Deciding knowledge in security protocols for monoidal equational theories *

Véronique Cortier and Stéphanie Delaune

LORIA, CNRS & INRIA project Cassis, Nancy, France

Abstract. In formal approaches, messages sent over a network are usually modeled by terms together with an equational theory, axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). The analysis of cryptographic protocols requires a precise understanding of the attacker knowledge. Two standard notions are usually used: deducibility and indistinguishability. Only few results have been obtained (in an ad-hoc way) for equational theories with associative and commutative properties, especially in the case of static equivalence. The main contribution of this paper is to propose a general setting for solving deducibility and indistinguishability for an important class (called *monoidal*) of these theories. Our setting relies on the correspondence between a monoidal theory E and a semiring $\mathcal{S}_\mathsf{E}$ which allows us to give an algebraic characterization of the deducibility and indistinguishability problems. As a consequence we recover easily existing decidability results and obtain several new ones.

1 Introduction

Security protocols are paramount in today's secure transactions through public channels. It is therefore essential to obtain as much confidence as possible in their correctness. Formal methods have proved their usefulness for precisely analyzing the security of protocols. Understanding security protocols often requires reasoning about knowledge of the attacker. In formal approaches, two main kind of definitions have been given in the literature for this knowledge. They are known as message deducibility and indistinguishability relations.

Most often, the knowledge of the attacker is described in terms of message deducibility [13, 16, 14]. Given some set of messages ϕ representing the knowledge of the attacker and another message M, intuitively the secret, one can ask whether an attacker is able to compute M from ϕ. To obtain such a message he uses his deduction capabilities. For instance, he may encrypt and decrypt using keys that he knows.

* This work has been partly supported by the RNTL project POSÉ and the ARA SSIA Formacrypt

This concept of deducibility does not always suffice for expressing the knowledge of an attacker. For example, if we consider a protocol that transmits an encrypted Boolean value (e.g. the value of a vote), we may ask whether an attacker can learn this value by eavesdropping the protocol. Of course, it seems to be completely unrealistic to say that the Boolean true and false are not deducible. We need to express the fact that the two transcripts of the protocol, one running with the Boolean value true and the other one with false are *indistinguishable*.

In both cases, deduction and indistinguishability apply to observations on messages at a particular point in time. They do not take into account the dynamic behavior of the protocol. For this reason the indistinguishability relation is called *static equivalence*. Nevertheless those relations are quite useful to reason about the dynamic behavior of a protocol. For instance, the deducibility relation is often used as a subroutine of many decision procedures [17, 7, 8]. In the applied-pi calculus framework [2], it has been shown that observational equivalence (relation which takes into account the dynamic behavior) coincides with labeled bisimulation which corresponds to checking static equivalences and some standard bisimulation conditions.

Both of these relations rely on an underlying equational theory axiomatizing the properties of the cryptographic functions (encryption, exclusive or, ...). Many decision procedures have been provided to decide these relations under a variety of equational theories. For instance algorithms for deduction are provided for exclusive or [8], homomorphic operators [9] and subterm theories [1]. These theories allow basic equations for functions such as encryption, decryption and digital signature. There are also results for static equivalence. For instance, a general decidability result for the class of subterm convergent equational theories is given in [1]. This class contains classical cryptographic primitives like encryption, signatures and hashes. Also in [1] some abstract conditions on the underlying equational theory are proposed to ensure decidability of deduction and static equivalence. Note that the use of this result requires checking some assumptions, which might be difficult to prove. Regarding theories with associative and commutative properties (AC), they only obtain decidability for pure AC and exclusive or. A weakness of most of these approaches is their lack of generality since each new theory requires a new proof. Homomorphic properties occur in many protocols, alone or in combination with other operators, and cannot be dealt with by a simple adaptation of the techniques that have been developed so far.

In this paper, we consider the axioms of Associativity-Commutativity (AC), Unit element (U), Nilpotency (N), Idempotency (I), homomorphism (h), and more especially the combinations of these axioms that constitute monoidal theories. We propose a general approach to handle *monoidal* theories that covers several cases already studied, and furthermore includes some new decidability and complexity results on homomorphic operators. Monoidal theories have been extensively studied by F. Baader and W. Nutt [15, 4, 5] who have provided a complete survey of unification in these theories. More recently, these theories have been studied in the context of security protocols. S. Delaune *et al.* have shown that deduction is decidable for a subclass of monoidal equational theories, also considering active attacks [10]. However, they do not address static equivalence.

Studying monoidal theories might seem very restricted since they do not contain the equational theories for classical operators like encryption or signatures. However, it has been shown in [3] that equational theories can easily be combined for both deduction and static equivalence, provided the signatures are disjoint. That is why it is sufficient to focus on the important case of monoidal theories. As a consequence of our general approach, we recover many existing results and we obtain several new ones (10 new decidability or complexity results) for static equivalence or deduction.

Outline of the paper. In Section 2 we recall some basic notation and the central notion of monoidal theory. Then, in Section 3, we define the two notions of knowledge we are interested in. In Section 4 we show how to represent terms and substitutions by means of vectors and matrices over semirings. Then Sections 5 and 6 are devoted to the study of deduction and static equivalence respectively. In Section 7, we sum up our results and provide new results obtained as a consequence of our main theorems.

