An Equation-Based Classical Logic*

Andreia Mordido and Carlos Caleiro

SQIG – Instituto de Telecomunicações
Dep. Mathematics, IST – Universidade de Lisboa, Portugal

Abstract. We propose and study a logic able to state and reason about equational constraints, by combining aspects of classical propositional logic, equational logic, and quantifiers. The logic has a classical structure over an algebraic base, and a form of universal quantification distinguishing between local and global validity of equational constraints. We present a sound and complete axiomatization for the logic, parameterized by an equational specification of the algebraic base. We also show (by reduction to SAT) that the logic is decidable, under the assumption that its algebraic base is given by a convergent rewriting system, thus covering an interesting range of examples. As an application, we analyze offline guessing attacks to security protocols, where the equational base specifies the algebraic properties of the cryptographic primitives.

Key words: classical logic, equational logic, completeness, decidability.

1 Introduction

The development of formal methods for the analysis of security protocols is a very active research area. Obviously, 'formal methods' should be read as 'logics', but the situation is more complicated. In fact, the problem at hand is usually so intricate that suitable fully-fledged logics have not been developed, and the reasoning is usually carried over in an underspecified higher-order metalogic, often incorporating many ingredients, ranging from equational to probabilistic reasoning, from communication and distribution, to temporal or epistemic reasoning [8].

In this paper we present and study a logic aimed at dealing with the reasoning necessary to the static analysis of so-called *offline guessing attacks* [4]. Typically, an attacker eavesdrops the network and gets hold of a number of messages exchanged by the parties. These messages are usually generated from random data and cyphered using secret keys, being immediately unreadable, but often are known to have strong algebraic relationships between them. If the

* This work was done in the scope of R&D Unit 50008, financed by the applicable financial framework (FCT/MEC through national funds and when applicable co-funded by FEDER–PT2020 partnership agreement). The first author was also supported by FCT under the doctoral grant SFRH/BD/77648/2011 and by the Calouste Gulbenkian Foundation under *Programa de Estímulo à Investigação* 2011. The second author also acknowledges the support of EU FP7 Marie Curie PIRSES-GA-2012-318986 project GeTFun: Generalizing Truth-Functionality.

attacker tries to guess the secret keys (a realistic hypothesis in many scenarios, including human-picked passwords, or protocols involving devices with limited computational power) he may use these relationships to validate his guess.

The logic is designed as a simple *global* classical logic built on top of a *local* equational base. These two layers are permeated by a second-order-like quantification mechanism over *outcomes*. Intuitively, the attacker refers to messages using *names* whose concrete values are not important, but are gathered in a set of *possible outcomes*. The local layer allows us to reason about and define equational constraints on individual outcomes. At the global layer, we can state and reason about properties of the set of all possible outcomes[1]. Interestingly, the quantification we use can be understood as an $S5$-like modality, which also explains why we will not need to consider nested quantifiers. The logic bears important similarities with exogenous logics in the sense of [11], and with probabilistic logics as developed, for instance, in [9].

We provide a sound and complete deductive system for the logic, given a Horn-clause equational specification of the algebraic base. We also show that the logic is decidable when the base equational theory can be given by means of a convergent rewriting system. Our decidability proof is actually more informative, as we develop a satisfiability procedure for our logic by means of a reduction to satisfiability for propositional classical logic. This strategy is useful as it provides the means to building prototype tools for the logic using available SAT-solvers, and uses techniques that are similar to those used in the SMT literature [12].

The paper is outlined as follows: in Section 2 we recall several useful notions of universal algebra and equational reasoning and fix some notation; then, in Section 3, we define our logic, its syntax and semantics, as well as a deductive system, whose soundness and completeness we prove, assuming that we are given an equational specification of the algebraic base; Section 4 is dedicated to showing, via a reduction to classical SAT, that our logic is decidable whenever the equational base is given by means of a convergent rewriting system; finally, in Section 5, we assess our contributions and discuss future work. We illustrate the usefulness of our logic with meaningful examples, namely related to the analysis of offline guessing attacks to security protocols. We add an Appendix with detailed proofs of some auxiliary results.

2 Algebraic preliminaries

Let us consider $F = \{F_n\}_{n\in\mathbb{N}}$ a $\mathbb{N}$-indexed family of countable sets F_n of function symbols of arity n. Given a set of generators G, we define the set of terms over G, $T_F(G)$, to be the carrier of the free F-algebra $\mathbb{T}_F(G)$ with generators in G. Throughout the text we drop the subscript F when it is clear from context. The

[1] This terminology stems from the intuition that names could be sampled from a distribution. As we discuss in the conclusion, our aim is indeed to add a probabilistic component to this logic. For the moment, however, outcomes should just be understood as being obtained non-deterministically.

set of subterms of a term $t \in T(G)$ is defined as usual and will be denoted by $subterms(t)$. Given sets G_1, G_2, a substitution is a function $\sigma : G_1 \to T(G_2)$ that can be easily extended to the set of terms over G_1, $\sigma : T(G_1) \to T(G_2)$.

We use $t_1 \approx t_2$ to represent an equation between terms $t_1, t_2 \in T(G)$. The set of all equations over G is denoted by $Eq(G)$. A Horn-clause over G is an expression $t_1 \approx t'_1 \& \ldots \& t_k \approx t'_k \Rightarrow t \approx t'$, with $k \geq 0$ and $t_1, \ldots, t_k, t'_1, \ldots, t'_k \in T(G)$. A clause is simply an equation when $k = 0$.

Fix a countable set of variables X and let us dub *algebraic terms* the elements of $T(X)$. $vars(t)$ stands for the set of variables in $t \in T(X)$. Given a F-algebra $\mathbb{A}$ with carrier set A, an assignment is a function $\pi : X \to A$, that is extended as usual to the set of algebraic terms, $[\![\cdot]\!]^{\pi}_{\mathbb{A}} : T(X) \to A$. We use A^X to denote the set of all assignments. The interpretation of a Horn clause in an algebra $\mathbb{A}$ with respect to $\pi \in A^X$ is defined by: $\mathbb{A}, \pi \Vdash t_1 \approx t'_1 \& \ldots \& t_k \approx t'_k \Rightarrow t \approx t'$ if $[\![t_1]\!]^{\pi}_{\mathbb{A}} = [\![t'_1]\!]^{\pi}_{\mathbb{A}}, \ldots, [\![t_k]\!]^{\pi}_{\mathbb{A}} = [\![t'_k]\!]^{\pi}_{\mathbb{A}}$ implies $[\![t]\!]^{\pi}_{\mathbb{A}} = [\![t']\!]^{\pi}_{\mathbb{A}}$. An algebra $\mathbb{A}$ satisfies a Horn clause if it is satisfied by $\mathbb{A}$ along with each $\pi \in A^X$. More generally, a Horn clause is satisfied in a class of algebras $\mathcal{A}$ if it is satisfied in every $\mathbb{A} \in \mathcal{A}$.

Later on, we will equip the signature F with a clausal theory represented by a set of Horn clauses Γ. The clausal theory of Γ, $Th(\Gamma)$, is the least set of clauses containing Γ that is stable under reflexivity, symmetry, transitivity and congruence and under application of substitutions. An equational theory is simply a clausal theory where Γ is composed by equations. We are particularly interested in equational theories generated by convergent rewriting systems. A rewriting system R is a finite set of rewrite rules $l \to r$, where $l, r \in T(X)$ and $vars(r) \subseteq vars(l)$. Given a rewriting system R and a set of generators G, the rewriting relation $\to_R \subseteq T(G) \times T(G)$ on $T(G)$ is the smallest relation such that:

- if $(l \to r) \in R$ and $\sigma : X \to T(G)$ is a substitution then $l\sigma \to_R r\sigma$
- if $f \in F_n$, $t_1, \ldots, t_n, t'_i \in T(G)$ and there exists $i \in \{1, \ldots, n\}$ such that $t_i \to_R t'_i$ then $f(t_1, \ldots, t_i, \ldots, t_n) \to_R f(t_1, \ldots, t'_i, \ldots, t_n)$.

