REPORTS ON MATHEMATICAL LOGIC
47 (2012), 3–28
DOI:10.4467/20842589RM.12.001.0682

George VOUTSADAKIS

SECRECY LOGIC: PROTOALGEBRAIC $\mathcal{S}$-SECRECY LOGICS

Abstract. In recent work the notion of a secrecy logic $\mathfrak{S}$ over a given deductive system $\mathcal{S}$ was introduced. Secrecy logics capture the essential features of structures that are used in performing secrecy-preserving reasoning in practical applications. More precisely, they model knowledge bases that consist of information, part of which is considered known to the user and part of which is to remain secret from the user. $\mathcal{S}$-secrecy structures serve as the models of secrecy logics. Several of the universal algebraic and model theoretic properties of the class of $\mathcal{S}$-secrecy structures of a given $\mathcal{S}$-secrecy logic have already been studied. In this paper, our goal is to show how techniques from the theory of abstract algebraic logic may be used to analyze the structure of a secrecy logic and draw conclusions about its algebraic character. In particular, the notion of a protoalgebraic $\mathcal{S}$-secrecy logic is introduced and several characterizing properties are provided. The relationship between protoalgebraic $\mathcal{S}$-secrecy logics and the protoalgebraicity of their underlying deductive systems is also investigated.

Received 2 May 2009

1. Introduction

In several older and recent works on the security of deductive databases and knowledge bases, secrecy-preserving reasoning is at the forefront of investigations. For instance, Sicherman, de Jonge and van de Riet [16] employ logical censors to either allow or refuse answering a query posed against a complete database with the goal of answering honestly as many queries as possible while at the same time protecting secrets. Bonatti, Kraus and Subrahmanian [9] introduce databases that consist of two parts: in the first part, one finds stored all the object information about the "outside world" whereas, in the second, a multi-modal logic is used to express assumptions about the user's beliefs concerning the world. Modalities are also used to express and reason about secrets that the database is assumed to conceal from the users. The framework is able to cope with both complete and incomplete databases, where, in the latter, some information is assumed to be unknown. More recently, in a series of papers, Biskup [2] and Biskup and Bonatti [3, 4, 5] deal with the same problem and investigate the relationship of various responding policies under a variety of assumptions comparing the advantages and disadvantages of the techniques of lying and refusal. Again the major goal is to provide as much information as possible to a querying agent while at the same time avoiding disclosure of secret or sensitive information. Similar problems have been investigated in the context of knowledge bases that are assumed to be expressed in some description logic or other decidable fragment of first-order logic in various other works (see, e.g., [17, 1, 10, 11, 18]).

In recent work introduced by the author [19], the common features of all these approaches were abstracted with the goal of initiating an investigation into the structure of the underlying logical systems and their algebraic and model-theoretic properties. A basic assumption is that reasoning is taking place over a fixed given sentential logic or deductive system $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$. This allows many of the techniques of universal algebra, model theory and abstract algebraic logic to be employed to study the ensuing models. Apart from the underlying logic, in the application of the framework to perform reasoning, there is always given a knowledge base K containing known facts about the "world". Moreover, part of the information contained in K, denoted by B, is considered to be known to the user, either because it constitutes background information or because the user that queries the knowledge base is not assumed to be completely uninformed about the state of the world. Finally, part of what is true in the knowledge base constitutes sensitive information that the knowledge base is supposed to keep secret from the user. Since the user is also reasoning and deducing information from the information that he has available, it is a basic assumption of the framework that both K and B are $\mathcal{S}$-theories. Furthermore, since the user is not supposed to consider true any false piece of information, we have that $B \subseteq K$ and, since the secret part S is assumed to be true in the knowledge base, we have $S \subseteq K$. For secrecy-preserving reasoning to be feasible, it is obvious that the user must neither know nor be able to deduce at the beginning any secret information, i.e., it must be the case that $B \cap S = \emptyset$. In conclusion, given the underlying deductive system $\mathcal{S}$, an $\mathcal{S}$-secrecy logic is a quadruple $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S\rangle$, where $\mathbf{Fm}_{\mathcal{L}}(V)$ is the free algebra of formulas over the language $\mathcal{L}$, K and B are $\mathcal{S}$-theories, with $B \subseteq K$, and S is a subset of K that is disjoint from B.

According to the model-theory of first-order logic, the natural models of an $\mathcal{S}$-secrecy logic are $\mathcal{S}$-secrecy structures [19]. These are tuples $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle$, where $\mathbf{A}$ is an $\mathcal{L}$-algebra, $K_{\mathcal{A}}$ and $B_{\mathcal{A}}$ are $\mathcal{S}$-filters on $\mathbf{A}$, with $B_{\mathcal{A}} \subseteq K_{\mathcal{A}}$ and $S_{\mathcal{A}} \subseteq K_{\mathcal{A}}$, such that $S_{\mathcal{A}} \cap B_{\mathcal{A}} = \emptyset$. The filters $K_{\mathcal{A}}$ and $B_{\mathcal{A}}$ are the knowledge and the browsable filters of the secrecy structure, respectively, and $S_{\mathcal{A}}$ is the secrecy set of the secrecy structure. These structures and many of the universal algebraic and model theoretic properties of their classes were investigated in [19]. In this paper, we initiate a study of the $\mathcal{S}$-secrecy logics themselves from an abstract algebraic logic perspective.

In Section 2, the formal definition of an $\mathcal{S}$-secrecy logic is introduced. We also define the notion of a safe theory of an $\mathcal{S}$-secrecy logic. Intuitively, a safe theory is a theory that consists of positive answers to queries posed against the knowledge base and that does not jeopardize secrecy. Not all answers are assumed to be truthful. In fact, it may be necessary on occasion to lie in order to protect secrets. The order-theoretic structure of the set of safe theories of a secrecy logic is examined and a consequence relation is defined based on these theories. The unfortunate characteristic is that this new logic may not be structural. It is structural only with respect to a special kind of substitutions that preserve the theories and the secrecy set defining the secrecy logic. These are termed secrecy substitutions.

In Section 3, drawing from the theory of abstract algebraic logic, we introduce Leibniz congruences for secrecy logics. A Leibniz congruence of a secrecy logic is the largest congruence on the underlying formula algebra that is compatible with each of the theories and the secrecy set of the secrecy logic. This construction gives rise to a Leibniz operator that associates with each safe theory its Leibniz congruence. The notion of a protoalgebraic logic is also introduced in this section. It is defined exactly as in the theory of abstract algebraic logic, except that the entailment used is with reference to the safe theories and not all original theories of the underlying deductive system. It is shown that, in this setting as well, protoalgebraic secrecy logics are characterized by the monotonicity of the new Leibniz operator on the safe theories of the logic. By providing a characterization of Leibniz congruences, we are able to show that, if a deductive system $\mathcal{S}$ is protoalgebraic in the ordinary sense of abstract algebraic logic, then all $\mathcal{S}$-secrecy logics must also be protoalgebraic. On the other hand, a counterexample is provided for the converse statement. There are protoalgebraic secrecy logics with non protoalgebraic underlying deductive systems. Intuitively, this phenomenon is anticipated because the choice of the theories and of the secrecy set that define the secrecy logic may drastically reduce the amount of safe theories as compared to the totality of theories of the underlying deductive system. And protoalgebraicity at this level requires looking only at this smaller set of theories.

Section 4 provides an attempt to introduce implication systems. In the ordinary theory of protoalgebraic deductive systems, it is proven that protoalgebraicity is equivalent to the existence of implication systems, i.e., sets of formulas $P(x,y)$ in two variables x,y, such that $P(\phi,\phi)$ are axioms of the logic and ϕ together with $P(\phi,\psi)$ imply ψ over the given logic, i.e., P acts collectively as the implication connective of classical logic with respect to modus ponens (see, e.g., Theorem 1.1.3 of [12]). The problem that we face when trying to carry this result over to the secrecy setting is that safe theories are not closed under inverse substitutions and, as a result, secrecy logics fail in general to be structural. Structurality is key in proving this result in abstract algebraic logic. We provide only a partial analog of this result under rather restrictive hypotheses that we do not expect to hold in many settings of practical interest. It is still open if some other method of proof or some appropriate modification of the notion exists that can relax these conditions and provide a more general version in the secrecy setting.

In Section 5 we recall the notion of an $\mathcal{S}$-secrecy structure from [19].

The notion of a safe or secrecy filter is introduced and that of a matrix of a secrecy logic. Safe filters correspond to safe theories in much the same way as filters on arbitrary algebras correspond to theories on the formula algebra in the study of deductive systems. Similarly with that framework, the notion of a Leibniz congruence may be extended to cover congruences on arbitrary algebras that are associated with given secrecy filters. We conclude the section by providing an analog of the characterization of protoalgebraic logics via the monotonicity of the associated Leibniz operators on the filters of every algebra. The characterization here is slightly different. We consider only secrecy structures for which there exists at least one strict surjective interpretation from the secrecy logic to the structure and show that the secrecy logic is protoalgebraic iff the new Leibniz operator is monotone on the collection of secrecy filters on these restricted set of secrecy structures.

Finally, in the last section of the paper, we draw on the correspondence property of protoalgebraic logics to provide yet one more characterization of protoalgebraic secrecy logics. Again, although the general spirit is very similar, attention is needed to modify the notions involved to take into account the unique features of secrecy logics. The main result characterizes protoalgebraic secrecy logics as those that have the modified correspondence property. Another characterization singles out a special class of models and, starting from strict surjective secrecy homomorphisms establishes isomorphisms between the lattices of the secrecy filters of the secrecy structures involved.