2 Preliminaries

2.1 Terms

A *signature* Σ consists of a finite set of function symbols, each with an arity. A function symbol with arity 0 is a constant symbol. We assume given a signature Σ, an infinite set of names $\mathcal{N}$, and an infinite set of variables $\mathcal{X}$. Let $\mathcal{M}$ be a set of names and variables, we denote by $\mathcal{T}(\Sigma, \mathcal{M})$ the set of *terms* over $\Sigma \cup \mathcal{M}$. $\mathcal{T}(\Sigma, \mathcal{N})$ is called the set of *ground* terms while $\mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$ is simply called the set of terms. We write $fn(M)$ (resp. $fv(M)$) for the set of names (resp. variables) that occur in the term M. A *substitution* σ is a mapping from a finite subset of $\mathcal{X}$ called its domain and written $dom(\sigma)$ to $\mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$. Substitutions are extended to endomorphisms of $\mathcal{T}(\Sigma, \mathcal{X})$ as usual. We use a postfix notation for their application. Given two terms u and v, the *replacement* of u by v, denoted by $[u \mapsto v]$, maps every term t to the term $t[u \mapsto v]$ which is obtained by replacing all occurrences of u in t by v.

2.2 Monoidal theories

Equational theories are very useful for modeling the algebraic properties of the cryptographic primitives. Given a signature Σ, an equational theory E is a set of equations (*i.e.* a set of unordered pairs of terms in $\mathcal{T}(\Sigma, \mathcal{X})$). Given two terms M and N such that $M, N \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$, we write $M =_{\mathsf{E}} N$ if the equation $M = N$ is a consequence of E. In this paper, we are particularly interested in the class of monoidal theories introduced by W. Nutt [15]. It captures many theories with AC properties, which are known to be difficult to deal with.

Definition 1 (monoidal theory). *A theory* E *over* Σ *is called* monoidal *if it satisfies the following properties:*

1. *The signature* Σ *contains a binary function symbol* $+$ *and a constant symbol* 0*, and all other function symbols in* Σ *are unary.*
2. *The symbol* $+$ *is associative-commutative with unit* 0*,* i.e. *the equations* $x + (y + z) = (x + y) + z$*,* $x + y = y + x$ *and* $x + 0 = x$ *are in* E*.*
3. *Every unary function symbol* $\mathsf{h} \in \Sigma$ *is an endomorphism for* $+$ *and* 0*, i.e.* $\mathsf{h}(x + y) = \mathsf{h}(x) + \mathsf{h}(y)$ *and* $\mathsf{h}(0) = 0$*.*

Example 1. Suppose $+$ is a binary function symbol and 0 is nullary. Moreover assume that the others symbols, *i.e* $-$, h, are unary symbols. The equational theories below are monoidal.

- The theory ACU over $\Sigma = \{+, 0\}$ which consists of the axioms of associativity and commutativity with unit 0.
- The theories ACUI and ACUN (*exclusive or*) over $\Sigma = \{+, 0\}$ which consist of the axioms (AC) and (U) with in addition Idempotency (I) $x + x = x$, or Nilpotency (N) $\quad x + x = 0$.
- The theory AG (*Abelian groups*) over $\Sigma = \{+, -, 0\}$ which is generated by the axioms (AC), (U) and $x + -(x) = 0$ (Inv). Indeed, the equations $-(x + y) = -(x) + -(y)$ and $-0 = 0$ are consequences of the others.
- The theories ACUh, ACUIh, ACUNh over $\Sigma = \{+, \mathsf{h}, 0\}$ and AGh over $\Sigma = \{+, -, \mathsf{h}, 0\}$: these theories correspond to the ones described

above extended by the homomorphism laws (h) for the symbol h, *i.e.* $\mathsf{h}(x+y) = \mathsf{h}(x) + \mathsf{h}(y)$ and $\mathsf{h}(0) = 0$ (if it is not a consequence of the others equations).

Note that there are two homomorphisms in the theory AGh, namely $-$ and h. These two homomorphisms commute: $\mathsf{h}(-x) = -(\mathsf{h}(x))$ is a consequence of the others. Other examples of monoidal theories can be found in [15].

3 Deduction and static equivalence

We now describe our two notions of knowledge for an intruder.

3.1 Assembling terms into frames

At a particular point in time, while engaging in one or more sessions of one or more protocols, an attacker may know a sequence of messages $M_1, \ldots, M_\ell$. This means that he knows each message but he also knows in which order he obtained the messages. So it is not enough for us to say that the attacker knows the set of terms $\{M_1, \ldots, M_\ell\}$ since the information about the order is lost. Furthermore, we should distinguish those names that the attacker knows from those that were freshly generated by others and which are *a priori* secret from the attacker; both kinds of names may appear in the terms. In the applied pi calculus [2], such a sequence of messages is organized into a *frame* $\phi = \nu\tilde{n}.\sigma$, where $\tilde{n}$ is a finite set of *restricted* names (intuitively the fresh ones), and σ is a substitution of the form:

$$\{^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}\} \quad \text{with} \quad dom(\sigma) = \{x_1, \ldots, x_\ell\}.$$

The variables enable us to refer to each M_i and we always assume that the terms M_i are ground. The names $\tilde{n}$ are bound to ϕ and can be renamed. Moreover names that do not appear in ϕ can be added or removed from $\tilde{n}$. In particular, we can always assume that two frames share the same set of restricted names.

3.2 Deduction

Given a frame ϕ that represents the information available to an attacker, we may ask whether a given ground term M may be deduced from ϕ.