We denote by $\to^*_R$ the reflexive and transitive closure of $\to_R$. R is confluent if, given $t \in T(G)$, $t \to^*_R t'$ and $t \to^*_R t''$ implies that there exists $t^* \in T(G)$ such that $t' \to^*_R t^*$ and $t'' \to^*_R t^*$. R is terminating if there exists no infinite rewriting sequence. R is convergent if it is confluent and terminating. If a rewriting system is convergent then any $t \in T(G)$ has a unique normal form (see [3]), i.e., there exists a term $t{\downarrow} \in T(G)$ such that $t \to^*_R t{\downarrow}$ and $t{\downarrow}$ is irreducible. The equational theory generated by a convergent rewriting system R is the relation $\approx_R \subseteq T(G) \times T(G)$ such that $t_1 \approx_R t_2$ if and only if $t_1{\downarrow} = t_2{\downarrow}$, also said to be a convergent equational theory, and is known to always be decidable (see [3]).

3 The logic

The logic relies on fixing a signature F and class $\mathcal{A}$ of F-algebras. We also introduce a countable set of *names* N, distinct from variables. We dub elements of $T(N)$ as *nominal terms*, and let $names(t)$ stand for the set of names that occur in $t \in T(N)$. Names can be thought of as being associated to values that are not

made explicit. We call *outcome* to each possible concrete assignment of values to names. The language of the logic, designed in order to express equational constraints locally on each outcome, but also global properties of the set of all intended outcomes, is the set Glob defined by the following grammar:

$$\begin{aligned} \mathit{Glob} &::= \forall \mathit{Loc} \mid \neg \mathit{Glob} \mid \mathit{Glob} \wedge \mathit{Glob} \\ \mathit{Loc} &::= \mathit{Eq}(N) \mid \neg \mathit{Loc} \mid \mathit{Loc} \wedge \mathit{Loc}. \end{aligned}$$

We abbreviate $\neg(t_1 \approx t_2)$ by $t_1 \not\approx t_2$ for any $t_1, t_2 \in T(N)$, and also use the usual abbreviations: $\psi_1 \vee \psi_2$ abbr. $\neg(\neg\psi_1 \wedge \neg\psi_2)$, $\psi_1 \to \psi_2$ abbr. $\neg\psi_1 \vee \psi_2$, $\psi_1 \leftrightarrow \psi_2$ abbr. $(\psi_1 \to \psi_2) \wedge (\psi_2 \to \psi_1)$, where either $\psi_1, \psi_2 \in \mathit{Loc}$ or $\psi_1, \psi_2 \in \mathit{Glob}$. Note that both the local and global languages are classical: the former with an equational base and the later over local formulas instead of propositional variables. We extend the notion of subterm to global formulas in a standard way. Similarly, we generalize the notion of names occurring in a nominal term to local and global formulas. We define the set of subformulas of either a local or a global formula ψ in the usual way and denote it by $\mathit{subform}(\psi)$.

Given a nominal term $t_0 \in T(N)$, a set of names $\tilde{n} = \{n_1, \ldots, n_k\} \subseteq N$ such that $\mathit{names}(t_0) \subseteq \tilde{n}$ and $\tilde{t} = \{t_1, \ldots, t_k\} \subseteq T(N)$ we denote by $[t_0]^{\tilde{n}}_{\tilde{t}}$ the nominal term obtained by replacing each occurrence of n_i by t_i, $i \in \{1, \ldots, k\}$, i.e., $[t_0]^{\tilde{n}}_{\tilde{t}} = \sigma(t)$ where σ is a substitution such that $\sigma(n_i) = t_i$ for each i. This notion is easily extended to local formulas.

Analogously, given a nominal term $t_0 \in T(N)$, a set of constant symbols $\tilde{c} = \{c_1, \ldots, c_k\} \subseteq F_0$ and $\tilde{t} = \{t_1, \ldots, t_k\} \subseteq T(N)$ we denote by $[t_0]^{\tilde{c}}_{\tilde{t}}$ the term that is obtained by replacing each occurrence of c_i by t_i, $i \in \{1, \ldots, k\}$. We can extend this notion of replacement to local and global formulas as well.

As explained above, names carry a form of undeterminedness, i.e., their values are fixed but we have no explicit knowledge about them. Given a F-algebra $\mathbb{A} = \langle A, -^{\mathbb{A}} \rangle$, we define an outcome as a function $\rho : N \to A$ and the set of all outcomes will be denoted by A^N. The interpretation of terms $[\![\cdot]\!]^{\rho}_{\mathbb{A}} : T_F(N) \to A$ is defined as usual. The satisfiability of local formulas is defined inductively by:

- $\mathbb{A}, \rho \Vdash_{loc} t_1 \approx t_2$ iff $[\![t_1]\!]^{\rho}_{\mathbb{A}} = [\![t_2]\!]^{\rho}_{\mathbb{A}}$
- $\mathbb{A}, \rho \Vdash_{loc} \neg\varphi$ iff $\mathbb{A}, \rho \nVdash_{loc} \varphi$
- $\mathbb{A}, \rho \Vdash_{loc} \varphi_1 \wedge \varphi_2$ iff $\mathbb{A}, \rho \Vdash_{loc} \varphi_1$ and $\mathbb{A}, \rho \Vdash_{loc} \varphi_2$.

Definition 1. A *F-structure* is a pair $(\mathbb{A}, S)$ where $\mathbb{A} = \langle A, -^{\mathbb{A}} \rangle$ is a F-algebra and $S \subseteq A^N$ is a non-empty set of *possible outcomes*.

Satisfaction of global formulas by a F-structure is defined inductively by:

- $(\mathbb{A}, S) \Vdash \forall\varphi$ iff $\mathbb{A}, \rho \Vdash_{loc} \varphi$ for every $\rho \in S$
- $(\mathbb{A}, S) \Vdash \neg\delta$ iff $\mathbb{A}, S \nVdash \delta$
- $(\mathbb{A}, S) \Vdash \delta_1 \wedge \delta_2$ iff $\mathbb{A}, S \Vdash \delta_1$ and $\mathbb{A}, S \Vdash \delta_2$.

As usual, given $\Delta \subseteq \mathit{Glob}$ we write $\mathbb{A}, S \Vdash \Delta$ if $\mathbb{A}, S \Vdash \delta$ for every $\delta \in \Delta$.

Definition 2. *Semantic consequence* is defined, as usual, by $\Delta \models_{\mathcal{A}} \delta$ whenever $(\mathbb{A}, S) \Vdash \Delta$ implies $(\mathbb{A}, S) \Vdash \delta$, for any F-structure $(\mathbb{A}, S)$ with $\mathbb{A} \in \mathcal{A}$.

Example 1. Consider the signature F^{com} where we require $s \in F_2^{com}$, and let $\mathcal{A}$ be the class of F^{com}-algebras satisfying the set of equations $\Gamma = \{s(x_1, x_2) \approx s(x_2, x_1)\}$, i.e., $\mathcal{A}$ is the class of all commutative groupoids. Then, for $n, m, a, b, c \in N$, we have:
$\forall(n \approx a \vee n \approx b), \forall(m \approx a \vee m \approx b), \forall(s(a, b) \approx c) \models_{\mathcal{A}} \forall(n \not\approx m \to s(n, m) \approx c)$.