2. $\mathcal{S}$-Secrecy Logic

Given an algebraic (or logical, depending on the point of view) language type $\mathcal{L}$, let $\mathrm{Fm}_{\mathcal{L}}(V)$ be the set of all $\mathcal{L}$-terms (or $\mathcal{L}$-formulas) with variables in a fixed denumerable set V and $\mathbf{Fm}_{\mathcal{L}}(V)$ the corresponding term or formula algebra. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be an $\mathcal{L}$-deductive system, i.e., a pair consisting of a fixed language type $\mathcal{L}$ and a finitary and structural consequence relation $\vdash_{\mathcal{L}} \subseteq \mathcal{P}(\mathrm{Fm}_{\mathcal{L}}(V)) \times \mathrm{Fm}_{\mathcal{L}}(V)$, that is, a relation satisfying the following properties, for every $\Gamma \cup \Delta \cup \{\phi, \psi\} \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$:

1. $\Gamma \vdash_{\mathcal{S}} \phi$, for all $\phi \in \Gamma$,

2. $\Gamma \vdash_{\mathcal{S}} \phi$ implies $\Delta \vdash_{\mathcal{S}} \phi$, for all $\Gamma \subseteq \Delta$,
3. $\Gamma \vdash_{\mathcal{S}} \phi$ and $\Delta \vdash_{\mathcal{S}} \psi$, for all $\psi \in \Gamma$, imply $\Delta \vdash_{\mathcal{S}} \phi$,
4. $\Gamma \vdash_{\mathcal{S}} \phi$ implies $\Gamma' \vdash_{\mathcal{S}} \phi$, for some finite $\Gamma' \subseteq \Gamma$,
5. $\Gamma \vdash_{\mathcal{S}} \phi$ implies $\sigma(\Gamma) \vdash_{\mathcal{S}} \sigma(\phi)$, for every endomorphism σ of $\mathbf{Fm}_{\mathcal{L}}(V)$.

Clearly endomorphisms of $\mathbf{Fm}_{\mathcal{L}}(V)$ are fully determined by their values on the variables in V. For this reason, they are also called **assignments** or **substitutions**.

We define next the notion of an $\mathcal{S}$-secrecy logic. $\mathcal{S}$-secrecy logics were first introduced in [19] and will be the main objects of study in this paper. Recall, e.g. from [12], that, given a deductive system $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ and an $\mathcal{L}$-algebra $\mathbf{A} = \langle A, \mathcal{L}^{\mathbf{A}} \rangle$, a subset $F \subseteq A$ is called an **$\mathcal{S}$-filter on A** if, for all $\Gamma \cup \{\phi\} \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$, such that $\Gamma \vdash_{\mathcal{S}} \phi$ and every homomorphism $h : \mathbf{Fm}_{\mathcal{L}}(V) \to \mathbf{A}$,

$$h(\Gamma) \subseteq F \quad \text{implies} \quad h(\phi) \in F.$$

The collection of all $\mathcal{S}$-filters on $\mathbf{A}$ is denoted by $\mathrm{Fi}_{\mathcal{S}}\mathbf{A}$ and forms a complete algebraic lattice under inclusion, denoted $\mathbf{Fi}_{\mathcal{S}}\mathbf{A} = \langle \mathrm{Fi}_{\mathcal{S}}\mathbf{A}, \subseteq \rangle$. The collection of $\mathcal{S}$-filters on the formula algebra coincides with the set of $\mathcal{S}$-theories

$$\mathrm{Th}\mathcal{S} = \{T \subseteq \mathrm{Fm}_{\mathcal{L}}(V) : (\forall \phi \in \mathrm{Fm}_{\mathcal{L}}(V))(T \vdash_{\mathcal{S}} \phi \text{ implies } \phi \in T)\}.$$

It is well-known from the theory of abstract algebraic logic that $\mathrm{Th}\mathcal{S}$ is closed under inverse substitutions (due to the structurality of the deductive system $\mathcal{S}$).

Definition 2.1. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system. A **secrecy logic $\mathfrak{S}$ over $\mathcal{S}$**, or an **$\mathcal{S}$-secrecy logic**, is a quadruple $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$, where

1. $K, B \in \mathrm{Th}\mathcal{S}$, such that $B \subseteq K$;
2. $S \subseteq K$, such that $S \cap B = \emptyset$.

K is called the **knowledge theory**, B the **browsable theory** and S the **secrect set** of $\mathfrak{S}$.

Given an $\mathcal{S}$-secrecy logic $\mathfrak{S}$, a substitution $h : \mathbf{Fm}_{\mathcal{L}}(V) \to \mathbf{Fm}_{\mathcal{L}}(V)$ is called an **$\mathfrak{S}$-substitution** if $h(K) \subseteq K$, $h(B) \subseteq B$ and $h(S) \subseteq S$. It is called a **strict $\mathfrak{S}$-substitution** if $K = h^{-1}(K), B = h^{-1}(B)$ and $S = h^{-1}(S)$.

Our analysis of $\mathcal{S}$-secrecy logics will rely to a large extent on the notion of a safe theory. Roughly speaking, safe theories constitute sets of formulas that, when posed as queries by an agent querying the knowledge base represented by the secrecy logic, may be given a positive answer safely without jeopardizing the secret status of the set S and without lying on the browsable theory B, that contains information that the agent is assumed to already know.

Definition 2.2. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be a secrecy logic over $\mathcal{S}$. A theory $T \in \mathrm{Th}\mathcal{S}$ is said to be a **safe theory (with respect to)** $\mathfrak{S}$ if $B \subseteq T$ and $T \cap S = \emptyset$. We write

$$\mathrm{STh}\mathcal{S} = \{T \in \mathrm{Th}\mathcal{S} : B \subseteq T \text{ and } T \cap S = \emptyset\}.$$

Note that the definition means that, if T is a safe theory, then all browsable formulas are contained in T and no secret formula is in T. Since T is a theory, this also implies that no secret formula may be entailed by T. It is not difficult to see, using Zorn's Lemma, that every safe theory is contained in a maximal safe theory.

Proposition 2.3. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ a secrecy logic over $\mathcal{S}$. Every safe theory $T \in \mathrm{STh}\mathcal{S}$ is contained in a maximal safe theory.*

Proof. Let $T \in \mathrm{STh}\mathcal{S}$. Consider the set

$$\begin{aligned} \mathfrak{T} &= \{Q \in \mathrm{STh}\mathcal{S} : T \subseteq Q\} \\ &= \{Q \in \mathrm{Th}\mathcal{S} : T \subseteq Q \text{ and } Q \cap S = \emptyset\}. \end{aligned}$$

This set is nonempty, since $T \in \mathfrak{T}$. Moreover, it is relatively easy to see that any chain in $\mathfrak{T}$ has an upper bound in $\mathfrak{T}$, namely the union of all its members. Thus, by Zorn's Lemma, $\mathfrak{T}$ has a maximal element, which, obviously, contains T. □

One of the most problematic features of the collection $\mathrm{STh}\mathcal{S}$, as regards the analysis of its structure from the abstract algebraic logic point of view, is that it is not, in general, invariant under inverse substitutions. Consider, for instance, a secrecy logic $\mathfrak{S}$ that contains in its browsable theory B a propositional variable b and in its secret set S a propositional variable s. Then, the substitution h that sends s to b and fixes the values of all other variables does not preserve $\mathrm{STh}\mathcal{S}$ with respect to $\mathfrak{S}$. To see this, it suffices to notice that $h^{-1}(B) \cap S \neq \emptyset$, which implies that $h^{-1}(B) \notin \mathrm{STh}\mathcal{S}$, despite the fact that $B \in \mathrm{STh}\mathcal{S}$.

In contrast to this state of affairs, it is an encouraging observation that $\mathrm{STh}\mathcal{S}$ is invariant under all $\mathfrak{S}$-substitutions.

Proposition 2.4. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ a secrecy logic over $\mathcal{S}$. Then for every $\mathfrak{S}$-substitution h, $h^{-1}(\mathrm{STh}\mathcal{S}) \subseteq \mathrm{STh}\mathcal{S}$.*

Proof. Suppose $T \in \mathrm{STh}\mathcal{S}$. Then $T \in \mathrm{Th}(\mathcal{S})$, such that $B \subseteq T$ and $T \cap S = \emptyset$. Then, we have (by standard sentential logic arguments) that $h^{-1}(T) \in \mathrm{Th}\mathcal{S}$ and, moreover, $B \subseteq h^{-1}(B) \subseteq h^{-1}(T)$ and $h^{-1}(T) \cap h^{-1}(S) = \emptyset$, which, since $S \subseteq h^{-1}(S)$, yields $h^{-1}(T) \cap S = \emptyset$. Hence $h^{-1}(T) \in \mathrm{STh}\mathcal{S}$. □

According to [15], a **complete semilattice** is defined to be a poset $\mathbf{L} = \langle L, \leq \rangle$, such that, for every nonempty $A \subseteq L$, $\bigwedge A$ exists and, for any directed set $D \subseteq L$, $\bigvee D$ also exists. By the definition of a safe theory, it is clear that the next proposition holds:

Proposition 2.5. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ a secrecy logic over $\mathcal{S}$. $\mathrm{STh}\mathcal{S}$ is a complete meet-subsemilattice of the complete meet-semilattice of all theories of $\mathcal{S}$. Moreover, B is the least element of $\mathrm{STh}\mathcal{S}$.*

By adjoining to $\mathrm{STh}\mathcal{S}$ the largest element $\mathrm{Fm}_{\mathcal{L}}(V)$ of $\mathrm{Th}\mathcal{S}$, which, although it is not a safe theory in our sense unless $S = \emptyset$, it is used to denote inconsistent secrecy reasoning, we obtain a complete lattice $\mathbf{STh}^{\top}\mathcal{S} = \langle \mathrm{STh}^{\top}\mathcal{S}, \leq \rangle$. This, however, is not a sublattice of the complete algebraic lattice $\mathbf{Th}\mathcal{S} = \langle \mathrm{Th}\mathcal{S}, \leq \rangle$.

