \boldsymbol{x}_1, \boldsymbol{x}_2.\, \boldsymbol{x}_1 =_\emptyset \boldsymbol{t}_1 \wedge \boldsymbol{x}_2 =_\emptyset \boldsymbol{t}_2 \wedge \bigwedge_{h \in H} (h \in fn(\boldsymbol{x}_1) \Rightarrow h \notin fn(\boldsymbol{x}_2))$$

The translation of frame composition then only needs to quantify over all 2-partitions of the set of active substitutions that yield orthogonal subframes:

$$(\!|H, S, \Phi_1 * \Phi_2|\!) := \bigvee_{S_1 \uplus S_2 = S} (codom(S_1) \bot^H codom(S_2) \wedge (\!|H, S_1, \Phi_1|\!) \wedge (\!|H, S_2, \Phi_2|\!))$$

This particular step of our translation would be unsound if substitutions of the frame could be applied to other substitutions of the frame, like in the original applied π-calculus. Finally, $(\!|H, S, \neg\Phi|\!) := \neg(\!|H, S, \Phi|\!)$, $(\!|H, S, \Phi_1 \wedge \Phi_2|\!) := (\!|H, S, \Phi_1|\!) \wedge (\!|H, S, \Phi_2|\!)$, and $(\!|H, S, \mathbf{0}|\!) := \top$ if $S = \emptyset$ and $\bot$ otherwise. From the inductive hypothesis of Lem. 3 we deduce:

Theorem 6. *For all frame $F = (H, S)$ and formula Φ of $\mathcal{FSL}$ one can effectively compute a formula ϕ of $\mathcal{L}_{eq}$ such that $F \vDash \Phi$ if and only if $\mathfrak{A} \vDash \phi$. Moreover, the predicates $=_{S'}$ that appear in ϕ are all such that $S' \subseteq S$.*

5.4 Deciding the model-checking of $\mathcal{FSL}$ and static equivalence

We now show how to apply Thm. 4 to the decidability of security properties of frames, namely the ones expressible in $\mathcal{FSL}$, as well as static equivalence.

Theorem 7. *Let (H, S) be a frame such that the completion of S under $R_\mathcal{E}$ terminates and is linear and variable disjoint. Then the problem to decide, for a formula $\Phi \in \mathcal{FSL}$, whether (H, S) satisfies Φ is decidable when the comparisons are all of the form $r =_{S'} r'$, $x =_{S'} r$ or $x =_{S'} x'$ where $S' \subseteq S$.*

Proof Let us write $\mathcal{A}_\phi$ (resp. $\mathcal{S}_\phi$) for the *finite* set of a (resp. S') such that $a \in fn(t)$ or $a \in fav(t)$ (resp. $=_{S'}$) appears in ϕ, and $\mathfrak{A}_\phi$ for $\mathfrak{A}(\Sigma, (=_{S'})_{S' \in \mathcal{S}_\phi}, (C_a)_{a \in \mathcal{A}_\phi}, R_\mathcal{E})$. For ϕ to be a formula over this structure (which does not include function symbols), the comparisons $t_1 =_S t_2$ have to be restricted to those of the forms $r =_S r'$, $x =_S r$ or $x =_S x'$ (where $r, r' \in T(\Sigma)$ denote *ground* terms and $x, x' \in V$ are term variables). This restriction corresponds to the hypothesis of the theorem on Φ, which is satisfied by all the formulas presented in this paper.

Let us observe that one can eliminate Gabbay-Pitts quantifiers in any formula by first rewriting the formula in prenex form (the only non-homomorphic case being $\exists x.\, \mathit{\Nu} n.\, \phi \Leftrightarrow \mathit{\Nu} n.\, \exists x.\, (\neg n \in fn(x)) \wedge \phi$), and then dropping them. Since by hypothesis the completion of S terminates under $R_\mathcal{E}$, the completions of every $S' \subseteq S$ also terminates. Moreover, the equations $=_{S'}$ are over ground terms, hence are trivially linear and variable-disjoint, and the languages C_a are all recognizable. Thus Thm. 4 applies on $\mathfrak{A}_\phi$, which shows that the satisfiability problem $\overset{?}{\vDash} \phi$ for the logic $\mathcal{L}_{\text{eq}}$ is decidable. □

In particular, the model-checking problem of $\mathcal{FSL}$ is decidable whenever the conditions on $R_{\mathcal{E}}$ and S of Lemma 2 are satisfied, hence for the equational theory of pairs or of fixed key symmetric or asymmetric encryption (or any combination thereof), whatever the considered frame S is.

This result also applies with the original definition of structural congruence for frames by Abadi and Fournet [2] (see the footnote page 11). However, our translation of the $*$ logical operator would not produce a finite formula anymore, hence this connector would have to be dropped to retain decidability. One may also easily add the Aπ variable hiding operator of $A\pi\mathcal{L}$ $\Phi \oslash u$, which we omitted to simplify our syntax for frames (in which hidden variables have no meaning), without impairing Thm. 7.