Given a theory E over Σ, this relation is written $\phi \vdash_{\mathsf{E}} M$ and is axiomatized by the rules:

$$\frac{}{\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M}\ \text{if } \exists x \in dom(\sigma) \text{ s.t. } x\sigma = M \qquad \frac{}{\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} s}\ s \in \mathcal{N} \smallsetminus \tilde{n}$$

$$\frac{\phi \vdash_{\mathsf{E}} M_1 \quad \dots \quad \phi \vdash_{\mathsf{E}} M_\ell}{\phi \vdash_{\mathsf{E}} f(M_1, \dots, M_\ell)}\ f \in \Sigma \qquad \frac{\phi \vdash_{\mathsf{E}} M}{\phi \vdash_{\mathsf{E}} M'}\ M =_{\mathsf{E}} M'$$

Intuitively, the deducible messages are the messages of ϕ and the names that are not protected in ϕ, closed by equality in E and closed by application of function symbols. Since the deducible messages depend on the underlying equational theory, we write $\vdash_{\mathsf{E}}$ and simply $\vdash$ when E is clear from the context. When $\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M$, any occurrence of names from $\tilde{n}$ in M is bound by $\nu\tilde{n}$. So $\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M$ could be formally written $\nu\tilde{n}.(\sigma \vdash_{\mathsf{E}} M)$. It is easy to prove by induction the following characterization of deduction.

Lemma 1 (characterization of deduction). *Let M be a ground term and $\nu\tilde{n}.\sigma$ be a frame. Then $\nu\tilde{n}.\sigma \vdash_{\mathsf{E}} M$ iff there exists $\zeta \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$ such that $fn(\zeta) \cap \tilde{n} = \emptyset$ and $\zeta\sigma =_{\mathsf{E}} M$. Such a term ζ is a* recipe *of the term M.*

Example 2. Consider $\Sigma = \{+, 0\}$ and the equational theory ACUN given in Example 1. Let $\phi = \nu n_1, n_2, n_3.\{^{n_1+n_2+n_3}/_{x_1}, {}^{n_1+n_2}/_{x_2}, {}^{n_2+n_3}/_{x_3}\}$. We have that $\phi \vdash n_2 + n_4$. Indeed the term $x_1 + x_2 + x_3 + n_4$ is a recipe of the term $n_2 + n_4$.

Deduction problem for the equational theory E built over Σ.
Entries: A frame ϕ and a term M (both built over Σ)
Question: $\phi \vdash_{\mathsf{E}} M$?

3.3 Static equivalence

Deduction does not always suffice for expressing the knowledge of an attacker. Sometimes, the attacker can deduce exactly the same set of terms from two different frames but he could still be able to tell the difference between these two frames. Static equivalence is particularly important when defining for example the confidentiality of a vote or anonymity-like properties.

Definition 2 (static equivalence). *Let ϕ be a frame and M,N be two terms. We say that M and N are* equal in ϕ *under the theory E, and* *write* $(M =_{\mathsf{E}} N)\phi$*, if there exists* $\tilde{n}$ *such that* $(fn(M) \cup fn(N)) \cap \tilde{n} = \emptyset$*,* $\phi = \nu\tilde{n}.\sigma$ *and* $M\sigma =_{\mathsf{E}} N\sigma$*. We say that two frames* $\phi_1 = \nu\tilde{n}.\sigma_1$ *and* $\phi_2 = \nu\tilde{n}.\sigma_2$ *are* statically equivalent *w.r.t.* E*, and write* $\phi_1 \approx_{\mathsf{E}} \phi_2$ *when* $dom(\phi_1) = dom(\phi_2)$*, and*

$$\forall M, N \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X}) \text{ we have that } (M =_{\mathsf{E}} N)\phi_1 \Leftrightarrow (M =_{\mathsf{E}} N)\phi_2.$$

Example 3. Consider the equational theory ACU given in Example 1 and let $\phi = \nu n_1, n_2, n_3.\{^{3n_1+2n_2+3n_3}/_{x_1}, {}^{n_2+3n_3}/_{x_2}, {}^{3n_2+n_3}/_{x_3}, {}^{3n_1+n_2+4n_3}/_{x_4}\}$ where the notation kn with $k \in \mathbb{N}$ denotes $n + \cdots + n$ (k times). Let $M = 2x_1 + x_2$ and $N = x_3 + 2x_4$. We have that $(M =_{\mathsf{E}} N)\phi$.

Static equivalence problem for the theory E built over Σ.
Entries: Two frames ϕ_1 and ϕ_2 (both built over Σ)
Question: $\phi_1 \approx_{\mathsf{E}} \phi_2$?

In what follows, we consider decidability and complexity issues for deduction and static equivalence for monoidal theories.

4 Monoidal theories

It has been shown that the deduction problem for ACU amounts to solving linear equations over the semiring $\mathbb{N}$ whereas for AGh this problem amounts to solving linear equations over the ring $\mathbb{Z}[\mathsf{h}]$, the ring of polynomials in one indeterminate with coefficients over $\mathbb{Z}$ [9]. Some results of this kind also exist in the case of static equivalence. For instance, static equivalence has been shown decidable for the equational theories ACUN and AC [1]. By using an algebraic characterization of the problem, we will generalize these results by associating to every monoidal theory E a semiring $\mathcal{S}_{\mathsf{E}}$, that will be used to solve the deduction and the static equivalence problems in E.

4.1 Monoidal theories define semirings

Monoidal theories have an algebraic structure close to rings except that elements might not have an inverse. Such a structure is called *semiring*.