The elements in $\mathrm{STh}^{\top}\mathcal{S}$ may be used to generate a new deductive system $\mathcal{S}_{\mathfrak{S}}$ as detailed in the following:

Definition 2.6. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be a secrecy logic over $\mathcal{S}$. Define $\mathcal{S}_{\mathfrak{S}} = \langle \mathcal{L}, \vdash_{\mathfrak{S}} \rangle$ by setting, for all $\Gamma \cup \{\phi\} \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$,

$$\Gamma \vdash_{\mathfrak{S}} \phi \quad \text{iff, for every } T \in \mathrm{STh}^{\top}\mathcal{S}, \ (\Gamma \subseteq T \text{ implies } \phi \in T).$$

We denote by $\mathrm{Th}\mathcal{S}_{\mathfrak{S}}$ the collection of all $\mathcal{S}_{\mathfrak{S}}$-theories, i.e., of all sets $T \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$, such that, for all $\phi \in \mathrm{Fm}_{\mathcal{L}}(V)$, $T \vdash_{\mathfrak{S}} \phi$, implies $\phi \in T$. It is not difficult to see that $\vdash_{\mathfrak{S}}$ is a consequence relation on $\mathrm{Fm}_{\mathcal{L}}(V)$ that is **$\mathfrak{S}$-structural** in the sense that, for every $\mathfrak{S}$-substitution h, $\Gamma \vdash_{\mathfrak{S}} \phi$ implies that $h(\Gamma) \vdash_{\mathfrak{S}} h(\phi)$, for all $\Gamma \cup \{\phi\} \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$. These remarks form the contents of the following proposition.

Proposition 2.7. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ a secrecy logic over $\mathcal{S}$.*

1. *$\vdash_{\mathfrak{S}}$ is an $\mathfrak{S}$-structural consequence relation;*
2. *$\mathrm{Th}\mathcal{S}_{\mathfrak{S}} = \mathrm{STh}^{\top}\mathcal{S}$.*

Proof.

1. That $\vdash_{\mathfrak{S}}$ is a consequence relation is obvious from Definition 2.6. Suppose that $\Gamma \vdash_{\mathfrak{S}} \phi$, h an $\mathfrak{S}$-substitution and $T \in \mathrm{STh}^{\top}\mathcal{S}$, such that $h(\Gamma) \subseteq T$. Then $\Gamma \subseteq h^{-1}(T) \in \mathrm{STh}^{\top}\mathcal{S}$, by Proposition 2.4. Hence, since $\Gamma \vdash_{\mathfrak{S}} \phi$, we get that $\phi \in h^{-1}(T)$, i.e., $h(\phi) \in T$. This shows that $h(\Gamma) \vdash_{\mathfrak{S}} h(\phi)$, whence $\vdash_{\mathfrak{S}}$ is $\mathfrak{S}$-structural.

2. Suppose, first, that $T \in \mathrm{STh}\mathcal{S}$, i.e., $T \in \mathrm{Th}\mathcal{S}$, such that $B \subseteq T$ and $T \cap S = \emptyset$. Let $\phi \in \mathrm{Fm}_{\mathcal{L}}(V)$, such that $T \vdash_{\mathfrak{S}} \phi$. Then, since $T \subseteq T \in \mathrm{STh}\mathcal{S}$, we have $\phi \in T$. Thus, T is a theory of $\mathcal{S}_{\mathfrak{S}}$.

   Assume, conversely, that $T \in \mathrm{Th}\mathcal{S}_{\mathfrak{S}}$. Since, by definition, $T = \mathrm{Fm}_{\mathcal{L}}(V) \in \mathrm{STh}^{\top}\mathcal{S}$, we assume that $T \neq \mathrm{Fm}_{\mathcal{L}}(V)$. If, for every $T' \in \mathrm{STh}\mathcal{S}$, $T \not\subseteq T'$, then $C_{\mathfrak{S}}(T) := \bigcap\{T' \in \mathrm{STh}^{\top}\mathcal{S} : T \subseteq T'\} = \mathrm{Fm}_{\mathcal{L}}(V)$, which contradicts $T \neq \mathrm{Fm}_{\mathcal{L}}(V)$. Thus, there exists $T' \in \mathrm{STh}\mathcal{S}$, such that $T \subseteq T'$. Now observe that

   $$T \subseteq \bigcap\{T' \in \mathrm{Th}\mathcal{S} : T \subseteq T'\} \subseteq \bigcap\{T' \in \mathrm{STh}\mathcal{S} : T \subseteq T'\} = C_{\mathfrak{S}}(T) = T.$$

   Thus, $T = \bigcap\{T' \in \mathrm{Th}\mathcal{S} : T \subseteq T'\} = C_{\mathcal{S}}(T)$, showing that $T \in \mathrm{Th}\mathcal{S}$.

□

3. Protoalgebraicity

In the theory of abstract algebraic logic, one of the most important notions, that plays a crucial role in the classification of logics in a hierarchy reflecting the strength of their algebraic character, is that of the Leibniz operator [7]. Recall that, given a congruence θ on an $\mathcal{L}$-algebra $\mathbf{A} = \langle A, \mathcal{L}^{\mathbf{A}} \rangle$ and a subset $F \subseteq A$, θ is said to be **compatible with** F if, for all $a, b \in A$

$$\langle a, b \rangle \in \theta \text{ and } a \in F \text{ imply } b \in F.$$

Given a deductive system $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ and a theory $T \in \mathrm{Th}\mathcal{S}$ (or, more generally, any subset $T \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$), the Leibniz congruence associated with T, written $\Omega_{\mathcal{S}}(T)$, is the largest congruence on the formula algebra $\mathbf{Fm}_{\mathcal{L}}(V)$ that is compatible with T. Moreover, given an $\mathcal{L}$-algebra $\mathbf{A} = \langle A, \mathcal{L}^{\mathbf{A}} \rangle$ and a filter $F \in \mathrm{Fi}_{\mathcal{S}}\mathbf{A}$ (or, similarly, any subset $F \subseteq A$), the Leibniz congruence of F on $\mathbf{A}$, written $\Omega_{\mathbf{A}}(F)$, is the largest congruence on $\mathbf{A}$ that is compatible with F. $\Omega_{\mathcal{S}}$ and $\Omega_{\mathbf{A}}$ seen as functions from $\mathcal{S}$-theories and $\mathcal{S}$-filters, respectively, to congruences are termed the Leibniz operators on $\mathbf{Fm}_{\mathcal{L}}(V)$ and $\mathbf{A}$, respectively. Recall from [6] (see also [12, 13, 14]) that a deductive system $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ is said to be protoalgebraic if, for every theory $T \in \mathrm{Th}\mathcal{S}$ and all $\phi, \psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, such that $\langle \phi, \psi \rangle \in \Omega_{\mathcal{S}}(T)$, we have $T, \phi \dashv\vdash_{\mathcal{S}} T, \psi$.

To formulate the notion of protoalgebraic $\mathcal{S}$-secrecy logic, we introduce, first, the notion of the Leibniz congruence on an $\mathcal{S}$-secrecy logic.

Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic. A congruence on $\mathbf{Fm}_{\mathcal{L}}(V)$ is called a **safe congruence** or a **secrecy congruence** if it is compatible with each of K, B and S.

Proposition 3.1. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic. Then, there exists a largest safe congruence on the formula algebra $\mathbf{Fm}_{\mathcal{L}}(V)$.*

Proof. As in the proof of the existence of the Leibniz congruence associated with a given theory of a deductive system in abstract algebraic logic, one may show that the hypothesis of Zorn's Lemma holds for the collection of all safe congruences on $\mathbf{Fm}_{\mathcal{L}}(V)$. Therefore this set has a maximal element. However, it is not difficult to see either that, given two such congruences, their join in the lattice of congruences on $\mathbf{Fm}_{\mathcal{L}}(V)$ is also a safe congruence. Hence there is a unique maximal safe congruence, which is the largest safe congruence of $\mathcal{S}$. □

Definition 3.2. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic. The largest safe congruence on $\mathbf{Fm}_{\mathcal{L}}(V)$, which always exists, by Proposition 3.1, is called the **Leibniz congruence of** $\mathfrak{S}$ and denoted by $\Omega(\mathfrak{S})$.

Next, we introduce the notion of the Leibniz congruence associated with a safe theory of an $\mathcal{S}$-secrecy logic $\mathfrak{S}$. This also gives rise to the notion of a Leibniz operator on $\mathfrak{S}$.

Proposition 3.3. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be an $\mathcal{S}$-secrecy logic, and let $T \in \mathrm{STh}^{\top}\mathcal{S}$. Then, there exists a largest safe congruence on $\mathbf{Fm}_{\mathcal{L}}(V)$ that is compatible with T.*

Proof. The proof is very similar to that of Proposition 3.1 and will be omitted. □

Definition 3.4. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be an $\mathcal{S}$-secrecy logic, and let $T \in \mathrm{STh}^{\top}\mathcal{S}$. The largest safe congruence on $\mathbf{Fm}_{\mathcal{L}}(V)$ that is compatible with T, which always exists, by Proposition 3.3, is called the **safe Leibniz congruence of** T and denoted by $\Omega_{\mathfrak{S}}(T)$. The function $\Omega_{\mathfrak{S}} : \mathrm{STh}^{\top}\mathcal{S} \to \mathrm{Con}\mathbf{Fm}_{\mathcal{L}}(V)$ is called the **safe Leibniz operator** of $\mathfrak{S}$.

We are now well equipped to define the notion of a protoalgebraic $\mathcal{S}$-secrecy logic.

Definition 3.5. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic. $\mathfrak{S}$ will be said to be **protoalgebraic** if, for all $T \in \mathrm{STh}^{\top}\mathcal{S}$ and all $\phi, \psi \in \mathrm{Fm}_{\mathcal{L}}(V)$,

$$\langle \phi, \psi \rangle \in \Omega_{\mathfrak{S}}(T) \text{ implies } T, \phi \dashv\vdash_{\mathfrak{S}} T, \psi.$$

The following theorem constitutes an analog of the well-known theorem of abstract algebraic logic characterizing protoalgebraic deductive systems in terms of the monotonicity of their Leibniz operator [6, 12].