Example 2. A standard example of an equational theory used in information security for formalizing (part of) the capabilities of a so-called *Dolev-Yao attacker* (see, for instance, [4, 2, 1]) consists in taking a signature F^{DY} with $\{\cdot\}_\cdot, \{\cdot\}_\cdot^{-1} \in F_2$, representing symmetric encryption and decryption of a message with a key, $(\cdot, \cdot) \in F_2$, representing message pairing, and $\pi_1, \pi_2 \in F_1$ representing projections. The algebraic properties of these operations are given by $\Gamma = \{\{\{x_1\}_{x_2}\}_{x_2}^{-1} \approx x_1, \pi_1(x_1, x_2) \approx x_1, \pi_2(x_1, x_2) \approx x_2\}$. Let $\mathcal{A}$ be the class of all algebras satisfying Γ. Then, we have that

$$\models_{\mathcal{A}} \forall(m \approx k) \to \forall\left(\{\{n\}_k\}_m^{-1} \approx \pi_2(a, n)\right).$$

3.1 Deductive system

In order to obtain a sound and complete deductive system for our logic, we must additionally require that the basic class $\mathcal{A}$ of algebras be axiomatized by a set Γ of Horn-clauses. From there, we can define the deductive system $\mathcal{H}_\Gamma$ as follows:

Eq1 $\dfrac{}{\forall(t \approx t)}$

Eq2 $\dfrac{}{\forall(t_1 \approx t_2 \to t_2 \approx t_1)}$

Eq3 $\dfrac{}{\forall(t_1 \approx t_2 \wedge t_2 \approx t_3 \to t_1 \approx t_3)}$

Eq4 $\dfrac{}{\forall(t_1 \approx t'_1 \wedge \ldots \wedge t_n \approx t'_n \to f(t_1, \ldots, t_n) \approx f(t'_1, \ldots, t'_n))}$

EqC1 $\dfrac{}{\forall(\varphi_1 \to (\varphi_2 \to \varphi_1))}$

EqC2 $\dfrac{}{\forall((\varphi_1 \to (\varphi_2 \to \varphi_3)) \to ((\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3)))}$

EqC3 $\dfrac{}{\forall((\neg\varphi_1 \to \neg\varphi_2) \to (\varphi_2 \to \varphi_1))}$

EqC4 $\dfrac{}{\forall(\varphi_1 \to ((\varphi_1 \to \varphi_2) \to \varphi_2))}$

C1 $\dfrac{}{\delta_1 \to (\delta_2 \to \delta_1)}$

C2 $\dfrac{}{(\delta_1 \to (\delta_2 \to \delta_3)) \to ((\delta_1 \to \delta_2) \to (\delta_1 \to \delta_3))}$

C3 $\dfrac{}{(\neg\delta_1 \to \neg\delta_2) \to (\delta_2 \to \delta_1)}$

C4 $\dfrac{\delta_1 \quad \delta_1 \to \delta_2}{\delta_2}$

N1 $\dfrac{}{\forall(\varphi_1 \wedge \varphi_2) \leftrightarrow (\forall\varphi_1 \wedge \forall\varphi_2)}$

N2 $\dfrac{}{\forall\neg\varphi \to \neg\forall\varphi}$

N3 $\dfrac{}{\neg\forall\varphi \to \forall\neg\varphi}$ if $names(\varphi) = \emptyset$

N4 $\dfrac{}{\forall(\varphi_1 \leftrightarrow \varphi_2) \to (\forall\varphi_1 \leftrightarrow \forall\varphi_2),}$

E(Γ) $\dfrac{}{\forall(\sigma(s_1) \approx \sigma(s'_1) \wedge \ldots \wedge \sigma(s_n) \approx \sigma(s'_n) \to \sigma(s) \approx \sigma(s'))}$ for $(s_1 \approx s'_1 \& \ldots \& s_n \approx s'_n \Rightarrow s \approx s') \in \Gamma$

$\mathcal{H}_\Gamma$ combines the different components inherent to this logic: axioms Eq1-Eq4 incorporate standard equational reasoning, namely reflexivity, symmetry, transitivity and congruence; C1-C4 and EqC1-EqC4 incorporate classical reasoning for the global and local layers (just note that locally, *modus ponens* becomes axiom EqC4); N1-N4 characterize the relationship between the local and global layers across the universal quantifier; and the axioms E(Γ) incorporate the equational theory underlying $\mathcal{A}$. We define, as usual, a deducibility relation $\vdash_\Gamma$. For instance, a normality-like axiom can be easily derived.

Lemma 1. *Given* $\varphi_1, \varphi_2 \in Loc$, $\vdash_\Gamma \forall(\varphi_1 \to \varphi_2) \to (\forall\varphi_1 \to \forall\varphi_2)$.

The logic is an extension of classical logic at both the local and the global layers. Namely, it is easy to see that the *deduction metatheorem* holds. Moreover, we can write any local or global formula in *disjunctive normal form (DNF)*.

Example 3. Recall Example 1. From the commutativity equation we obtain the axiom $\forall(s(n_1, n_2) \approx s(n_2, n_1))$, for $n_1, n_2 \in N$. By using also Eq3-4, EqC1-4, N1, and finally applying inference rule C4, we can easily show that $\forall(n \approx a \vee n \approx b), \forall(m \approx a \vee m \approx b), \forall(s(a, b) \approx c) \vdash_\Gamma \forall(n \not\approx m \to s(n, m) \approx c)$.

We define *consistency* as usual: $\Delta \subseteq Glob$ is *consistent* if there exists $\delta \in Glob$ such that $\Delta \nvdash_\Gamma \delta$. Since the logic is classically based, $\Delta \nvdash_\Gamma \delta$ if and only if $\Delta \cup \{\neg\delta\}$ is consistent. Furthermore, as a consequence of Lindenbaum's Lemma and given any set K, we have that $\{\bigvee_{i=1}^{n_k} \delta_{k,i} \mid k \in K\}$ is consistent if and only if, for every $k \in K$, there exists $1 \leq i_k \leq n_k$ such that $\{\delta_{k,i_k} \mid k \in K\}$ is consistent.

3.2 Soundness and completeness

We now prove that $\mathcal{H}_\Gamma$ is a sound and complete proof system for the logic based on the class $\mathcal{A}$ of all algebras that satisfy Γ.

Theorem 1. *The deductive system* $\mathcal{H}_\Gamma$ *is sound and complete.*

Proof. The proof of soundness is straightforward. We proceed with completeness. Let $\Delta \subseteq Glob$, $\delta \in Glob$ and assume $\Delta \nvdash_\Gamma \delta$. We need to prove that $\Delta \not\models_{\mathcal{A}} \delta$ by defining a F-structure $(\mathbb{A}, S)$ such that $\mathbb{A}$ satisfies Γ, $(\mathbb{A}, S) \Vdash \Delta$ and $(\mathbb{A}, S) \nVdash \delta$. We begin by writing each element of $\Delta \cup \{\neg\delta\}$ in DNF:

$$\left\{ \xi^{DNF} = \bigvee_{j=1}^{m_\xi} \bigwedge_{i=1}^{n_j} \psi_{\xi,j,i} \mid \xi \in \Delta \cup \{\neg\delta\} \right\}, \tag{1}$$

where $m_\xi, n_j \in \mathbb{N}$, and either $\psi_{\xi,j,i} \in \forall Loc$ or $\psi_{\xi,j,i} \in \neg\forall Loc$. Let

$$\left\{ \bigwedge_{i=1}^{n_{j_\xi}} \psi_{\xi,j_\xi,i} \mid \xi \in \Delta \cup \{\neg\delta\} \right\} \quad \text{be a consistent set} \tag{2}$$

constructed by one disjunct of each element in (1). We are looking for a F-structure satisfying each of the *relevant atoms*:

$$RelAt(\Delta \cup \{\neg\delta\}) = \bigcup_{\xi \in \Delta \cup \{\neg\delta\}} \left\{ \psi_{\xi,j_\xi,1}, \ldots, \psi_{\xi,j_\xi,n_{j_\xi}} \right\} \subseteq \forall Loc \cup \neg\forall Loc. \tag{3}$$

To define the F-structure $\mathbb{A}$ we follow a Henkin construction, adding enough constants to the language in order to introduce all the necessary witnesses for formulas of the form $\neg\forall\varphi$. Note that the set of local formulas is countable and thus

we introduce a set of new constants for each of them, that we will use to instantiate all names in N: $\bigcup_{\varphi \in Loc} \{c_{\varphi,n} \mid n \in N\}$. We denote the extended signature by F^+. We now extend the set (3) with such witnesses. Fix an enumeration for $Loc \times Loc$ and consider the following inductive definition:

$$W_0 = RelAt(\Delta \cup \{\neg\delta\}),$$
$$W_{i+1} = W_i \cup \left\{ \neg\forall\varphi_i^1 \to \left(\forall[\neg\varphi_i^1]^{\tilde{n}}_{\tilde{c}_{\varphi_i^1}} \wedge \left(\forall\varphi_i^2 \to \forall[\varphi_i^2]^{\tilde{n}}_{\tilde{c}_{\varphi_i^1}} \right) \right) \right\},$$

where $names(\varphi_i^1) \cup names(\varphi_i^2) = \tilde{n} = \{n_1, \ldots, n_m\}$, $\tilde{c}_\varphi = \{c_{\varphi,n_1}, \ldots, c_{\varphi,n_m}\}$. This way, given $i \in \mathbb{N}$ we introduce, where appropriate, a witness for $\neg\forall\varphi_i^1$.