Definition 3 (semiring). *A* semiring *is a set* $\mathcal{S}$ *(called the* universe *of the semiring) with distinct elements* 0 *and* 1 *that is equipped with two binary operations* $+$ *and* $\cdot$ *such that* $(\mathcal{S}, +, 0)$ *is a commutative monoid,* $(\mathcal{S}, \cdot, 1)$ *is a monoid, and the following identities hold for all* $\alpha, \beta, \gamma \in \mathcal{S}$*:*

– $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$ *(right distributivity)*

- $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ *(left distributivity)*
- $0 \cdot \alpha = \alpha \cdot 0 = 0$ *(zero laws).*

We call the binary operations $+$ and $\cdot$ respectively the *addition* and the *multiplication* of the semiring. The elements 0 and 1 are called respectively *zero* and *unit*. In the sequel we will often omit the $\cdot$ sign and write $\alpha\beta$ instead of $\alpha \cdot \beta$. A semiring is *commutative* if its multiplication is commutative. Semirings are different from rings in that they need not be groups with respect to addition. Every ring is a semiring. In a ring, we will denote by $-\alpha$ the additive inverse of α, and we write $\alpha - \beta$ as an abbreviation of $\alpha + (-\beta)$.

It has been shown in [15] that for any monoidal theory E there exists a corresponding semiring $\mathcal{S}_{\mathsf{E}}$. We can rephrase the definition of $\mathcal{S}_{\mathsf{E}}$ as follows. Let $\mathbf{1}$ be a free constant ($\mathbf{1} \notin \Sigma$), the universe of $\mathcal{S}_{\mathsf{E}}$ is $\mathcal{T}(\Sigma, \{\mathbf{1}\})/\mathsf{E}$, that is the set of equivalence classes of terms built over Σ and $\mathbf{1}$ under equivalence by the equational axioms E. The constant 0 and the sum $+$ of the semiring are defined as in the algebra $\mathcal{T}(\Sigma, \{\mathbf{1}\})/\mathsf{E}$. The multiplication in the semiring is defined by $s \cdot t := s[\mathbf{1} \mapsto t]$. As a consequence, $\mathbf{1}$ acts as a neutral element of multiplication in $\mathcal{S}_{\mathsf{E}}$. This is the reason why we call this new generator $\mathbf{1}$ instead of, say, x, as it is often done in the literature. It can be shown [15] that $\mathcal{S}_{\mathsf{E}}$ is a ring if, and only if, E is a group theory, and also that $\mathcal{S}_{\mathsf{E}}$ is commutative if, and only if, E has commuting homomorphisms, *i.e.* $\mathsf{h}_1(\mathsf{h}_2(x)) =_{\mathsf{E}} \mathsf{h}_2(\mathsf{h}_1(x))$ for any two homomorphisms h_1 and h_2. For instance, we have that

1. The semiring $\mathcal{S}_{\mathsf{ACU}}$ is isomorphic to $\mathbb{N}$, the semiring of natural numbers.
2. The semiring $\mathcal{S}_{\mathsf{ACUN}}$ consists of the two elements 0 and $\mathbf{1}$ and we have $0 + \mathbf{1} = \mathbf{1} + 0 = \mathbf{1}$, $0 + 0 = \mathbf{1} + \mathbf{1} = 0$, $0 \cdot 0 = \mathbf{1} \cdot 0 = 0 \cdot \mathbf{1} = 0$, and $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$. Hence, $\mathcal{S}_{\mathsf{ACUN}}$ is isomorphic to the commutative ring (field) $\mathbb{Z}/2\mathbb{Z}$.
3. The semiring $\mathcal{S}_{\mathsf{AGh}}$ is isomorphic to $\mathbb{Z}[\mathsf{h}]$ which is a commutative ring.

Let b be a free symbol (name or variable). We denote by $\psi_b \colon \mathcal{T}(\Sigma, \{b\}) \to \mathcal{S}_{\mathsf{E}}$ the function which maps any term $M \in \mathcal{T}(\Sigma, \{b\})$ to $M[b \mapsto \mathbf{1}]$ considered as an element of the semiring $\mathcal{S}_{\mathsf{E}}$.

Example 4. Let $\mathsf{E} = \mathsf{ACUN}$ and $t = b+b+b$. We have $\psi_b(t) = \mathbf{1}+\mathbf{1}+\mathbf{1} = \mathbf{1}$.

4.2 Representation of terms and frames

A *base* $\mathcal{B}$ is a sequence $[b_1, \ldots, b_m]$ of free symbols (names or variables), We say that $\mathcal{B}$ is a *base of names* when $b_1, \ldots, b_m$ are names.