Theorem 3.6. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be an $\mathcal{S}$-secrecy logic. $\mathfrak{S}$ is protoalgebraic iff, for all $T_1, T_2 \in \mathrm{STh}^{\top}\mathcal{S}$,*

$$T_1 \subseteq T_2 \textit{ implies } \Omega_{\mathfrak{S}}(T_1) \subseteq \Omega_{\mathfrak{S}}(T_2).$$

Proof. Suppose, first, that $\mathfrak{S}$ is protoalgebraic. Let $T_1, T_2 \in \mathrm{STh}^{\top}\mathcal{S}$, such that $T_1 \subseteq T_2$. To see that $\Omega_{\mathfrak{S}}(T_1) \subseteq \Omega_{\mathfrak{S}}(T_2)$, it suffices to show that $\Omega_{\mathfrak{S}}(T_1)$ is a safe congruence that is compatible with T_2, since $\Omega_{\mathfrak{S}}(T_2)$ is the largest such. Since $\Omega_{\mathfrak{S}}(T_1)$ is safe, by definition, it suffices to show its compatibility with T_2. Let $\phi, \psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, such that $\langle \phi, \psi \rangle \in \Omega_{\mathfrak{S}}(T_1)$ and $\phi \in T_2$. Then, by protoalgebraicity, $T_1, \phi \dashv\vdash_{\mathfrak{S}} T_1, \psi$, whence, since $T_1 \subseteq T_2$, we get $T_2, \phi \dashv\vdash_{\mathfrak{S}} T_2, \psi$ and, since $\phi \in T_2$, by Proposition 2.7, $\psi \in T_2$. Hence $\Omega_{\mathfrak{S}}(T_1)$ is compatible with T_2.

Assume, conversely, that, for every $T_1, T_2 \in \mathrm{STh}^{\top}\mathcal{S}$, with $T_1 \subseteq T_2$, we have $\Omega_{\mathfrak{S}}(T_1) \subseteq \Omega_{\mathfrak{S}}(T_2)$. Let $T \in \mathrm{STh}^{\top}\mathcal{S}$ and $\phi, \psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, such that $\langle \phi, \psi \rangle \in \Omega_{\mathfrak{S}}(T)$. Consider the safe theory $T' = C_{\mathfrak{S}}(T \cup \{\phi\})$. Then, we have $T \subseteq T'$, whence, by hypothesis, $\Omega_{\mathfrak{S}}(T) \subseteq \Omega_{\mathfrak{S}}(T')$ and, since $\langle \phi, \psi \rangle \in \Omega_{\mathfrak{S}}(T)$, we obtain $\langle \phi, \psi \rangle \in \Omega_{\mathfrak{S}}(T')$. But $\phi \in T'$, whence, by compatibility, $\psi \in T'$, showing that $T, \phi \vdash_{\mathfrak{S}} \psi$. By symmetry $T, \phi \dashv\vdash_{\mathfrak{S}} T, \psi$ and $\mathfrak{S}$ is protoalgebraic. □

Theorem 3.6 may be used to provide clues regarding the relation between ordinary protoalgebraicity of a deductive system $\mathcal{S}$ and protoalgebraicity of an $\mathcal{S}$-secrecy logic. More specifically, we would like to know whether there is a connection between a deductive system $\mathcal{S}$ being protoalgebraic in the ordinary sense and an $\mathcal{S}$-secrecy logic being protoalgebraic in the sense of Definition 3.5.

Example: Consider any non-protoalgebraic deductive system $\mathcal{S}$ that has a one-element theory, denoted by $\{\top\}$. Let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be the $\mathcal{S}$-secrecy logic defined by

- $K = \mathrm{Fm}_{\mathcal{L}}(V)$;
- $B = \{\top\}$;
- $S = \mathrm{Fm}_{\mathcal{L}}(V) \backslash \{\top\}$.

Since $\mathrm{STh}^{\top}\mathcal{S} = \{\{\top\}, \mathrm{Fm}_{\mathcal{L}}(V)\}$ and $\Omega_{\mathfrak{S}}(\{\top\}) = \Omega_{\mathfrak{S}}(\mathrm{Fm}_{\mathcal{L}}(V)) = \Omega(\mathfrak{S})$, we get that $\mathfrak{S}$ is protoalgebraic. This example illustrates the fact that the protoalgebraicity of $\mathfrak{S}$ depends crucially on K, B and S, besides the underlying deductive system $\mathcal{S}$. □

On the other hand, it is true that, if a deductive system $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ is protoalgebraic in the standard sense, then every $\mathcal{S}$-secrecy logic $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ is protoalgebraic. To show this, we prove the following general proposition relating the Leibniz congruences associated with the sets K, B and S of $\mathfrak{S}$ and the safe Leibniz congruence of a safe theory T of $\mathfrak{S}$.

Proposition 3.7. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic. Then*

1. $\Omega(\mathfrak{S}) = \Omega_{\mathcal{S}}(K) \cap \Omega_{\mathcal{S}}(B) \cap \Omega_{\mathcal{S}}(S)$.
2. *For every safe theory $T \in \mathrm{STh}\mathcal{S}$, $\Omega_{\mathfrak{S}}(T) = \Omega(\mathfrak{S}) \cap \Omega_{\mathcal{S}}(T)$.*

Proof.

1. Since $\Omega(\mathfrak{S})$ is compatible with each of K, B and S, we have that $\Omega(\mathfrak{S}) \subseteq \Omega_{\mathcal{S}}(K)$, $\Omega(\mathfrak{S}) \subseteq \Omega_{\mathcal{S}}(B)$ and $\Omega(\mathfrak{S}) \subseteq \Omega_{\mathcal{S}}(S)$. Therefore $\Omega(\mathfrak{S}) \subseteq \Omega_{\mathcal{S}}(K) \cap \Omega_{\mathcal{S}}(B) \cap \Omega_{\mathcal{S}}(S)$. On the other hand, $\Omega_{\mathcal{S}}(K) \cap \Omega_{\mathcal{S}}(B) \cap \Omega_{\mathcal{S}}(S)$ is a congruence on $\mathbf{Fm}_{\mathcal{L}}(V)$, which is compatible with each of K, B and S. Therefore, by the definition of $\Omega(\mathfrak{S})$, we get that $\Omega_{\mathcal{S}}(K) \cap \Omega_{\mathcal{S}}(B) \cap \Omega_{\mathcal{S}}(S) \subseteq \Omega(\mathfrak{S})$.
2. Since $\Omega_{\mathfrak{S}}(T)$ is compatible with each of K, B, S and T, we have that $\Omega_{\mathfrak{S}}(T) \subseteq \Omega_{\mathcal{S}}(K)$, $\Omega_{\mathfrak{S}}(T) \subseteq \Omega_{\mathcal{S}}(B)$, $\Omega_{\mathfrak{S}}(T) \subseteq \Omega_{\mathcal{S}}(S)$ and $\Omega_{\mathfrak{S}}(T) \subseteq \Omega_{\mathcal{S}}(T)$. Therefore, $\Omega_{\mathfrak{S}}(T) \subseteq \Omega(\mathfrak{S}) \cap \Omega_{\mathcal{S}}(T)$. On the other hand, it can be easily verified that $\Omega(\mathfrak{S}) \cap \Omega_{\mathcal{S}}(T)$ is a congruence on $\mathbf{Fm}_{\mathcal{L}}(V)$, that is compatible with each of K, B, S and T. Since, by definition, $\Omega_{\mathfrak{S}}(T)$ is the largest such, we get that $\Omega(\mathfrak{S}) \cap \Omega_{\mathcal{S}}(T) \subseteq \Omega_{\mathfrak{S}}(T)$.

□

Proposition 3.7 allows us to prove that the protoalgebraicity of $\mathcal{S}$ in the sense of abstract algebraic logic implies the protoalgebraicity of every $\mathcal{S}$-secrecy logic.

Corollary 3.8. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be an $\mathcal{S}$-secrecy logic. If $\mathcal{S}$ is protoalgebraic, then $\mathfrak{S}$ is protoalgebraic.*

Proof. If $\mathcal{S}$ is protoalgebraic, then the Leibniz operator $\Omega_{\mathcal{S}}$ is monotone on the lattice of $\mathcal{S}$-theories. Therefore, for every $T_1, T_2 \in \mathrm{STh}^{\top}(\mathcal{S})$, such that $T_1 \subseteq T_2$, we obtain

$$\begin{array}{rcl} \Omega_{\mathfrak{S}}(T_1) & = & \Omega(\mathfrak{S}) \cap \Omega_{\mathcal{S}}(T_1) \quad \text{(by Proposition 3.7)} \\ & \subseteq & \Omega(\mathfrak{S}) \cap \Omega_{\mathcal{S}}(T_2) \quad \text{(by protoalgebraicity)} \\ & = & \Omega_{\mathfrak{S}}(T_2) \quad \text{(by Proposition 3.7)}, \end{array}$$

whence, by Theorem 3.6, $\mathfrak{S}$ is protoalgebraic. □

4. Implication Systems

In this section, an attempt is made to relate protoalgebraicity of secrecy logics with existence of an analog of implication systems of abstract algebraic logic. Recall from the theory of abstract algebraic logic that a deductive system $\mathcal{S}$ is protoalgebraic iff there exists a possibly infinite set $P(p,q)$ of formulas in two variables p and q, called an **implication system**, such that $\vdash_{\mathcal{S}} P(\phi,\phi)$ and $\phi, P(\phi,\psi) \vdash_{\mathcal{S}} \psi$, for all formulas ϕ,ψ. We would like to prove a similar result, if possible, for secrecy logics, i.e., that a secrecy logic is protoalgebraic iff such a set exists that satisfies the two conditions, where $\mathcal{S}$ is replaced by $\mathcal{S}_{\mathfrak{S}}$. However, one of the key properties that allows the proof of the result in the traditional setting is the structurality of $\mathcal{S}$. And we have already seen that $\mathfrak{S}$ is only $\mathfrak{S}$-structural, but not structural, in general. Therefore, we are able in this section to carry the result over to the secrecy setting only under some stringent hypotheses on the secrecy logic that make it possible to use some necessary aspects of structurality.