Lemma 2. *$W = \bigcup_{i\in\mathbb{N}} W_i$ is consistent (regarding F^+).*

Let $\Xi \subseteq Glob^+$ (over F^+) be a maximal consistent set extending W, and consider the congruence relation $\equiv$ over $T_{F^+}(N)$ defined by $t_1 \equiv t_2$ if $\forall(t_1 \approx t_2) \in \Xi$. Axioms Eq1-4 together with Lemma 1, make $\equiv$ be a congruence relation. We define the F-algebra $\mathbb{A} = \langle A, -^A \rangle$ to be the reduct of the quotient F^+-algebra $\mathbb{T}_{F^+}(N)_{/\equiv}$. Note that by definition of $\equiv$, E(Γ), C4, Lemma 1, and recalling that Ξ is maximally consistent, it is easy to check that $\mathbb{A}$ satisfies Γ. For the construction of S we choose to define an outcome for each element of $\neg\forall Loc$ in Ξ. Given $\neg\forall\varphi \in \Xi$, let $\rho^{\neg\forall\varphi} : N \to A$ be the outcome defined by $\rho(n) = [c_{\varphi,n}]_\equiv$ for each $n \in N$. Finally, define $S = \left\{\rho^{\neg\forall\varphi} \mid \neg\forall\varphi \in \Xi\right\}$. Note that $S \neq \emptyset$ because, given $t \in T(N)$, axiom Eq1 implies that $\forall(\neg(t \not\approx t)) \in \Xi$, which together with axiom N2 means that $\neg\forall(t \not\approx t) \in \Xi$.

Lemma 3. *$(\mathbb{A}, S) \Vdash \gamma$, for each $\gamma \in RelAt(\Delta \cup \{\neg\delta\})$.*

As an immediate corollary we have that $(\mathbb{A}, S)$ satisfies the set defined in (2), and therefore $(\mathbb{A}, S) \Vdash \Delta \cup \{\neg\delta\}$. □

4 Decidability

In general, our logic cannot be expected to be decidable, as equational theories can easily be undecidable [3]. We will show, however, that our logic is decidable if we just require that the base equational theory is convergent. Our decidability result will be proved by reduction to the SAT problem for classical logic. Along the proof, we need to translate local formulas to the propositional context. Hence, let us consider a set of propositional variables corresponding to equations between nominal terms $Eq(N)^p = \{p_{t_1 \approx t_2} \mid t_1, t_2 \in T(N)\}$, and expand this notion to local formulas: given $\varphi \in Loc$ we define p_φ inductively by:

- if φ is of the form $t_1 \approx t_2$, p_φ is precisely $p_{t_1 \approx t_2}$,
- if φ is of the form $\neg\psi$ then p_φ is $\neg p_\psi$,
- if φ is of the form $\varphi_1 \wedge \varphi_2$ then p_φ is $p_{\varphi_1} \wedge p_{\varphi_2}$.

Given $\Psi \subseteq Loc$, we will use $\Psi^p = \{p_\varphi \mid \varphi \in \Psi\}$.

Theorem 2. *If Γ is a convergent equational theory then the logic is decidable.*

Proof. Let $\delta \in Glob$ be an arbitrary formula. We want to decide whether $\vdash_\Gamma \delta$ or $\nvdash_\Gamma \delta$. We will proceed by checking the satisfiability of $\neg\delta$. Let $RelTerm \subseteq T(N)$ be the set of relevant nominal terms for this proof. $RelTerm$ is such that $subterms(\delta) \subseteq RelTerm$ and $RelTerm$ is closed for rewriting under R, the convergent rewriting system for Γ, that is: if $t \to_R t'$ and $t \in RelTerm$ then $t' \in RelTerm$. Note that $t{\downarrow} \in RelTerm$ whenever $t \in RelTerm$. The propositional variables of interest are those that represent equations between terms in $RelTerm$, and are gathered in the set $\mathcal{B} = \{p_{t_1 \approx t_2} \mid t_1, t_2 \in RelTerm\}$. Equational statements obey some relations that should be imposed to their propositional representatives. These restrictions are established in Φ, defined as follows:

$$\begin{aligned}\Phi = {} & \{p_{t\approx t} \mid t \in RelTerm\} \cup \{p_{t_1\approx t_2} \to p_{t_2\approx t_1} \mid t_1, t_2 \in RelTerm\} \cup \\ & \{p_{t_1\approx t_2} \wedge p_{t_2\approx t_3} \to p_{t_1\approx t_3} \mid t_1, t_2, t_3 \in RelTerm\} \cup \\ & \{p_{t_1\approx t_1'} \wedge \ldots \wedge p_{t_n\approx t_n'} \to p_{f(t_1,\ldots,t_n)\approx f(t_1',\ldots,t_n')} \mid t_1, t_1', \ldots, t_n, t_n', t, t' \in RelTerm\} \cup \\ & \{p_{\sigma(s)\approx\sigma(s')} \mid \sigma \in T(N)^X, s \to s' \in R, \sigma(s), \sigma(s') \in RelTerm\}.\end{aligned}$$

Given $t \in RelTerm$ it is straightforward to check that $p_{t\approx t{\downarrow}}$ is a propositional consequence of Φ. We should also emphasize that, since $subterms(\delta)$ is a finite set and the equational theory is convergent, $RelTerm$ is a finite set. Denoting $|RelTerm| = k$, Φ has at most $k + k^2 + k^3 + k^{2a+2} + k^2$ elements, where a is the maximum arity of the function symbols occurring in $RelTerm$.

To describe a procedure that verifies the satisfiability of $\neg\delta$, let $(\neg\delta)^{DNF} = \bigvee_{j=1}^{m} \bigwedge_{i=1}^{n_j} \delta_i^j$. The procedure will verify the satisfiability of each disjunct. Note that the j^{th} disjunct $\delta_1^j \wedge \ldots \wedge \delta_{n_j}^j$, is a conjunction of global formulas of the form $\forall\varphi$ or $\neg\forall\varphi$. Specifying explicitly those components, let the j^{th} disjunct be:

$$\neg\forall\varphi_1^j \wedge \ldots \wedge \neg\forall\varphi_{k_j}^j \wedge \forall\varphi_{k_j+1}^j \wedge \ldots \wedge \forall\varphi_{n_j}^j.$$

Satisfiability
Let $j := 1$.

1. Fix $l := 1$.
2. Let $\Delta_l^j := \Phi \cup \left\{\varphi_{k_j+1}^j, \ldots, \varphi_{n_j}^j\right\}^p \cup \left\{\neg p_{\varphi_l^j}\right\}$.
3. Apply SAT to Δ_l^j.
   3.1. if SAT answers **YES** , let $l := l + 1$
      3.1.1. if $l \leq k_j$ proceed to 2.
      3.1.2. if $l > k_j$ then $\Delta_1^j, \ldots, \Delta_{k_j}^l$ have models given, respectively, by $(\{0,1\}, v_1), \ldots, (\{0,1\}, v_{k_j})$. The output is **YES**, $(\neg\delta)^{DNF}$ is satisfiable.
   3.2. If SAT answers **NO**, let $j := j + 1$,
      3.2.1. if $j \leq m$ proceed to 1.
      3.2.2. if $j > m$ then output **NO**, $(\neg\delta)^{DNF}$ is not satisfiable.