Definition 4 (decomposable in a base). *A term $M \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$ is* decomposable *in $\mathcal{B}$ if $fn(M) \cup fv(M) \subseteq \mathcal{B}$. Let $\phi = \nu\tilde{n}.\{^{M_1}/_{x_1}, \ldots, {}^{M_\ell}/_{x_\ell}\}$ be a frame. We say that ϕ is* decomposable *in $\mathcal{B}$ if each M_i is decomposable in $\mathcal{B}$.*

Let $\mathcal{B} = [b_1, \ldots, b_m]$. We generalize the construction of the previous section and obtain a function which assigns to any term in $\mathcal{T}(\Sigma, \mathcal{B})$ a tuple in $\mathcal{S}_{\mathsf{E}}^m$, that is a tuple of m elements over $\mathcal{S}_{\mathsf{E}}$. The function $\psi_{\mathcal{B}}$ of domain $\mathcal{T}(\Sigma, \{b_1, \ldots, b_m\})$ is defined as follows: Any term $M \in \mathcal{T}(\Sigma, \{b_1, \ldots, b_m\})$ has a unique decomposition $M_1, \ldots, M_m$ such that $M = M_1 + \ldots + M_m$ with $M_i \in \mathcal{T}(\Sigma, \{b_i\})$ [15]. Let $\psi_{\mathcal{B}}(M) = (\psi_{b_1}(M_1), \ldots, \psi_{b_m}(M_m)) \in \mathcal{S}_{\mathsf{E}}^m$. Given a vector $X \in \mathcal{S}_{\mathsf{E}}^m$ of size m, $\psi_{\mathcal{B}}^{-1}(X)$ is a term $M \in \mathcal{T}(\Sigma, \mathcal{B})$ such that $\psi_{\mathcal{B}}(M) = X$. This term is uniquely defined modulo E.

Example 5. Taking into account that the semiring $\mathcal{S}_{\mathsf{AGh}}$ is (isomorphic to) $\mathbb{Z}[\mathsf{h}]$, we have $\psi_{[b_1,b_2,b_3]}(b_1 + b_1 + \mathsf{h}(b_3) + \mathsf{h}(\mathsf{h}(\mathsf{h}(b_3)))) = (2, 0, \mathsf{h} + \mathsf{h}^3)$. Indeed, we have that $\psi_{b_1}(b_1 + b_1) = 2$, $\psi_{b_2}(0) = 0$ and $\psi_{b_3}(\mathsf{h}(b_3) + \mathsf{h}(\mathsf{h}(\mathsf{h}(b_3)))) = \mathsf{h} + \mathsf{h}^3$.

A term can be uniquely decomposed on a base $\mathcal{B}$. This can be extended to associate a (unique) matrix to a frame. Let $\phi = \nu\tilde{n}.\sigma$ be a frame and $\mathcal{B} = [b_1, \ldots, b_m]$ be a base of names in which ϕ is decomposable. Let $\sigma = \{^{M_1}/_{x_1} \ldots {}^{M_\ell}/_{x_\ell}\}$. We denote by $\psi_{\mathcal{B}}(\phi)$ the matrix of size $\ell \times m$ (ℓ rows and m columns) defined by $(\psi_{\mathcal{B}}(M_1); \ldots; \psi_{\mathcal{B}}(M_\ell))$. This matrix is the decomposition of ϕ in $\mathcal{B}$.

Example 6. Consider the frame ϕ given in Example 3 and consider the base $\mathcal{B} = [n_1, n_2, n_3]$. We have that

$$\psi_{\mathcal{B}}(\phi) = \begin{pmatrix} 3 & 2 & 3 \\ 0 & 1 & 3 \\ 0 & 3 & 1 \\ 3 & 1 & 4 \end{pmatrix} \quad \text{since} \quad \begin{array}{l} - \ \psi_{\mathcal{B}}(3n_1 + 2n_2 + 3n_3) = (3, 2, 3), \\ - \ \psi_{\mathcal{B}}(n_2 + 3n_3) = (0, 1, 3), \\ - \ \psi_{\mathcal{B}}(3n_2 + n_3) = (0, 3, 1), \text{ and} \\ - \ \psi_{\mathcal{B}}(3n_1 + n_2 + 4n_3) = (3, 1, 4). \end{array}$$

Applying a recipe to a frame is equivalent to multiplying the corresponding matrices.

Lemma 2. *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and ζ be a term in $\mathcal{T}(\Sigma, dom(\phi))$. Let $\mathcal{B}$ be a base of names in which we can decompose ϕ. We have that*

$$\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{dom(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi).$$

Proof. Let $\sigma = \{^{M_1}/_{x_1}, \ldots, ^{M_\ell}/_{x_\ell}\}$ and ζ be a term in $\mathcal{T}(\Sigma, dom(\phi))$. We have that $\zeta = \zeta_1 + \ldots + \zeta_\ell$ for some $\zeta_i \in \mathcal{T}(\Sigma, \{x_i\})$.

$$\begin{aligned}\psi_{\mathcal{B}}(\zeta\sigma) &= \psi_{\mathcal{B}}(\zeta_1\sigma + \ldots + \zeta_\ell\sigma)\\ &= \psi_{\mathcal{B}}(\zeta_1[x_1 \mapsto M_1] + \ldots + \zeta_\ell[x_\ell \mapsto M_\ell])\\ &= \psi_{\mathcal{B}}(\zeta_1[x_1 \mapsto M_1]) + \ldots + \psi_{\mathcal{B}}(\zeta_\ell[x_\ell \mapsto M_\ell])\\ &= \psi_{x_1}(\zeta_1) \cdot \psi_{\mathcal{B}}(M_1) + \ldots + \psi_{x_\ell}(\zeta_\ell) \cdot \psi_{\mathcal{B}}(M_\ell)\\ &= \psi_{dom(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi)\end{aligned}$$ $\square$

Note that to apply the equation stated in Lemma 2, the recipe ζ has to be built without names. To ensure that such kind of recipes always exist, we will work with frames saturated w.r.t. $\mathcal{B}$ (base of names in which the frames are decomposable).