We say that a set of formulas $\Phi \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$ is **closed under** a substitution σ or that it is **σ-invariant** if $\sigma(\Phi) \subseteq \Phi$.

Suppose that $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ is a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ is an $\mathcal{S}$-secrecy logic. Define

$$E_{\mathfrak{S}} = \{\phi(p,q,\vec{r}) : \phi(p,p,\vec{r}) \in B\}.$$

If the two variables $p, q \in V$ are such that the substitution $\sigma_{p\to q}$, mapping q to p and leaving all other variables fixed, is an $\mathfrak{S}$-substitution, then, by Proposition 2.4, $E_{\mathfrak{S}}$ is a safe theory. The same holds in case B is $\sigma_{p\to q}$-invariant. Moreover, although the analog of Lemma 1.1.2 of [12] does not hold in general, it may be shown that it does under some additional conditions.

Lemma 4.1. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be an $\mathcal{S}$-secrecy logic. Suppose $\sigma_{p \to q}$ is an $\mathfrak{S}$-substitution or that B is $\sigma_{p \to q}$-invariant.*

1. *If e is an $\mathfrak{S}$-substitution or B is e-invariant, respectively, and $\sigma_{p \to q}(ep) = \sigma_{p \to q}(eq)$, then $E_{\mathfrak{S}}$ is closed under e.*
2. *If $\langle p, q \rangle \in \Omega(\mathfrak{S})$, then $\langle p, q \rangle \in \Omega_{\mathfrak{S}}(E_{\mathfrak{S}})$.*

Proof.

1. Suppose $\sigma_{p \to q}(e(p)) = \sigma_{p \to q}(e(q))$. Let $\phi \in E_{\mathfrak{S}}$. Then $\sigma_{p \to q}(\phi) \in B$, by the definition of $E_{\mathfrak{S}}$. By easy induction on the complexity of ϕ, we can see that $\sigma_{p \to q}(e(\phi)) = \sigma_{p \to q}(e(\sigma_{p \to q}(\phi)))$. Thus, by the invariance of B, we get that $\sigma_{p \to q}(e(\sigma_{p \to q}(\phi))) \in B$. Therefore, by the equality above, $\sigma_{p \to q}(e(\phi)) \in B$, showing that $e(\phi) \in E_{\mathfrak{S}}$. Thus, $E_{\mathfrak{S}}$ is e-invariant.
2. We have $\sigma_{p \to q}(\sigma_{p \to r}(\phi)) = \sigma_{p \to q}(\sigma_{q \to r}(\phi))$, for every formula ϕ. Therefore, $\sigma_{p \to q}(\sigma_{p \to r}(\phi)) \in B$ iff $\sigma_{p \to q}(\sigma_{q \to r}(\phi)) \in B$, showing that $\sigma_{p \to r}(\phi) \in E_{\mathfrak{S}}$ iff $\sigma_{q \to r}(\phi) \in E_{\mathfrak{S}}$. This shows that $\langle p, q \rangle \in \Omega_{\mathcal{S}}(E_{\mathfrak{S}})$ and, since, by hypothesis $\langle p, q \rangle \in \Omega(\mathfrak{S})$, we get, by Proposition 3.7, that $\langle p, q \rangle \in \Omega_{\mathfrak{S}}(E_{\mathfrak{S}})$.

□

Using Lemma 4.1, we may now prove that, under some conditions on the secrecy logic under consideration, protoalgebraicity of the secrecy logic is equivalent to the existence of an implication system relative to the logic. This theorem forms an analog of Theorem 1.1.3 of [12], characterizing protoalgebraic deductive systems in terms of the existence of implication systems.

Theorem 4.2. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be an $\mathcal{S}$-secrecy logic. Assume that p, q are such that, for all $\phi, \psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, the substitution $\sigma_{\phi \to p, \psi \to q}$, that sends p to ϕ and q to ψ and leaves all other variables fixed, and the substitution σ, that fixes p and sends every other variable to q, are $\mathfrak{S}$-substitutions and that $\langle p, q \rangle \in \Omega(\mathfrak{S})$. Then, the following are equivalent:*

1. *$\mathfrak{S}$ is protoalgebraic;*

2. *$q \in C_{\mathfrak{S}}(\{p\} \cup E_{\mathfrak{S}})$;*

3. *There exists a set $P(p,q) \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$ in the two variables p,q, such that $P(p,p) \subseteq B$ and $q \in C_{\mathfrak{S}}(\{p\} \cup P(p,q))$.*

Proof.

$(1 \to 2)$: By Lemma 4.1.2, we get that $\langle p,q\rangle \in \Omega_{\mathfrak{S}}(E_{\mathfrak{S}})$. Thus, by protoalgebraicity and Theorem 3.6, $\langle p,q\rangle \in \Omega_{\mathfrak{S}}(C_{\mathfrak{S}}(\{p\} \cup E_{\mathfrak{S}}))$. Therefore, by the compatibility property, we get $q \in C_{\mathfrak{S}}(\{p\} \cup E_{\mathfrak{S}})$.

$(2 \to 3)$: Let $P(p,q) = \sigma(E_{\mathfrak{S}})$. Then, $\sigma_{p\to q}(\sigma(p)) = p = \sigma_{p\to q}(\sigma(q))$, whence, by Lemma 4.1.1, $E_{\mathfrak{S}}$ is σ-invariant, showing that $P(p,q) \subseteq E_{\mathfrak{S}}$. Therefore $P(p,p) \subseteq B$. Since σ is assumed to be an $\mathfrak{S}$-substitution, we obtain, by Part 1 of Proposition 2.7, that $q \in C_{\mathfrak{S}}(\{p\} \cup P(p,q))$.

$(3 \to 1)$: Let $\phi,\psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, $T \in \mathrm{STh}^{\top}\mathcal{S}$ and $\langle \phi,\psi\rangle \in \Omega_{\mathfrak{S}}(T)$. Then, by the congruence property, for all $\delta \in P(p,q)$, $\langle \delta(\phi,\phi), \delta(\phi,\psi)\rangle \in \Omega_{\mathfrak{S}}(T)$. But, by hypothesis and the fact that $\sigma_{\phi\to p,\psi\to q}$ is an $\mathfrak{S}$-substitution, we get that $\delta(\phi,\phi) \in B \subseteq T$, whence, by compatibility, $P(\phi,\psi) \subseteq T$. Once more, by hypothesis and the fact that $\sigma_{\phi\to p,\psi\to q}$ is an $\mathfrak{S}$-substitution, we get that $\psi \in C_{\mathfrak{S}}(\{\phi\} \cup P(\phi,\psi)) \subseteq C_{\mathfrak{S}}(T \cup \{\phi\})$. By symmetry, we obtain $T,\phi \dashv\vdash_{\mathfrak{S}} T,\psi$ and $\mathfrak{S}$ is protoalgebraic.

□

Although Proposition 4.2 provides a characterization of protoalgebraicity for an $\mathcal{S}$-secrecy logic, it is not very satisfactory, since the hypotheses are rather strict. For instance, if p or q are in either B or S, then the assumption that, for all $\phi,\psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, the substitutions $\sigma_{\phi\to p,\psi\to q}$ are $\mathfrak{S}$-substitutions forces B or S, respectively, to be $\mathrm{Fm}_{\mathcal{L}}(V)$. In the first case, the secrecy logic has the single safe theory $\mathrm{Fm}_{\mathcal{L}}(V)$ and, in the second, the only safe theory is $\emptyset$, if $\mathcal{S}$ does not have theorems, and there is no safe theory, otherwise. Thus in either case, the hypotheses lead into a trivial secrecy logic in some sense. However, under less stringent hypotheses, it might not be possible to do much better, given the wide variety of secrecy logics that might be obtained by varying the knowledge and browsable theories and the secrecy set of the logic.

5. Leibniz Operator on Secrecy Structures

The natural models for secrecy logics, according to the model theory of first-order logic, are the secrecy structures that were introduced in [19]. Several of the universal algebraic and categorical properties of their classes were considered. In this section we review the definition and define the Leibniz congruence of a secrecy matrix, which consists of a secrecy structure together with a secrecy filter on the structure. We show that protoalgebraicity of secrecy logics may be characterized by the monotonicity of a Leibniz operator on the secrecy filters of an appropriately chosen subclass of the class of all secrecy structures.

Definition 5.1. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system. An **$\mathcal{S}$-secrecy structure** $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ is a quadruple consisting of

1. An $\mathcal{L}$-algebra $\mathbf{A} = \langle A, \mathcal{L}^{\mathbf{A}} \rangle$;

2. Two $\mathcal{S}$-filters $K_{\mathcal{A}}, B_{\mathcal{A}}$ on $\mathbf{A}$, such that $B_{\mathcal{A}} \subseteq K_{\mathcal{A}}$;

3. A subset $S_{\mathcal{A}} \subseteq K_{\mathcal{A}}$, such that $S_{\mathcal{A}} \cap B_{\mathcal{A}} = \emptyset$.

The $\mathcal{S}$-filters $K_{\mathcal{A}}$ and $B_{\mathcal{A}}$ are referred to as the **knowledge** and **browsable filter**, respectively, and $S_{\mathcal{A}}$ as the **secrecy set** of the $\mathcal{S}$-secrecy structure $\mathcal{A}$.

Secrecy interpretations correspond to algebra homomorphisms from the free formula algebra to a given algebra that map the theories and the secrecy set of a given secrecy logic into the corresponding filters and secrecy set of a secrecy structure with underlying algebra the given algebra.

Definition 5.2. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure. A **secrecy interpretation** $h : \mathfrak{S} \to \mathcal{A}$ is an $\mathcal{L}$-homomorphism $h : \mathbf{Fm}_{\mathcal{L}}(V) \to \mathbf{A}$, such that $h(K) \subseteq K_{\mathcal{A}}$, $h(B) \subseteq B_{\mathcal{A}}$ and $h(S) \subseteq S_{\mathcal{A}}$.
A secrecy interpretation h is called **strict** if

$$K = h^{-1}(K_{\mathcal{A}}), \quad B = h^{-1}(B_{\mathcal{A}}), \quad S = h^{-1}(S_{\mathcal{A}}).$$

It is called **surjective** if h is surjective.