The procedure tries to satisfy each disjunct of $(\neg\delta)^{DNF}$. Each disjunct is written as a conjunction of elements from $\forall Loc \cup \neg\forall Loc$. Satisfying an element of the form $\forall\varphi$ imposes that φ must be verified in all possible outcome, whereas satisfying a formula as $\neg\forall\varphi$ requires that at least one possible outcome satisfies $\neg\varphi$. The satisfiability of such conjuncts is tested in several iterations (one for

each conjunct of the form $\neg\forall Loc$). When all iterations are successful, we conclude that $(\neg\delta)^{DNF}$ is satisfiable.

Lemma 4. *Given $\delta \in Glob$, $(\neg\delta)^{DNF}$ is satisfiable if and only if there exists $j \in \{1,\ldots,m\}$ such that each of $\Delta^j_1,\ldots,\Delta^j_{k_j}$ is satisfiable, where $\Delta^j_1,\ldots,\Delta^j_{k_j}$ are defined in the satisfiability procedure.*

Proving the Lemma requires showing that satisfiability at the propositional level carries over to our logic. Details can be found in the Appendix. □

Example 4. To analyze *offline guessing* [4], one assumes that an attacker has observed messages named $m_1,\ldots,m_k$ (terms in some algebra). Typically, the attacker may know exactly that the messages were built as $t_1,\ldots,t_k \in T(N)$, but he just cannot know the concrete values of the random and secret names used to build them. Still, he can try to mount an attack by guessing some weak secret $s \in N$ used by the parties executing the protocol. The attack is successful if the attacker can distinguish whether his guess is correct or not. In our logic, if Γ is the equational specification of the underlying algebraic base, we can express this by requiring that the attacker finds two terms (also called *recipes*) $t, t' \in T(\{m_1,\ldots,m_k,g\})$ such that

$$\forall(m_1 \approx t_1 \wedge \cdots \wedge m_k \approx t_k) \not\vdash_\Gamma \forall(t \approx t') \text{ but}$$
$$\forall(m_1 \approx t_1 \wedge \cdots \wedge m_k \approx t_k) \vdash_\Gamma \forall(g \approx s \to t \approx t').$$

Of course, this task is undecidable in general, as the two recipes may be arbitrarily complex. Still, for the Dolev-Yao theory of Example 2, $Th(\Gamma)$ is generated by the convergent rewriting system obtained by orienting the given equations from left to right. The resulting system is even further said to be *subterm convergent*, as each rule rewrites a term to a strict subterm. Under such particular conditions, it is known that the problem is decidable, as only a finite number of 'dangerous' recipes need to be tested [4, 2, 1].

Consider the following protocol adapted from [7], where $a, b, n_a, p_{ab} \in N$.

1. $a \to b : (a, n_a)$
2. $b \to a : \{n_a\}_{p_{ab}}$

In the first step, some party named a sends a message to another party named b in order to initiate some communication session. The message is a pair containing a's name and a random value (*nonce*) named n_a, that a generated freshly, and which is intended to distinguish this request from other, similar, past or future, requests. Upon reception of the first message, b responds by cyphering n_a with a secret password p_{ab} shared with a. When receiving the second message, a can decrypt it and recognize b's response to his request to initiate a session.

It is relatively simple, in this case, to see that the secret shared password p_{ab} is vulnerable to an offline guessing attack. Suppose that the attacker observes the execution of the protocol by parties a and b, and got hold of the two exchanged messages m_1 and m_2. He can now manipulate these messages, using his guess g of p_{ab}, and come up with recipes $\{m_2\}_g^{-1}$ and $\pi_2(m_1)$. Indeed, only under the correct guess, should the decryption of m_2 with g coincide with the second projection of m_1, that is, n_a. We can use our logic to check that, indeed,

$$\forall(m_1 \approx (a, n_a) \wedge m_2 \approx \{n_a\}_{p_{ab}}) \not\vdash_\Gamma \forall(\{m_2\}_g^{-1} \approx \pi_2(m_1)) \text{ and}$$
$$\forall(m_1 \approx (a, n_a) \wedge m_2 \approx \{n_a\}_{p_{ab}}) \vdash_\Gamma \forall(g \approx p_{ab} \to \{m_2\}_g^{-1} \approx \pi_2(m_1)),$$

namely using the three $\mathrm{E}(\Gamma)$ axioms that encode the equations in Γ.

5 Conclusion and future work

We combined aspects from classical, equational and quantifier logics to construct a logic suited for reasoning about equational constraints over sets of outcomes. The design of the logic was aimed at formalizing the kind of reasoning carried out in security protocol analysis. Parameterized by suitable properties of the underlying algebraic base, we have also obtained a sound and complete deductive system for our logic, as well as satisfiability and decidability results. It goes without saying that these results can be used to decide the existence of offline guessing attacks whenever the underlying equational theories are subterm convergent, by capitalizing on the results in [4, 2, 1], but that being so generic this approach will never be able to compete with extremely efficient dedicated tools such as [5].

We are working on extending the logic with explicit probabilities and domains, in the lines of [9, 11], in a way that may enable us to provide a suitable formalization of the reasoning underlying [6], which extends the analysis of protocols well beyond equational reasoning, by allowing the attacker to do a fair amount of cryptanalysis, exploring known details of the implementation of the cryptographic primitives, and ultimately estimate the probability of success of the adopted attack strategy. We expect to be able to provide a deductive system for the extended logic, as well as, when applicable, decidability and satisfiability results. In particular, we expect to be able to take advantage of a suitable reduction to probabilistic satisfiability (PSAT) [10, 13], an interesting probabilistic generalization of the classical SAT problem.

References

1. M. Abadi and V. Cortier. Deciding knowledge in security protocols under (many more) equational theories. In *Proc. 18th IEEE Computer Security Foundations Workshop (CSFW'05)*, pages 62–76. IEEE Comp. Soc. Press, 2005.
2. M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 387(1-2):2–32, 2006.
3. F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.
4. M. Baudet. Deciding security of protocols against off-line guessing attacks. In *Proceedings of the 12th ACM Conf. on Computer and Communications Security*, CCS '05, pages 16–25, New York, NY, USA, 2005. ACM.
5. B. Conchinha, D. A. Basin, and C. Caleiro. Efficient decision procedures for message deducibility and static equivalence. In P. Degano, S. Etalle, and J. D. Guttman, editors, *Formal Aspects of Security and Trust - 7th International Workshop, FAST 2010, Pisa, Italy, September 16-17, 2010. Revised Selected Papers*, volume 6561 of *Lecture Notes in Computer Science*, pages 34–49. Springer, 2010.
6. B. Conchinha, D. A. Basin, and C. Caleiro. Symbolic probabilistic analysis of off-line guessing. In J. Crampton, S. Jajodia, and K. Mayes, editors, *ESORICS*, volume 8134 of *Lecture Notes in Computer Science*, pages 363–380. Springer, 2013.
7. R. Corin and S. Etalle. A simple procedure for finding guessing attacks (extended abstract), 2004.
8. V. Cortier, S. Kremer, and B. Warinschi. A survey of symbolic methods in computational analysis of cryptographic systems. *Journal of Automated Reasoning*, 46(3-4):225–259, 2010.
9. R. Fagin, J. Y. Halpern, and N. Megiddo. A logic for reasoning about probabilities. *Inf. Comput.*, 87(1-2):78–128, 1990.
10. M. Finger and G.D. Bona. Probabilistic satisfiability: Logic-based algorithms and phase transition. In T. Walsh, editor, *IJCAI*, pages 528–533. IJCAI/AAAI, 2011.
11. P. Mateus, A. Sernadas, and C. Sernadas. Exogenous semantics approach to enriching logics. In *Essays on the Found. of Mathematics and Logic, volume 1 of Advanced Studies in Mathematics and Logic*, pages 165–194. Polimetrica, 2005.
12. R. Nieuwenhuis, A. Oliveras, and C. Tinelli. Solving SAT and SAT modulo theories: From an abstract Davis–Putnam–Logemann–Loveland procedure to DPLL(T). *J. ACM*, 53(6):937–977, 2006.
13. N. J. Nilsson. Probabilistic logic. *Artif. Intell.*, 28(1):71–88, February 1986.