Definition 5 (frame saturated w.r.t. $\mathcal{B}$). *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and $\mathcal{B}$ be a base of names $[b_1, \ldots, b_m]$ in which ϕ is decomposable. We say that ϕ is* saturated *w.r.t. $\mathcal{B}$ if for each $b_i \in \mathcal{B}$ such that $b_i \notin \tilde{n}$ we have that $b_i = x\sigma$ for some $x \in dom(\phi)$.*

Given a frame $\phi = \nu\tilde{n}.\{^{M_1}/_{x_1}, .., ^{M_\ell}/_{x_\ell}\}$ and a base of names $\mathcal{B} = [b_1, .., b_k]$ in which ϕ is decomposable, we denote by $\overline{\phi}^{\mathcal{B}}$ the frame defined as follows:

$$\overline{\phi}^{\mathcal{B}} = \nu\tilde{n}.\{^{M_1}/_{x_1}, \ldots, ^{M_\ell}/_{x_\ell}, ^{b_{i_1}}/_{y_1}, \ldots, ^{b_{i_p}}/_{y_p}\}$$

where $b_{i_1}, \ldots, b_{i_p}$ is a subsequence of $\mathcal{B}$ such that $b_{i_j} \notin \tilde{n}$ and $b_{i_j} \neq x\sigma$ for every $x \in dom(\phi)$. The variables $y_1, \ldots y_p$ are fresh, which means that they do not appear in $dom(\phi)$. Note that the resulting frame $\overline{\phi}^{\mathcal{B}}$ is saturated w.r.t. $\mathcal{B}$.

Example 7. Let ϕ be the frame given in Example 3. Let $\mathcal{B} = [n_1, n_2, n_3]$. We have that ϕ is decomposable on $\mathcal{B}$ and also that ϕ is saturated w.r.t. $\mathcal{B}$. However, note that ϕ is not saturated w.r.t. $\mathcal{B}' = [n_1, n_2, n_3, n_4]$. We have $\overline{\phi}^{\mathcal{B}'} = \nu\tilde{n}.\{^{3n_1+2n_2+3n_3}/_{x_1}, ^{n_2+3n_3}/_{x_2}, ^{3n_2+n_3}/_{x_3}, ^{3n_1+n_2+4n_3}/_{x_4}, ^{n_4}/_{y_1}\}$ where the sequence $\tilde{n}$ denotes n_1, n_2, n_3.

5 Deduction

We show that solving a deduction problem can be reduced to solving a linear system of equations in the corresponding semiring.

Theorem 1. *Let E be a monoidal theory and $\mathcal{S}_{\mathsf{E}}$ be its associated semiring. Deduction in E is reducible in polynomial time to the following problem:*

Entries*: A matrix A over $\mathcal{S}_{\mathsf{E}}$ of size $\ell \times m$ and a vector b over $\mathcal{S}_{\mathsf{E}}$ of size ℓ*
Question*: Does there exists X (element of $\mathcal{S}_{\mathsf{E}}^{\ell}$) such that $X \cdot A = b$?*

Note that when $\mathcal{S}_{\mathsf{E}}$ is commutative, this problem is equivalent to the problem of deciding whether $A^{\mathsf{T}} \cdot Y = b^{\mathsf{T}}$, *i.e* whether b^{T} is in the image of A^{T} where M^{T} is the transpose of M. Before proving the reduction we need to establish that we can restrict our attention to saturated frames. Moreover, for such frames, it is sufficient to consider recipes without names, *i.e.* such that $fn(\zeta) = \emptyset$.

Lemma 3. *Let $\phi = \nu\tilde{n}.\sigma$ be a frame and M be a ground term. Let $\mathcal{B}$ be a base of names in which ϕ and M are decomposable. We have that $\phi \vdash_{\mathsf{E}} M$ if and only if $\overline{\phi}^{\mathcal{B}} \vdash_{\mathsf{E}} M$. Moreover when $\overline{\phi}^{\mathcal{B}} \vdash_{\mathsf{E}} M$ there exists a recipe ζ of M such that $fn(\zeta) = \emptyset$.*

Proof. Intuitively, the first point is due to the fact that we extend ϕ with some names which are deducible from ϕ. Hence, in term of deducible power ϕ and $\overline{\phi}^{\mathcal{B}}$ are equivalent. More formally, if $\phi \vdash_{\mathsf{E}} M$, we can assume that there exists ζ such that $fn(\zeta) \subseteq \mathcal{B} \smallsetminus \tilde{n}$ and $fv(\zeta) \subseteq dom(\phi)$. From such a ζ it is easy to compute ζ' by replacing any occurrence of a name in $\mathcal{B} \smallsetminus \tilde{n}$ by the corresponding variable in $dom(\overline{\phi}^{\mathcal{B}})$ which refers to this name. Note that since, we can always assume that $fn(\zeta) \subseteq \mathcal{B} \smallsetminus \tilde{n}$, we have that $fn(\zeta') = \emptyset$. The reverse transformation, *i.e.* the replacement of variables in $dom(\overline{\phi}^{\mathcal{B}}) \smallsetminus dom(\phi)$ by names refereed by these variables in $\overline{\phi}^{\mathcal{B}}$, allows us to conclude for the converse. □

Reduction. Let $\phi = \nu\tilde{n}.\sigma$ be a frame and M be a ground term. Let $\mathcal{B}$ be a base of names in which ϕ and M are decomposable. We will also assume w.l.o.g. that ϕ is saturated w.r.t. $\mathcal{B}$. Let $A = \psi_{\mathcal{B}}(\phi)$, matrix of size $\ell \times m$ over $\mathcal{S}_{\mathsf{E}}$, and $b = \psi_{\mathcal{B}}(M)$, vector of size m over $\mathcal{S}_{\mathsf{E}}$.