Notice that a secrecy interpretation is a special case of a secrecy homomorphism, as defined in [19]. The same holds for strict and surjective secrecy interpretations. They form, respectively, special cases of strict and surjective secrecy homomorphisms between $\mathcal{S}$-secrecy structures.

For arbitrary $\mathcal{S}$-secrecy structures, safe sets are subsets of their domain, that contain the browsable filter and are disjoint from the secrecy set.

Definition 5.3. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure. A subset $F \subseteq A$ is called **safe** if $B_{\mathcal{A}} \subseteq F$ and $F \cap S_{\mathcal{A}} = \emptyset$.

Based on this notion, the notion of a secrecy filter or $\mathfrak{S}$-filter on a secrecy structure may be defined. These are safe sets that happen to be $\mathcal{S}_{\mathfrak{S}}$-filters on the underlying algebra of the secrecy structure.

Definition 5.4. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure. A **secrecy filter** or an **$\mathfrak{S}$-filter on** $\mathcal{A}$ is a safe set $F \subseteq A$, such that, for every $\Gamma \cup \{\phi\} \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$, with $\Gamma \vdash_{\mathfrak{S}} \phi$, and every secrecy interpretation $h : \mathfrak{S} \to \mathcal{A}$,

$$h(\Gamma) \subseteq F \quad \text{implies} \quad h(\phi) \in F.$$

We denote by $\mathrm{Fi}_{\mathfrak{S}}(\mathcal{A})$ the collection of all $\mathfrak{S}$-filters on $\mathcal{A}$ and by $\mathrm{Fi}^{\top}_{\mathfrak{S}}(\mathcal{A})$ the same collection augmented by A.

Note that, although, in general, A is not a safe set, it does satisfy the extra condition for being an $\mathfrak{S}$-filter on $\mathcal{A}$. Safe matrices and secrecy matrices are pairs consisting of a secrecy structure together with a safe set and a secrecy filter, respectively:

Definition 5.5. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure. A **safe matrix on** $\mathcal{A}$ is a pair $\mathfrak{A} = \langle \mathcal{A}, F \rangle$, where F is a safe set of $\mathcal{A}$.

If, in addition, $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ is an $\mathcal{S}$-secrecy logic, a safe matrix $\mathfrak{A} = \langle \mathcal{A}, F \rangle$ on $\mathcal{A}$ is said to be a **secrecy matrix** or an **$\mathfrak{S}$-matrix** if F is an $\mathfrak{S}$-filter on $\mathcal{A}$.

Given two secrecy matrices $\langle \mathcal{A}, F \rangle$ and $\langle \mathcal{B}, G \rangle$, a **secrecy matrix homomorphism** $h : \langle \mathcal{A}, F \rangle \to \langle \mathcal{B}, G \rangle$ is a secrecy homomorphism $h : \mathcal{A} \to \mathcal{B}$, such that $h(F) \subseteq G$. It is said to be a **strict secrecy matrix homomorphism** if $h : \mathcal{A} \to \mathcal{B}$ is strict and, in addition, $F = h^{-1}(G)$.

Given an $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, we call a congruence θ on $\mathbf{A}$ a **safe congruence** or a **secrecy congruence** if it is compatible with each of $K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}$.

Recall that, given an algebra homomorphism $h : \mathbf{A} \to \mathbf{B}$, its kernel $\mathrm{Ker}(h)$ is the set of all pairs $\langle a, b \rangle \in A^2$, such that $h(a) = h(b)$. In the following lemma, it is shown that the kernel of a strict matrix homomorphism is a safe congruence on the domain that is compatible with the secrecy filter of the matrix.

Lemma 5.6. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ be an $\mathcal{S}$-secrecy logic. Let, also $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, $\mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ be two $\mathcal{S}$-secrecy structures and F, G two $\mathfrak{S}$-filters on $\mathcal{A}$ and $\mathcal{B}$, respectively. If $h : \langle \mathcal{A}, F \rangle \to \langle \mathcal{B}, G \rangle$ is a strict matrix homomorphism, then* $\mathrm{Ker}(h)$ *is a safe congruence on $\mathcal{A}$ that is compatible with F.*

Proof. It is clear, since $h : \mathbf{A} \to \mathbf{B}$ is an algebra homomorphism, that $\mathrm{Ker}(h)$ is a congruence on $\mathbf{A}$. We must show that it is compatible with $K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}$ and F. All these may be shown similarly, whence we only show in detail compatibility with $K_{\mathcal{A}}$. If $\langle a_1, a_2 \rangle \in \mathrm{Ker}(h)$ and $a_1 \in K_{\mathcal{A}}$, then $h(a_2) = h(a_1) \in K_{\mathcal{B}}$, whence $a_2 \in h^{-1}(K_{\mathcal{B}}) = K_{\mathcal{A}}$. Thus, $\mathrm{Ker}(h)$ is compatible with $K_{\mathcal{A}}$. □

It may be shown, exactly as in the case of $\mathcal{S}$-secrecy logics, that given an $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, there exists a largest safe congruence on $\mathbf{A}$. It will be denoted by $\Omega(\mathcal{A})$ and called the **Leibniz congruence of** $\mathcal{A}$. Moreover, given a safe matrix $\mathfrak{A} = \langle \mathcal{A}, F \rangle$ on $\mathcal{A}$, there exists a largest safe congruence on $\mathcal{A}$ that is compatible with F. It will be called the **Leibniz congruence associated with** F and denoted by $\Omega_{\mathcal{A}}(F)$. It is clear that $\Omega_{\mathcal{A}}$ is an operator from the collection of safe matrices on $\mathcal{A}$ to the collection of safe congruences on $\mathcal{A}$.

The following lemma establishes an analog of a well-known result from the theory of deductive systems and logical matrices. It is well-known that the inverse image of a logical filter on an algebra under a homomorphism from the algebra of formulas into the algebra is a theory of the logic. The same holds for secrecy logics and secrecy structures as long as one restricts to secrecy interpretations rather than arbitrary homomorphisms.

Lemma 5.7. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure. For every $\mathfrak{S}$-filter F on $\mathcal{A}$ and every $\mathfrak{S}$-interpretation $h : \mathfrak{S} \to \mathcal{A}$, $h^{-1}(F)$ is an $\mathfrak{S}$-theory.*

Proof. Suppose that $h^{-1}(F) \vdash_{\mathfrak{S}} \phi$, for some $\phi \in \mathrm{Fm}_{\mathcal{L}}(V)$. Then, since F is an $\mathfrak{S}$-filter, h is an $\mathfrak{S}$-interpretation and $h(h^{-1}(F)) \subseteq F$, we must have $h(\phi) \in F$, i.e., $\phi \in h^{-1}(F)$. This shows that $h^{-1}(F) \in \mathrm{STh}^{\top}\mathcal{S}$. □

Another result that carries over to the secrecy setting from the theory of abstract algebraic logic, provided, once more, that we restrict attention to secrecy interpretations, is the one asserting the commutativity of the Leibniz operator with inverse strict surjective homomorphisms.

Lemma 5.8. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure. For every $\mathfrak{S}$-filter F on $\mathcal{A}$ and every surjective strict $\mathfrak{S}$-interpretation $h : \mathfrak{S} \to \mathcal{A}$, $h^{-1}(\Omega_{\mathcal{A}}(F)) = \Omega_{\mathfrak{S}}(h^{-1}(F))$.*

Proof. First, note that, by Lemma 5.7, the set $h^{-1}(F)$ is an $\mathfrak{S}$-theory, whence it makes sense to compute the quantity $\Omega_{\mathfrak{S}}(h^{-1}(F))$. To see that $h^{-1}(\Omega_{\mathcal{A}}(F)) \subseteq \Omega_{\mathfrak{S}}(h^{-1}(F))$, it suffices to show that $h^{-1}(\Omega_{\mathcal{A}}(F))$ is a congruence compatible with $h^{-1}(F)$. That it is a congruence on $\mathbf{Fm}_{\mathcal{L}}(V)$ (given that $\Omega_{\mathcal{A}}(F)$ is a congruence on $\mathbf{A}$) is well-known from universal algebra. If $\langle \phi, \psi \rangle \in h^{-1}(\Omega_{\mathcal{A}}(F))$ and $\phi \in h^{-1}(F)$, then $\langle h(\phi), h(\psi) \rangle \in \Omega_{\mathcal{A}}(F)$ and $h(\phi) \in F$, whence, by compatibility, $h(\psi) \in F$, showing that $\psi \in h^{-1}(F)$. Thus, $h^{-1}(\Omega_{\mathcal{A}}(F))$ is compatible with $h^{-1}(F)$. This shows that $h^{-1}(\Omega_{\mathcal{A}}(F)) \subseteq \Omega_{\mathfrak{S}}(h^{-1}(F))$.