6 Appendix

Proof (Lemma 1). To deduce $\forall(\varphi_1 \to \varphi_2) \to (\forall\varphi_1 \to \forall\varphi_2)$ we assume $\forall(\varphi_1 \to \varphi_2)$ and prove that $\forall\varphi_1 \to \forall\varphi_2$. Applying MTD we will be done.

1. $\forall(\varphi_1 \to \varphi_2)$	(hypothesis)
2. $\forall\left((\varphi_1 \to \varphi_2) \leftrightarrow \neg(\varphi_1 \wedge \neg\varphi_2)\right) \to (\forall(\varphi_1 \to \varphi_2) \leftrightarrow \forall\neg(\varphi_1 \wedge \neg\varphi_2))$	(instance of $N4$)
3. $\forall\left((\varphi_1 \to \varphi_2) \leftrightarrow \neg(\varphi_1 \wedge \neg\varphi_2)\right)$	(tautology)
4. $\forall(\varphi_1 \to \varphi_2) \leftrightarrow \forall\neg(\varphi_1 \wedge \neg\varphi_2)$	(apply $C4$ to 2. and 3.)
5. $\forall\neg(\varphi_1 \wedge \neg\varphi_2)$	(apply $C4$ to 1. and 4.)
6. $\forall\varphi_1$	(hypothesis)
7. $\forall\neg(\varphi_1 \wedge \neg\varphi_2) \to (\forall\varphi_1 \to (\forall\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \forall\varphi_1))$	(tautology)
8. $\forall\varphi_1 \to (\forall\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \forall\varphi_1)$	(apply $C4$ to 5. and 7.)
9. $\forall\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \forall\varphi_1$	(apply $C4$ to 6. and 8.)

10. $\forall\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \forall\varphi_1 \leftrightarrow \forall\,(\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \varphi_1)$ (instance of $N1$)
11. $\forall\,(\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \varphi_1)$ (apply $C4$ to 9. and 10.)
12. $\forall\,(\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \varphi_1 \leftrightarrow \varphi_2 \wedge \varphi_1)$ (tautology)
13. $\forall\,(\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \varphi_1 \leftrightarrow \varphi_2 \wedge \varphi_1) \rightarrow (\forall(\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \varphi_1) \leftrightarrow \forall(\varphi_2 \wedge \varphi_1))$ ($N4$)
14. $\forall\,(\neg(\varphi_1 \wedge \neg\varphi_2) \wedge \varphi_1) \leftrightarrow \forall(\varphi_2 \wedge \varphi_1)$ (apply $C4$ to 12. and 13.)
15. $\forall(\varphi_2 \wedge \varphi_1)$ (apply $C4$ to 11. and 14.)
16. $\forall(\varphi_2 \wedge \varphi_1) \leftrightarrow \forall\varphi_2 \wedge \forall\varphi_1$ (instance of $N1$)
17. $\forall\varphi_2 \wedge \forall\varphi_1$ (apply $C4$ to 15. and 16.)
18. $\forall\varphi_2 \wedge \forall\varphi_1 \rightarrow \forall\varphi_2$ (tautology)
19. $\forall\varphi_2$ (apply $C4$ to 17. and 18.) □

In order to prepare the proof of Lemma 3 we present an auxiliary result whose proof we omit but follows easily by induction on the complexity of φ.

Lemma 5. *Given $\neg\forall\varphi_0 \in \Xi$ and a local formula $\varphi \in Loc$ with $names(\varphi) = \tilde{n}$, $\forall[\varphi]^{\tilde{n}}_{\tilde{c}_{\varphi_0}} \in \Xi$ if and only if $\mathbb{A}, \rho^{\neg\forall\varphi_0} \Vdash_{loc} [\varphi]^{\tilde{n}}_{\tilde{c}_{\varphi_0}}$.*

Proof (Lemma 3). Recall that $RelAt(\Delta \cup \{\neg\delta\}) \subseteq \forall Loc \cup \neg\forall Loc$ and let $\gamma \in RelAt(\Delta \cup \{\neg\delta\})$. We split the proof in two cases:

- if γ is of the form $\forall\varphi$ with $names(\varphi) = \tilde{n}$, we need to prove that for any $\rho \in S$ $\mathbb{A}, \rho \Vdash_{loc} \varphi$. Let $\rho \in S$ and recall that ρ was motivated by some $\neg\forall\varphi_0 \in \Xi$, say that $\rho = \rho^{\neg\forall\varphi_0}$. Since $\forall\varphi \in RelAt(\Delta \cup \{\neg\delta\}) \subseteq \Xi$ it follows that $\forall[\varphi]^{\tilde{n}}_{\tilde{c}_{\varphi_0}} \in \Xi$ by construction of W. Using Lemma 5 we conclude that $\mathbb{A}, \rho^{\neg\forall\varphi_0} \Vdash_{loc} \forall[\varphi]^{\tilde{n}}_{\tilde{c}_{\varphi_0}}$, which according to definition of $\rho^{\neg\forall\varphi_0}$ implies $\mathbb{A}, \rho^{\neg\forall\varphi_0} \Vdash_{loc} \varphi$.
- on the other hand, if γ is of the form $\neg\forall\varphi$ with $names(\neg\varphi) = names(\varphi) = \tilde{n}$, consider the already defined outcome $\rho^{\neg\forall\varphi} \in S$. Notice that since $\neg\forall\varphi \in \Xi$ it follows that $\forall[\neg\varphi]^{\tilde{n}}_{\tilde{c}_\varphi} \in \Xi$. Lemma 5 implies $\mathbb{A}, \rho^{\neg\forall\varphi} \Vdash_{loc} [\neg\varphi]^{\tilde{n}}_{\tilde{c}_\varphi}$, which by definition of $\rho^{\neg\forall\varphi}$ implies $\mathbb{A}, \rho^{\neg\forall\varphi} \Vdash_{loc} \neg\varphi$. Therefore $\mathbb{A}, S \Vdash \neg\forall\varphi$. □

To prove soundness and completeness of the procedure of **Satisfiability** presented in proof of Theorem 2 (Lemma 4) we define a translation of outcomes with values in a F-algebra $\langle A, -^{\mathbb{A}}\rangle$ to valuations in the propositional context, and vice-versa. For the first kind of translation, denote by $v_{(\cdot)}$ the transformation of outcomes into valuations, $v_{(\cdot)} : A^N \rightarrow \{0,1\}^{\mathcal{B}}$: given $\rho \in A^N$, let $v_\rho : \mathcal{B} \rightarrow \{0,1\}$ be defined by

$$v_\rho(p_{t_1 \approx t_2}) = 1 \text{ iff } [\![t_1]\!]^\rho_{\mathbb{A}} = [\![t_2]\!]^\rho_{\mathbb{A}}. \tag{4}$$

This translation is sound and complete, the following Lemma is easily proved by induction on φ.