Proof. (of Theorem 1) The construction described above is such that $X \cdot A = b$ has a solution over $\mathcal{S}_{\mathsf{E}}$ if and only if $\phi \vdash_{\mathsf{E}} M$.
($\Rightarrow$) We know that there exists $X \in \mathcal{S}_{\mathsf{E}}^{\ell}$ such that $X \cdot A = b$. Consider the recipe $\zeta = \psi^{-1}_{dom(\phi)}(X)$. By construction, we have that $fn(\zeta) \cap \tilde{n} = \emptyset$. It remains to show that $\zeta\sigma =_{\mathsf{E}} M$. For this, we establish that $\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{\mathcal{B}}(M)$. Thanks to Lemma 2, we have that $\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{dom(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi)$. Hence we deduce that $\psi_{\mathcal{B}}(\zeta\sigma) = X \cdot A = b = \psi_{\mathcal{B}}(M)$. Hence the result.
($\Leftarrow$) Assume that $\phi \vdash_{\mathsf{E}} M$. Thanks to Lemma 3 and by the fact that ϕ is saturated w.r.t. $\mathcal{B}$, we know that there exists $\zeta \in \mathcal{T}(\Sigma, dom(\phi))$ such that $\zeta\sigma =_{\mathsf{E}} M$. Let $Y = \psi_{dom(\phi)}(\zeta)$. It remains to establish that $Y \cdot A = b$. Since $\zeta\sigma =_{\mathsf{E}} M$, we have $\psi_{\mathcal{B}}(\zeta\sigma) = \psi_{\mathcal{B}}(M)$. By Lemma 2, we have $\psi_{dom(\phi)}(\zeta) \cdot \psi_{\mathcal{B}}(\phi) = \psi_{\mathcal{B}}(M)$, *i.e.* $Y \cdot A = b$ witnessing the fact that $X \cdot A = b$ has a solution over $\mathcal{S}_{\mathsf{E}}$. □

Example 8. Consider the theory ACUNh and the term $M = n_1 + \mathsf{h}(\mathsf{h}(n_1))$. Let $\phi = \nu n_1, n_2.\{^{n_1+\mathsf{h}(n_1)+\mathsf{h}(\mathsf{h}(n_1))}/_{x_1}, {}^{n_2+\mathsf{h}(\mathsf{h}(n_1))}/_{x_2}, {}^{\mathsf{h}(n_2)+\mathsf{h}(\mathsf{h}(n_1))}/_{x_3}\}$. We have that:

$$A = \begin{pmatrix} 1+\mathsf{h}+\mathsf{h}^2 & \mathsf{h}^2 & \mathsf{h}^2 \\ 0 & 1 & \mathsf{h} \end{pmatrix} \text{ and } b = \begin{pmatrix} 1+\mathsf{h}^2 \\ 0 \end{pmatrix}$$

The equation $X \cdot A = b$ has a solution over $\mathbb{Z}/2\mathbb{Z}[\mathsf{h}]$: $(1+\mathsf{h}, \mathsf{h}, 1)$. The term M is deducible from ϕ by using the recipe $x_1 + \mathsf{h}(x_1) + \mathsf{h}(x_2) + x_3$.

As a consequence, decidability/complexity results for deduction can be deduced from decidability/complexity results for solving linear system of equations (see Section 7).

6 Static equivalence

We show that deciding whether two frames are equivalent can be reduced to deciding whether two matrices satisfy the same set of equalities.

Theorem 2. *Let E be a monoidal theory and $\mathcal{S}_\mathsf{E}$ be its associated semiring. Static equivalence in E is reducible in polynomial time to the following problem:*

Entries*: Two matrices A_1 and A_2 over $\mathcal{S}_\mathsf{E}$ of size $\ell \times m$*
Question*: Does the following equality holds?*
$\{(X,Y) \in \mathcal{S}_\mathsf{E}^\ell \times \mathcal{S}_\mathsf{E}^\ell \mid X \cdot A_1 = Y \cdot A_1\} = \{(X,Y) \in \mathcal{S}_\mathsf{E}^\ell \times \mathcal{S}_\mathsf{E}^\ell \mid X \cdot A_2 = Y \cdot A_2\}$

Similarly to deduction, we first show that we can restrict our attention to saturated frames. Moreover, we show that it is sufficient to consider recipes, *i.e.* tests (M,N), without names.

Lemma 4. *Let $\phi_1 = \nu\tilde{n}.\sigma_1, \phi_2 = \nu\tilde{n}.\sigma_2$ and $\mathcal{B}$ be a base of names in which ϕ_1 and ϕ_2 are decomposable. We have that $\phi_1 \approx_\mathsf{E} \phi_2$ if and only if $\overline{\phi_1}^\mathcal{B} \approx_\mathsf{E} \overline{\phi_2}^\mathcal{B}$. Moreover, if $\overline{\phi_1}^\mathcal{B} \not\approx_\mathsf{E} \overline{\phi_2}^\mathcal{B}$ then there exist $M, N \in \mathcal{T}(\Sigma, dom(\overline{\phi_1}^\mathcal{B}))$ such that $(M =_\mathsf{E} N)\overline{\phi_1}^\mathcal{B} \not\Leftrightarrow (M =_\mathsf{E} N)\overline{\phi_2}^\mathcal{B}$.*