For the reverse inclusion, assume that $\phi, \psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, such that $\langle \phi, \psi \rangle \in \Omega_{\mathfrak{S}}(h^{-1}(F))$. Let $G \in \{K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}, F\}$, $\delta(x, \vec{y}) \in \mathrm{Fm}_{\mathcal{L}}(V)$ and $\vec{\chi}' \in A^{|\vec{y}|}$. Then, we have

$$\begin{array}{rll}
\delta(h(\phi), \vec{\chi}') \in F & \text{iff} & \delta(h(\phi), h^{|\vec{y}|}(\vec{\chi})) \in F, \text{ for some } \vec{\chi} \in \mathrm{Fm}_{\mathcal{L}}(V)^{|\vec{y}|} \\
 & \text{iff} & h(\delta(\phi, \vec{\chi})) \in F \\
 & \text{iff} & \delta(\phi, \vec{\chi}) \in h^{-1}(F) \\
 & \text{iff} & \delta(\psi, \vec{\chi}) \in h^{-1}(F) \\
 & \text{iff} & h(\delta(\psi, \vec{\chi})) \in F \\
 & \text{iff} & \delta(h(\psi), h^{|\vec{y}|}(\vec{\chi})) \in F \\
 & \text{iff} & \delta(h(\phi), \vec{\chi}') \in F,
\end{array}$$

whence $\langle h(\phi), h(\psi)\rangle \in \Omega(\mathcal{A}) \cap \Omega_{\mathbf{A}}(F) = \Omega_{\mathcal{A}}(F)$. Thus, $h(\Omega_{\mathfrak{S}}(h^{-1}(F))) \subseteq \Omega_{\mathcal{A}}(F)$, showing that $\Omega_{\mathfrak{S}}(h^{-1}(F)) \subseteq h^{-1}(\Omega_{\mathcal{A}}(F))$. □

Finally, the following is an analog (only partial, since it does not include all secrecy structures) of a well-known transfer property, that holds for protoalgebraic deductive systems, stating that a deductive system $\mathcal{S}$ is protoalgebraic if and only if the Leibniz operator on every algebra $\mathbf{A}$ is monotone on the lattice of all $\mathcal{S}$-filters on $\mathbf{A}$.

Theorem 5.9. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}}\rangle$ be a deductive system and let $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S\rangle$ be an $\mathcal{S}$-secrecy logic. Then $\mathfrak{S}$ is protoalgebraic iff, for every $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle$, for which there exists at least one strict surjective secrecy homomorphism $h : \mathfrak{S} \to \mathcal{A}$, $\Omega_{\mathcal{A}}$ is monotone on* $\mathrm{Fi}^{\top}_{\mathfrak{S}}\mathcal{A}$.

Proof. Suppose that $\mathfrak{S}$ is protoalgebraic. Let $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle$ be an $\mathcal{S}$-secrecy structure, such that, there exists a strict surjective secrecy homomorphism $h : \mathfrak{S} \to \mathcal{A}$, and $F, G \in \mathrm{Fi}^{\top}_{\mathfrak{S}}\mathcal{A}$, with $F \subseteq G$. Then, by Lemma 5.7, $h^{-1}(F), h^{-1}(G) \in \mathrm{STh}^{\top}\mathcal{S}$, such that $h^{-1}(F) \subseteq h^{-1}(G)$. Thus, by protoalgebraicity and Theorem 3.6, $\Omega_{\mathfrak{S}}(h^{-1}(F)) \subseteq \Omega_{\mathfrak{S}}(h^{-1}(G))$, whence, by Lemma 5.8, $h^{-1}(\Omega_{\mathcal{A}}(F)) \subseteq h^{-1}(\Omega_{\mathcal{A}}(G))$. Therefore, since h is surjective, we get that $\Omega_{\mathcal{A}}(F) \subseteq \Omega_{\mathcal{A}}(G)$. Note the crucial role that the existence of the strict surjective secrecy homomorphism h played in this part of the proof.

If, conversely, for every $\mathcal{S}$-secrecy structure $\mathcal{A}$, for which there exists a strict surjective secrecy homomorphism $h : \mathfrak{S} \to \mathcal{A}$, $\Omega_{\mathcal{A}}$ is monotone on $\mathrm{Fi}^{\top}_{\mathfrak{S}}\mathcal{A}$, then, in particular, for the $\mathcal{S}$-secrecy logic $\mathfrak{S}$, viewed as an $\mathcal{S}$-secrecy structure, we have that $\Omega_{\mathfrak{S}}$ is monotone on $\mathrm{STh}^{\top}\mathcal{S}$, showing that $\mathfrak{S}$ is protoalgebraic. □

In the sequel, the class of all $\mathcal{S}$-secrecy structures $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle$, for which there exists at least one strict surjective secrecy homomorphism $h : \mathfrak{S} \to \mathcal{A}$ will be denoted by $\mathbf{H}_{SS}(\mathfrak{S})$. This is the class of those structures for which, by Theorem 5.9 one may guarantee monotonicity of $\Omega_{\mathcal{A}}$ on $\mathrm{Fi}^{\top}_{\mathfrak{S}}\mathcal{A}$ provided that $\mathfrak{S}$ is protoalgebraic. The notation $\mathbf{H}_{SS}$ is suggested by "**H**omomorphic images under $\underline{\text{S}}$rict surjective $\underline{\text{S}}$ecrecy homomorphisms".

6. The Correspondence Property

In this final section of the paper, we present an analog of the well-known correspondence property as a means of providing yet another characterization of protoalgebraicity of secrecy logics. Recall that, a given deductive system $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ has the correspondence property if, for every strict homomorphism $h : \langle \mathbf{A}, F \rangle \to \langle \mathbf{B}, G \rangle$ between two $\mathcal{S}$-matrices and every $\mathcal{S}$-filter H of $\langle \mathbf{A}, F \rangle$, i.e., such that $F \subseteq H$, it holds that $H = h^{-1}(h(H))$. (See Definition 1.1.7 of [12].) In Theorem 1.1.8 of [12], it is shown that a deductive system is protoalgebraic if and only if it has the correspondence property (see also [8]). In Definition 6.1, an analog of the correspondence property, suitable for secrecy logics, is introduced and the section concludes with Theorem 6.5, where it is shown that protoalgebraicity of secrecy logics is equivalent to having this modified notion of the correspondence property.

Definition 6.1. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic. Consider the collection $\mathbf{Mod}\mathfrak{S} = \{\langle \mathcal{A}, F \rangle : \mathcal{A} \in \mathbf{H}_{SS}(\mathfrak{S}) \text{ and } F \in \mathrm{Fi}_{\mathfrak{S}}\mathcal{A}\}$. The $\mathcal{S}$-secrecy logic $\mathfrak{S}$ has the **correspondence property** if, for all $\langle \mathcal{A}, F \rangle, \langle \mathcal{B}, G \rangle \in \mathbf{Mod}\mathfrak{S}$, every strict secrecy homomorphism $h : \langle \mathcal{A}, F \rangle \to \langle \mathcal{B}, G \rangle$ and all $\mathfrak{S}$-filters F' on $\mathcal{A}$, with $F \subseteq F'$, it holds that $F' = h^{-1}(h(F'))$. The collection of all $\mathfrak{S}$-filters F' on $\mathcal{A}$, such that $F \subseteq F'$ will be denoted by $\mathrm{Fi}_{\mathfrak{S}}\langle \mathcal{A}, F \rangle$.

Our goal in this section is to relate protoalgebraicity of a secrecy logic with the correspondence property. We start by proving that monotonicity of the secrecy Leibniz operator on all secrecy structures in $\mathbf{H}_{SS}\mathfrak{S}$ implies that $\mathfrak{S}$ has the correspondence property.

Lemma 6.2. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$ an $\mathcal{S}$-secrecy logic. Suppose that, for every $\mathcal{S}$-secrecy structure $\mathcal{A} \in \mathbf{H}_{SS}\mathfrak{S}$, $\Omega_{\mathcal{A}}$ is monotone on $\mathrm{Fi}^{\top}_{\mathfrak{S}}\mathcal{A}$. Then $\mathfrak{S}$ has the correspondence property.*

Proof. Let $\langle \mathcal{A}, F \rangle, \langle \mathcal{B}, G \rangle$ be $\mathfrak{S}$-secrecy matrices in $\mathbf{Mod}\mathfrak{S}$, $h : \langle \mathcal{A}, F \rangle \to \langle \mathcal{B}, G \rangle$ a strict $\mathfrak{S}$-matrix homomorphism and $F' \in \mathrm{Fi}_{\mathfrak{S}}\langle \mathcal{A}, F \rangle$. It is obvious that $F' \subseteq h^{-1}(h(F'))$. To see that the reverse inclusion also holds, assume that $a \in h^{-1}(h(F'))$. Then, $h(a) \in h(F')$, whence, there exists $a' \in F'$, such that $h(a) = h(a')$. This shows that $\langle a, a' \rangle \in \mathrm{Ker}(h)$, which, by Lemma 5.6 is a safe congruence on $\mathcal{A}$ compatible with F. Thus, using the hypothesis, we conclude that $\langle a, a'\rangle \in \Omega_{\mathcal{A}}(F) \subseteq \Omega_{\mathcal{A}}(F')$. Therefore, by compatibility, since $a' \in F'$, we get that $a \in F'$. □

The next step involves showing that the correspondence property induces an isomorphism between the partially ordered sets of filters of any two secrecy matrices in $\mathbf{Mod}\mathfrak{S}$ related by a strict surjective matrix homomorphism.

Lemma 6.3. *Let* $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}}\rangle$ *be a deductive system and* $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S\rangle$ *an* $\mathcal{S}$*-secrecy logic. If* $\mathfrak{S}$ *has the correspondence property, then, for all* $\langle \mathcal{A}, F\rangle, \langle \mathcal{B}, G\rangle \in \mathbf{Mod}\mathfrak{S}$ *and every surjective strict* $\mathfrak{S}$*-matrix homomorphism* $h : \langle \mathcal{A}, F\rangle \to \langle \mathcal{B}, G\rangle$*, the mapping* $\mathbf{h}$*, defined by* $F' \mapsto h(F')$ *is an isomorphism between* $\mathrm{Fi}_{\mathfrak{S}}(\langle \mathcal{A}, F\rangle)$ *and* $\mathrm{Fi}_{\mathfrak{S}}(\langle \mathcal{B}, G\rangle)$*.*

Proof. It is easy to see that, since $F' = h^{-1}(h(F'))$ and F' is an $\mathfrak{S}$-filter on $\mathcal{A}$, $h(F')$ is an $\mathfrak{S}$-filter on $\mathcal{B}$. Thus, $\mathbf{h} : \mathrm{Fi}_{\mathfrak{S}}\langle \mathcal{A}, F\rangle \to \mathrm{Fi}_{\mathfrak{S}}\langle \mathcal{B}, G\rangle$ is well defined. It is also a bijection. If $\mathbf{h}(F') = \mathbf{h}(F'')$, then $h^{-1}(h(F')) = h^{-1}(h(F''))$, which gives $F' = F''$, showing that $\mathbf{h}$ is injective. If $G' \in \mathrm{Fi}_{\mathfrak{S}}\langle \mathcal{B}, G\rangle$, then $h^{-1}(G') \in \mathrm{Fi}_{\mathfrak{S}}\langle \mathcal{A}, F\rangle$ and $h(h^{-1}(G')) = G'$ because h is surjective. Thus $\mathbf{h}$ is also surjective. Finally, it is trivially inclusion-preserving and, if $\mathbf{h}(F') \subseteq \mathbf{h}(F'')$, then $h^{-1}(h(F')) \subseteq h^{-1}(h(F''))$, showing that $F' \subseteq F''$. □

Finally, to complete the cycle, we show that, if, for all $\langle \mathcal{A}, F\rangle, \langle \mathcal{B}, G\rangle \in \mathbf{Mod}\mathfrak{S}$ and every surjective strict $\mathfrak{S}$-matrix homomorphism $h : \langle \mathcal{A}, F\rangle \to \langle \mathcal{B}, G\rangle$, $\mathbf{h}$, as defined in Lemma 6.3, is an isomorphism, then the secrecy logic $\mathfrak{S}$ is protoalgebraic.