Lemma 6. *For any $\varphi \in subform((\neg\delta)^{DNF}) \cap Loc$ and $\rho \in A^N$, $\mathbb{A}, \rho \Vdash_{loc} \varphi$ iff $\{0,1\}, v_\rho \Vdash p_\varphi$.*

For the second kind of translation, we denote by $[\cdot]$ the transformation of valuations into outcomes $[\cdot] : \{0,1\}^{\mathcal{B}} \rightarrow 2^{(A^N)}$ such that, given $v \in \{0,1\}^{\mathcal{B}}$

$$[v] = \left\{\rho \in A^N \mid v_\rho \cong v\right\} \tag{5}$$

where v_ρ was defined in (4) and $\cong$ represents equality of functions. To prove that this translation is sound and complete we need an auxiliary result,

Lemma 7. *For any $t_1, t_2 \in subterms(\delta)$, $v \in \{0,1\}^{\mathcal{B}}$ and assuming $[v] \neq \emptyset$, $\{0,1\}, v \Vdash p_{t_1 \approx t_2}$ if and only if for every $\rho \in [v], \mathbb{A}, \rho \Vdash_{loc} t_1 \approx t_2$.*

Proof. Let $t_1, t_2 \in subterms(\delta)$, $v \in \{0,1\}^{\mathcal{B}}$ and assume $\{0,1\}, v \Vdash p_{t_1 \approx t_2}$. Note that for any $\rho \in [v]$ $v_\rho \cong v$. Since $\{0,1\}, v \Vdash p_{t_1 \approx t_2}$ we also have $\{0,1\}, v_\rho \Vdash p_{t_1 \approx t_2}$, which by definition of $v_{(.)}$ is equivalent to $[\![t_1]\!]^\rho_{\mathbb{A}} = [\![t_2]\!]^\rho_{\mathbb{A}}$ or: $\mathbb{A}, \rho \Vdash t_1 \approx t_2$. Reciprocally, assume that for every $\rho \in [v]$ $\mathbb{A}, \rho \Vdash t_1 \approx t_2$, i.e., $\{0,1\}, v_\rho \Vdash p_{t_1 \approx t_2}$. This implies $\{0,1\}, v \Vdash p_{t_1 \approx t_2}$. □

Lemma 8. *For any $\varphi \in subform((\neg\delta)^{DNF}) \cap Loc$, $v \in \{0,1\}^{\mathcal{B}}$ and assuming $[v] \neq \emptyset$, $\{0,1\}, v \Vdash p_\varphi$ if and only if for any $\rho \in [v]$ $\mathbb{A}, \rho \Vdash_{loc} \varphi$.*

Proof. This proof uses the previous result and explores the construction of φ:

- if φ is of the form $t_1 \approx t_2$ the result follows from the previous lemma,
- if φ is of the form $\neg\varphi'$ for some $\varphi' \in Loc$, then $\varphi' \in subform((\neg\delta)^{DNF})$ and
  $\{0,1\}, v \Vdash p_{\neg\varphi'}$ iff $\{0,1\}, v \Vdash \neg p_{\varphi'}$ iff $\{0,1\}, v \nVdash p_{\varphi'}$
  iff for any $\rho \in [v]$ $\{0,1\}, v_\rho \nVdash p_{\varphi'}$ iff for any $\rho \in [v]$ $\mathbb{A}, \rho \nVdash \varphi'$
  iff for any $\rho \in [v]$ $\mathbb{A}, \rho \Vdash \neg\varphi'$
- if φ is of the form $\varphi_1 \wedge \varphi_2$ for some $\varphi_1 \wedge \varphi_2 \in Loc$, then φ_1, $\varphi_2 \in subform((\neg\delta)^{DNF})$ and we have the following equivalences
  $\{0,1\}, v \Vdash p_{\varphi_1 \wedge \varphi_2}$ iff $\{0,1\}, v \Vdash p_{\varphi_1} \wedge p_{\varphi_2}$
  iff $\{0,1\}, v \Vdash p_{\varphi_1}$ and $\{0,1\}, v \Vdash p_{\varphi_2}$
  iff for any $\rho \in [v]$ $\{0,1\}, v_\rho \Vdash p_{\varphi_1}$ and $\{0,1\}, v_\rho \Vdash p_{\varphi_2}$
  iff for any $\rho \in [v]$ $\mathbb{A}, \rho \Vdash \varphi_1$ and $\mathbb{A}, \rho \Vdash \varphi_2$
  iff for any $\rho \in [v]$ $\mathbb{A}, \rho \Vdash \varphi_1 \wedge \varphi_2$. □

Proof (Lemma 4). Let $\delta \in Glob$ be any global formula. For the direct implication, let $(\mathbb{A}, S)$ be a model for $(\neg\delta)^{DNF}$: $\mathbb{A}, S \Vdash \bigvee_{j=1}^{m} \bigwedge_{i=1}^{n_j} \delta_i^j$. Exists $1 \leq j \leq m$ such that $\mathbb{A}, S \Vdash \bigwedge_{i=1}^{n_j} \delta_i^j$. Since each δ_i^j is either of the form $\forall\varphi$ or $\neg\forall\varphi$ we can rewrite it as

$$\mathbb{A}, S \Vdash \neg\forall\varphi_1^j \wedge \ldots \wedge \neg\forall\varphi_{k_j}^j \wedge \forall\varphi_{k_j+1}^j \wedge \ldots \wedge \forall\varphi_{n_j}^j.$$

Notice that, for any $l \in \{1, \ldots, k_j\}$ and $s \in \{k_j + 1, \ldots, n_j\}$

$$\begin{array}{ll} \mathbb{A}, S \Vdash \neg\forall\varphi_l & \text{i.e. exists } \rho \in S \text{ such that } \mathbb{A}, \rho \Vdash_{loc} \neg\varphi_l. \\ \mathbb{A}, S \Vdash \forall\varphi_s & \text{i.e. for every } \rho \in S\ \mathbb{A}, \rho \Vdash_{loc} \varphi_s \end{array} \tag{6}$$

For each $\neg\forall\varphi_l^j \in \{\neg\forall\varphi_1^j, \ldots, \neg\forall\varphi_{k_j}^j\}$, let $\rho^{\varphi_l^j}$ be the outcome whose existence is ensured by (6). The valuation $v_{\rho^{\varphi_l^j}}$ is the valuation we are looking for. Recalling that for each $1 \leq l \leq k_j$, $\Delta_l^j = \Phi \cup \left\{\varphi_{k_j+1}^j, \ldots, \varphi_{n_j}^j\right\}^p \cup \{\neg p_{\varphi_l^j}\}$, from Lemma 6, (6) and since $(\mathbb{A}, S)$ satisfies each instance of $Eq1{-}4, E$ we have $\{0,1\}, v_{\rho^{\varphi_l^j}} \Vdash \Delta_l^j$.

Reciprocally, let $j \in \{1, \ldots, m\}$ be in the conditions written in the statement. For each $l \in \{1, \ldots, k_j\}$, let $\{0,1\}, v_l \Vdash \Delta_l^j$. $\{v_1, \ldots, v_{k_j}\}$ are the relevant valuations for the remaining construction.

Notice that, if we define a model $(\mathbb{A}, S)$ for the j^{th} disjunct $\mathbb{A}, S \Vdash \bigwedge_{i=1}^{n_j} \delta_i^j$, it will be a model for $(\neg\delta)^{DNF}$ as well. Let us define such F-structure. Begin defining the free algebra $\mathbb{A} = \langle A, -^{\mathbb{A}} \rangle$ where $A = T(N)_{/\equiv}$ and $\equiv$ is the congruence relation on $T(N)$ generated by the following rule: given $s \approx s' \in \Gamma$ and $\sigma \in T(N)^X$, $\sigma(s) \equiv \sigma(s')$. From a simple observation we find that, given $s \in T(X)$ and $\sigma \in T(N)^X$, $\sigma(s) \equiv \sigma(s\downarrow)$. Besides the definition of $\mathbb{A}$, we need to define S. Let $S = \bigcup_{l=1}^{k_j} [v_l]$. Before proving that $(\mathbb{A}, S)$ is actually a F-structure, let us refer to an important Lemma that reports to definition (5).

Lemma 9. *Let $v \in \{0,1\}^{\mathcal{B}}$ be any valuation. If $\{0,1\}, v \Vdash \Phi$ then $[v] = \{\rho \in A^N \mid v_\rho \cong v\} \neq \emptyset$, where A was already defined by $A = T(N)_{/\equiv}$.*

Proof. Let us begin defining $\equiv_v \subseteq A \times A$ the congruence generated by the rule:

$$\text{For any } t_1, t_2 \in RelTerm, [t_1]_\equiv \equiv_v [t_2]_\equiv \text{ iff } \{0,1\}, v \Vdash p_{t_1 \approx t_2}.$$

$\equiv_v$ **is well-defined:** Given $t_1', t_2' \in T(N)$ such that

$$t_1' \in [t_1]_\equiv, \quad t_2' \in [t_2]_\equiv, \tag{7}$$

we pretend to prove that $\{0,1\}, v \Vdash p_{t_1' \approx t_2'}$. Moreover, we know that

$$\{0,1\}, v \Vdash p_{t_1 \approx t_2}. \tag{8}$$

By (7), exist $\overline{t_1}, \ldots, \overline{t_k} \in T(N)$ such that $\overline{t_1} = t_1$, $\overline{t_k} = t_1'$ and for each $1 \leq i \leq k$ exists $\sigma_i \in T(N)^X$, $s_i, s_{i+1} \in T(X)$ with $\overline{t_i} = \sigma_i(s_i)$, $\overline{t_{i+1}} = \sigma_i(s_{i+1})$ and either $s_1 \approx s_{i+1} \in \Gamma$ or $s_{i+1} \approx s_i \in \Gamma$, i.e. $\sigma(s_i) \equiv \sigma(s_{i+1})$ or yet $\overline{t_i} \approx \overline{t_{i+1}}$.