Finally, $\mathcal{L}_{\text{eq}}$ can also express static equivalence between two frames $F = (\{h_i\}_i, S)$ and $F' = (\{h'_i\}_i, S')$ by the following formula, thus providing a decidable way of deciding such a relation when the equational theory obeys the constraints above:

$$F \approx_s F' \text{ iff } \forall x, x'.\ \bigwedge_{i,i'} \neg h_i h'_{i'} \in \mathit{fn}(x, x') \Rightarrow (x =_S x' \Leftrightarrow x =_{S'} x')$$

6 Conclusion

Classically used decision procedures for first-order theories seem not be applicable when faced with multiple congruence relations defined by independent equational axioms. Automata-based methods, on the other hand, have the advantage that the combination of different predicates, each of them recognizable for the same encoding of the elements of the algebra, comes for free. However, they can handle only restricted classes of equational axioms. Whether it is possible to push the method to, for instance, non left-linear background equational theories like $check(x, pub(k), sign(x, k)) \rightarrow ok$ is up to future work.

As an application, we have obtained a decidability result for the model-checking of a rich fragment of $A\pi\mathcal{L}$ and static equivalence, under a class of realistic equational theories. It is incomparable with previous decidability results obtained for deducibility and static equivalence only [1]. Considering a larger fragment of $A\pi\mathcal{L}$ would be challenging, in particular in the handling of Aπ variable revelation $\mathsf{H}u.\Phi$, which is not supported in our setting as it amounts to quantifying over a new, unknown substitution $u = r$ against which terms can be tested. Such an extension would require not only to consider multiple congruence relations, but also to quantify over them. We conjecture that techniques similar to those exposed in this paper could be applied to the study of the model-checking of the frame logic of Hüttel and Pedersen.

References

1. M. Abadi and V. Cortier. Deciding Knowledge in Security Protocols under Equational Theories. *Theoretical Computer Science*, 367(1-2):2–32, 2006.
2. M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *POPL'01*.

3. F. Baader and W. Snyder. Unification theory. In *Handbook of Automated Reasoning*, volume I, chapter 8, pages 445–532. Elsevier and MIT Press, 2001.
4. A. Blumensath and E. Grädel. Automatic structures. In *Logic in Computer Science*, pages 51–62, Santa Barbara, CA, June 2000.
5. A.-C. Caron, J.-L. Coquide, and M. Dauchet. Encompassment properties and automata with constraints. In *RTA*, volume 690 of *LNCS*, pages 328–342. Springer, 1993.
6. H. Comon. Solving symbolic ordering constraints. *IJCS*, 1(4):387–412, 1990.
7. H. Comon, M. Dauchet, R. Gilleron, C. Löding, F. Jacquemard, D. Lugiez, S. Tison, and M. Tommasi. Tree automata techniques and applications. Available on: `http://www.grappa.univ-lille3.fr/tata`, 2007. release October, 12th 2007.
8. H. Comon and C. Delor. Equational formulae with membership constraints. *Information and Computation*, 112(2):167–216, Aug. 1994.
9. H. Comon, M. Haberstrau, and J.-P. Jouannaud. Syntacticness, cycle-syntacticness and shallow theories. *Information and Computation*, 111(1):154–191, May 1994.
10. H. Comon and P. Lescanne. Equational problems and disunification. *Journal of Symbolic Computation*, 7:371–425, 1989.
11. M. Dauchet, S. Tison, T. Heuillard, and P. Lescanne. Decidability of the confluence of ground term rewriting systems. In *LICS*, pages 353–359, 1987.
12. M. Dauchet, S. Tison, T. Heuillard, and P. Lescanne. Decidability of the confluence of finite ground term rewrite systems and of other related term rewrite systems. *Information and Computation*, 88(2):187–201, October 1990.
13. G. Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *J. ACM*, 27(4):797–821, Oct. 1980.
14. H. Hüttel and M. D. Pedersen. A logical characterisation of static equivalence. *Electronic Notes in Theoretical Computer Science*, 173:139–157, 2007.
15. J.-P. Jouannaud and M. Okada. Satisfiability of systems of ordinal notation with the subterm property is decidable. In *ICALP*, volume 510 of *LNCS*, pages 455–468, 1991.
16. V. Kuncak and M. C. Rinard. Structural subtyping of non-recursive types is decidable. In *Logic in Computer Science*, pages 96–107, Ottawa, Canada, June 2003.
17. É. Lozes and J. Villard. A spatial equational logic for the applied π-calculus. In *CONCUR*, volume 5201 of *LNCS*, pages 387–401. Springer, 2008.
18. É. Lozes and J. Villard. A spatial equational logic for the applied π-calculus. *Distributed Computing*, 23(1):61–83, Sept. 2010.
19. M. J. Maher. Complete axiomatizations of the algebras of finite, rational and infinite trees. In *LICS*, pages 348–357, Edinburgh, Scotland, UK, July 1988.
20. A. I. Malc'ev. Axiomatizable classes of locally free algebras of various type. In *The Metamathematics of Algebraic Systems: Collected Papers 1936–1967*, chapter 23. 1971.
21. J. Marcinkowski. Undecidability of the $\exists^*\forall^*$ part of the theory of ground term algebra modulo an AC symbol. In *RTA*, volume 1631 of *LNCS*, pages 92–102, 1999.
22. Z. Su, A. Aiken, J. Niehren, T. Priesnitz, and R. Treinen. The first-order theory of subtyping constraints. In *POPL*, pages 203–216. ACM, 2002.
23. R. Treinen. A new method for undecidability proofs of first order theories. *Journal of Symbolic Computation*, 14(5):437–457, Nov. 1992.