Lemma 6.4. *Let* $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}}\rangle$ *be a deductive system and* $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S\rangle$ *an* $\mathcal{S}$*-secrecy logic. If, for all* $\langle \mathcal{A}, F\rangle, \langle \mathcal{B}, G\rangle \in \mathbf{Mod}\mathfrak{S}$ *and every surjective strict* $\mathfrak{S}$*-matrix homomorphism* $h : \langle \mathcal{A}, F\rangle \to \langle \mathcal{B}, G\rangle$*, the mapping* $\mathbf{h} : F' \mapsto h(F')$ *is an isomorphism between* $\mathrm{Fi}_{\mathfrak{S}}(\langle \mathcal{A}, F\rangle)$ *and* $\mathrm{Fi}_{\mathfrak{S}}(\langle \mathcal{B}, G\rangle)$*, then* $\mathfrak{S}$ *is protoalgebraic.*

Proof. Assume that $T, T' \in \mathrm{STh}^{\top}\mathcal{S}$, such that $T \subseteq T'$. Then

$$h : \langle \mathfrak{S}, T\rangle \to \langle \mathfrak{S}/\Omega_{\mathfrak{S}}(T), T/\Omega_{\mathfrak{S}}(T)\rangle$$

is a strict surjective homomorphism, whence, since $T' \in \mathrm{Fi}_{\mathfrak{S}}\langle \mathfrak{S}, T\rangle$, we get that $\mathbf{h}(T') \in \mathrm{Fi}_{\mathfrak{S}}\langle \mathfrak{S}/\Omega_{\mathfrak{S}}(T), T/\Omega_{\mathfrak{S}}(T)\rangle$, and, therefore, that $h^{-1}(h(T')) \in$

$\mathrm{Fi}_{\mathfrak{S}}\langle\mathfrak{S},T\rangle$. Since h is surjective, $h(T') = h(h^{-1}(h(T')))$, whence $T' = h^{-1}(h(T'))$. This shows that $\Omega_{\mathfrak{S}}(T)$ is compatible with T'. Thus $\Omega_{\mathfrak{S}}(T) \subseteq \Omega_{\mathfrak{S}}(T')$. Therefore, by Theorem 3.6, $\mathfrak{S}$ is protoalgebraic. □

If Lemmas 6.2, 6.3 and 6.4 are put together, the following characterization of protoalgebraicity of an $\mathcal{S}$-secrecy logic can be obtained.

Theorem 6.5. *Let $\mathcal{S} = \langle\mathcal{L},\vdash_{\mathcal{S}}\rangle$ be a deductive system and let $\mathfrak{S} = \langle\mathbf{Fm}_{\mathcal{L}}(V), K, B, S\rangle$ be an $\mathcal{S}$-secrecy logic. Then, the following are equivalent:*

(i) *$\mathfrak{S}$ is protoalgebraic;*

(ii) *For all $\mathcal{A} \in \mathbf{H}_{SS}\mathfrak{S}$, $\Omega_{\mathcal{A}}$ is monotone on $\mathrm{Fi}_{\mathfrak{S}}\mathcal{A}$;*

(iii) *$\mathfrak{S}$ has the correspondence property;*

(iv) *For every $\langle\mathcal{A},F\rangle, \langle\mathcal{B},G\rangle \in \mathbf{Mod}\mathfrak{S}$ and every surjective strict $\mathfrak{S}$-matrix homomorphism $h : \langle\mathcal{A},F\rangle \to \langle\mathcal{B},G\rangle$, the mapping $\mathbf{h} : F' \mapsto h(F')$ is an isomorphism between $\mathrm{Fi}_{\mathfrak{S}}(\langle\mathcal{A},F\rangle)$ and $\mathrm{Fi}_{\mathfrak{S}}(\langle\mathcal{B},G\rangle)$.*

Proof. *(i)* ⇒ *(ii)* is given by Theorem 5.9. *(ii)* ⇒ *(iii)* is given by Lemma 6.2. *(iii)* ⇒ *(iv)* is given by Lemma 6.3. Finally, *(iv)* ⇒ *(i)* is given by Lemma 6.4.

□

We close the section by discussing a question that is open for further investigation. In [19], various constructions of universal algebraic and categorical character, including a detailed study of the formation of subdirect products, were carried out for the class of $\mathcal{S}$-secrecy structures endowed with secrecy homomorphisms between them. In Theorem 1.3.7 of [12] (see also [8]), on the other hand, Czelakowski proves that protoalgebraicity of a deductive system is equivalent with its class of reduced matrices being closed under subdirect products. Since the constructions of [19] could be transferred with some care to the context of $\mathfrak{S}$-matrices, it would be an interesting topic of investigation to find out whether it is possible to extend or modify Theorem 1.3.7 of Czelakowski to the setting of $\mathcal{S}$-secrecy logics to provide another characterization of the notion of protoalgebraic $\mathcal{S}$-secrecy logic.

References

[1] J. Bao, G. Slutzki, and V. Honavar, Privacy-Preserving Reasoniong on the Semantic Web, Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence 2007, pp. 791–797.

[2] J. Biskup, *For Unknown Secrecies Refusal is Better Than Lying*, Data and Knowledge Engineering **33** (2000), pp. 1–23.

[3] J. Biskup and P.A. Bonatti, *Lying Versus Refusal for Known Potential Secrets*, Data and Knowledge Engineering **38** (2001), pp. 199–222.

[4] J. Biskup and P.A. Bonatti, *Controlled Query Evaluation for Known Policies by Combining Lying and Refusal*, Annals of Mathematics and Artificial Intelligence **40** (2004), pp. 37–62.

[5] J. Biskup and P. Bonatti, *Controlled Query Evaluation for Enforcing Confidentiality in Complete Information Systems*, International Journal of Information Security **3** (2004), pp. 14–27.

[6] W.J. Blok and D. Pigozzi, *Protoalgebraic Logics*, Studia Logica **45** (1986), pp. 337–369.

[7] W.J. Blok and D. Pigozzi, Algebraizable Logics, Memoirs of the American Mathematical Society **77**, No. 396 (1989).

[8] W.J. Blok and D. Pigozzi, *Algebraic Semantics for Universal Horn Logic Without Equality*, in: Universal Algebra and Quasigroup Theory, A. Romanowska and J.D.H. Smith, Eds., Heldermann Verlag, Berlin 1992

[9] P.A. Bonatti, S. Kraus, and V.S. Subrahmanian, *Foundations of Secure Deductive Databases*, IEEE Transactions of Knowledge and Data Engineering **7**:3 (1995), pp. 406–422.

[10] D. Calvanese, G. De Giacomo, M. Lenzerini, and R. Rosati, *View-Based Query Answering over Description Logic Ontologies*, Proceedings of the 11th International Conference of Knowledge Representation and Reasoning, KR 2008, pp. 242–251.

[11] B. Cuenca Grau and I. Horrocks, *Privacy-Preserving Query Answering in Logic-Based Information Systems*, 18th European Conference on Artificial Intelligence, ECAI 2008, pp. 40–44.

[12] J. Czelakowski, Protoalgebraic Logics, Trends in Logic-Studia Logica Library 10, Kluwer, Dordrecht, 2001.

[13] J.M. Font and R. Jansana, *A General Algebraic Semantics for Sentential Logics*, Lecture Notes in Logic **332**: 7 (1996), Springer-Verlag, Berlin Heidelberg, 1996

[14] J.M. Font, R. Jansana, and D. Pigozzi, *A Survey of Abstract Algebraic Logic*, Studia Logica **74**:1/2 (2003), pp. 13–97.

[15] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M.W. Mislove, and D.S. Scott, Continuous Lattices and Domains, Cambridge University Press, Cambridge, 2003.

[16] G.L. Sicherman, W. de Jonge, and R.P. van de Riet, *Answering Queries Without Revealing Secrets*, ACM Transactions on Database Systems **8**:1 (1983), pp. 41–59.

[17] P. Stouppa and T. Studer, *A Formal Model of Data Privacy*, 6th International Andrei Ershov Memorial Conference, Perspectives of Systems Informatics, PSI 2006, pp. 400–408.

[18] P. Stouppa and T. Studer, *Data Privacy for ALC Knowledge Bases*, Logical Foundations of Computer Science, LFCS 2009, pp. 409–421.

[19] G. Voutsadakis, *Secrecy Logic: $\mathcal{S}$-Secrecy Structures*, Turkish Journal of Mathematics **35**:1 (2011), pp. 1–28.

Department of Computer Science, Iowa State University,
Ames, IA 50011, U.S.A.,
and
School of Mathematics and Computer Science,
Lake Superior State University,
Sault Sainte Marie, MI 49783, U.S.A.,
gvoutsad@lssu.edu