Let us prove, by induction on k that $p_{t_1 \approx t_1'}$:

- if $k = 1$, $t_1 = \overline{t_1} = t_1'$ so that $t_1' \in RelTerm$ and by reflexivity $p_{t_1 \approx t_1'} \in \Phi$,
- if $k = 2$, $t_1 = \overline{t_1} = \sigma_1(s_1) \equiv \sigma_1(s_2) = \overline{t_2} = t_1'$, so that t_1' is obtained by reduction of Γ from t_1 and $t_1' \in RelTerm$. Moreover $p_{\sigma_1(s_1) \approx \sigma_1(s_2)} \in \Phi$, i.e., $p_{t_1 \approx t_1'}$.
- Assume the assertion for $k \in \mathbb{N}$ and let us prove by induction for $k+1$: let $\overline{t_1}, \ldots, \overline{t_k}, \overline{t_{k+1}} \in T(N)$ be such that $\overline{t_1} = t_1$, $\overline{t_{k+1}} = t_1'$ and for each $i \in \{1, \ldots, k+1\}$ exists $\sigma_i \in T(N)^X$, $s_i, s_{i+1} \in T(X)$ with $\overline{t_i} = \sigma_i(s_i)$, $\overline{t_{i+1}} = \sigma_i(s_{i+1})$ and $\sigma(s_i) \equiv \sigma(s_{i+1})$ i.e. $\overline{t_1} \equiv \overline{t_{i+1}}$. By induction hypothesis $p_{t_1 \approx \overline{t_k}} \in \Phi$ and $\overline{t_k} \in RelTerm$. Moreover, do not forget that $\overline{t_k} = \sigma_k(s_k) \equiv \sigma_k(s_{k+1}) = \overline{t_{k+1}} = t_1'$ i.e. $p_{\overline{t_k} \approx t_1'} \in \Phi$ and t_1' is obtained by reduction of Γ from $\overline{t_k}$, which itself belongs to $RelTerm$, so $t_1' \in RelTerm$. By transitivity we have $p_{t_1 \approx t_1'} \in \Phi$.

A similar reasoning can be done to conclude that $\{0,1\}, v \Vdash p_{t_1' \approx t_2'}$.

Let $[[t]_{\equiv}]^*_{\equiv_v}$ be a representative for the equivalence class $[[t]_{\equiv}]_{\equiv_v}$ and consider the outcome

$$\begin{aligned} \rho^v : N &\to A \\ n &\mapsto [[n]_{\equiv}]^*_{\equiv_v} \end{aligned}$$

Let us check that $\rho^v \in [v]$, i.e., that $v_{\rho^v} = v$: given $\varphi \in Loc$, we prove by induction on φ that $\{0,1\}, v_{\rho^v} \Vdash p_\varphi$ if and only if $\{0,1\}, v \Vdash p_\varphi$.

- if φ is of the form $t_1 \approx t_2$,

$$\begin{array}{lll} \{0,1\}, v_{\rho^v} \Vdash p_{t_1 \approx t_2} & \text{iff } [\![t_1]\!]^{\rho^v}_{\mathbb{A}} = [\![t_2]\!]^{\rho^v}_{\mathbb{A}} & \text{(by definition of } v_{(\cdot)}) \\ & \text{iff } [[t_1]_{\equiv}]^*_{\equiv_v} = [[t_2]_{\equiv}]^*_{\equiv_v} & \text{(by definition of } \rho^v) \\ & \text{iff } [t_1]_{\equiv} \equiv_v [t_2]_{\equiv} & (***) \\ & \text{iff } \{0,1\}, v \Vdash p_{t_1 \approx t_2} & \text{(by definition of } \equiv_v). \end{array}$$

  (***) the reciprocal implication is immediate, for the direct one assume the equivalence classes $[t_1]_{\equiv}$ and $[t_2]_{\equiv}$ are not the same, $[t_1]_{\equiv} \not\equiv_v [t_2]_{\equiv}$. This means that $[[t_1]_{\equiv}]_{\equiv_v} \cap [[t_2]_{\equiv}]_{\equiv_v} = \emptyset$, then they would not have the same representative.

- if φ is of the form $\neg\varphi'$,

$$\begin{array}{l} \{0,1\}, v_{\rho^v} \Vdash p_{\neg\varphi'} \text{ iff } \{0,1\}, v_{\rho^v} \Vdash \neg p_{\varphi'} \text{ iff } \{0,1\}, v_{\rho^v} \nVdash p_{\varphi'} \\ \text{iff } \{0,1\}, v \nVdash p_{\varphi'} \quad \text{iff } \{0,1\}, v \Vdash \neg p_{\varphi'} \quad \text{iff } \{0,1\}, v \Vdash p_{\neg\varphi'} \end{array}$$

- if φ is of the form $\varphi_1 \wedge \varphi_2$,

$$\begin{array}{ll} \{0,1\}, v_{\rho^v} \Vdash p_{\varphi_1 \wedge \varphi_2} & \text{iff } \{0,1\}, v_{\rho^v} \Vdash \neg p_{\varphi_1} \wedge p_{\varphi_2} \\ & \text{iff } \{0,1\}, v_{\rho^v} \Vdash p_{\varphi_1} \text{ and } \{0,1\}, v_{\rho^v} \Vdash p_{\varphi_2} \\ & \text{iff } \{0,1\}, v \Vdash p_{\varphi_1} \text{ and } \{0,1\}, v \Vdash p_{\varphi_2} \\ & \text{iff } \{0,1\}, v \Vdash p_{\varphi_1} \wedge p_{\varphi_2} \\ & \text{iff } \{0,1\}, v \Vdash p_{\varphi_1 \wedge \varphi_2} \end{array}$$

□

It remains to prove that $(\mathbb{A}, S)$ is a F-structure. For that we should notice that $\mathbb{A}$ satisfies Γ immediately by definition of $\equiv$ and conclude that $\emptyset \neq S \subseteq A^N$ as a corollary of Lemma 9.

To prove that $\mathbb{A}, S \Vdash \bigwedge_{i=1}^{n_j} \delta^j_i$, i.e., $\mathbb{A}, S \Vdash \neg\forall\varphi^j_1 \wedge \ldots \wedge \neg\forall\varphi^j_{k_j} \wedge \forall\varphi^j_{k_j+1} \wedge \ldots \wedge \forall\varphi^j_{n_j}$, notice that for each $\varphi \in \{\varphi^j_{k_j+1}, \ldots, \varphi^j_{n_j}\}$

$$\{0,1\}, v_l \Vdash p_\varphi \text{ for any } l \in \{1, \ldots n_j\}.$$

So that, by Lemma 8, for any $\rho \in S$, $\mathbb{A}, \rho \Vdash_{loc} \varphi$, and it follows that $\mathbb{A}, S \Vdash \forall\varphi$. Whereas, for each $\neg\forall\varphi \in \{\neg\forall\varphi^j_1, \ldots, \neg\forall\varphi^j_{k_j}\}$, exists $l \in \{1, \ldots, k_j\}$ such that $\{0,1\}, v_l \nVdash \neg p_\varphi$. Then, by Lemma 8, for any $\rho \in [v_l]$, $\mathbb{A}, \rho \Vdash_{loc} \neg\varphi$ and it follows that $\mathbb{A}, S \Vdash \neg\forall\varphi$, as we wanted. □