Proof. ($\Rightarrow$) Assume that $\phi_1 \approx_\mathsf{E} \phi_2$. We have that $\overline{\phi_1}^\mathcal{B} = \nu\tilde{n}.(\sigma_1 \cup \sigma_1^0)$ and $\overline{\phi_2}^\mathcal{B} = \nu\tilde{n}.(\sigma_2 \cup \sigma_2^0)$ for some substitutions σ_1^0 and σ_2^0 such that $\sigma_1^0 = \sigma_2^0$. Indeed, otherwise, we will obtain a test of the form $x = n_i$ with $x \in dom(\phi_1)$ and $n_i \in \mathcal{B} \smallsetminus \tilde{n}$ such that $(x =_\mathsf{E} n_i)\phi_1 \not\Leftrightarrow (x =_\mathsf{E} n_i)\phi_2$. Hence, we have that $dom(\overline{\phi_1}^\mathcal{B}) = dom(\overline{\phi_2}^\mathcal{B})$. Now, assume that $\overline{\phi_1}^\mathcal{B} \not\approx_\mathsf{E} \overline{\phi_2}^\mathcal{B}$, then

there exists a test (M, N) such that $(M =_{\mathsf{E}} N)\overline{\phi_1}^{\mathcal{B}}$ whereas $(M \neq_{\mathsf{E}} N)\overline{\phi_2}^{\mathcal{B}}$ (or the converse). Let $M' = M\sigma_1^0$ and $N' = N\sigma_1^0$. We have $(M' =_{\mathsf{E}} N')\phi_1$ whereas $(M' \neq_{\mathsf{E}} N')\phi_2$. Hence contradiction.
($\Leftarrow$) Assume that $\phi_1 \not\approx_{\mathsf{E}} \phi_2$. Let M, N be such that $(M =_{\mathsf{E}} N)\phi_1$ whereas $(M \neq_{\mathsf{E}} N)\phi_2$ (or the converse). It is clear that $\overline{\phi_1}^{\mathcal{B}} \not\approx_{\mathsf{E}} \overline{\phi_2}^{\mathcal{B}}$. Indeed, a witness of this fact is the test (M, N).

Lastly, if we have that $\phi_1 \not\approx_{\mathsf{E}} \phi_2$, then there exists a witness (M, N) such that $fn(M) \cup fn(N) \subseteq \mathcal{B} \smallsetminus \tilde{n}$. Hence, if we consider M' and N' the terms obtained from M and N by replacing any occurrence of a name in $\mathcal{B} \smallsetminus \tilde{n}$ by the corresponding variables in $dom(\overline{\phi_1}^{\mathcal{B}})$ which refers to this name, we easily conclude. □

Reduction. Let $\phi_1 = \nu\tilde{n}.\sigma_1$ and $\phi_2 = \nu\tilde{n}.\sigma_2$ be two frames having the same domain. Let $\mathcal{B}$ be a base of names in which the two frames are decomposable. We assume w.l.o.g. that ϕ_1 and ϕ_2 are saturated w.r.t. $\mathcal{B}$. Let $m = |\mathcal{B}|$. Let $A_1 = \psi_{\mathcal{B}}(\phi_1)$ and $A_2 = \psi_{\mathcal{B}}(\phi_2)$, two matrices of size $\ell \times m$, over $\mathcal{S}_{\mathsf{E}}$.

Proof. (of Theorem 2) The construction above is such that $\phi_1 \approx_{\mathsf{E}} \phi_2$ iff $\{(X, Y) \in \mathcal{S}_{\mathsf{E}}^{\ell} \times \mathcal{S}_{\mathsf{E}}^{\ell} \mid X \cdot A_1 = Y \cdot A_1\} = \{(X, Y) \in \mathcal{S}_{\mathsf{E}}^{\ell} \times \mathcal{S}_{\mathsf{E}}^{\ell} \mid X \cdot A_2 = Y \cdot A_2\}$.
($\Rightarrow$) Assume by contradiction that there exists a pair (X_M, X_N) such that $X_M \cdot A_1 = X_N \cdot A_1$ and $X_M \cdot A_2 \neq X_N \cdot A_2$ (or the converse). Let $M = \psi^{-1}_{dom(\phi_1)}(X_M)$ and $N = \psi^{-1}_{dom(\phi_1)}(X_N)$. We have that

- $(M =_{\mathsf{E}} N)\phi_1$. It is sufficient to show that $\psi_{\mathcal{B}}(M\sigma_1) = \psi_{\mathcal{B}}(N\sigma_1)$, *i.e.* $\psi_{dom(\phi_1)}(M) \cdot \psi_{\mathcal{B}}(\phi_1) = \psi_{dom(\phi_1)}(N) \cdot \psi_{\mathcal{B}}(\phi_1)$ thanks to Lemma 2. Now to conclude, it is sufficient to notice that we have $X_M = \psi_{dom(\phi_1)}(M)$, $X_N = \psi_{dom(\phi_1)}(N)$ and $A_1 = \psi_{\mathcal{B}}(\phi_1)$ and to rely on the hypothesis.
- $(M \neq_{\mathsf{E}} N)\phi_2$ can be shown similarly.

($\Leftarrow$) Assume that $\phi_1 \not\approx_{\mathsf{E}} \phi_2$. We have that there exists a test (M, N) such that $(M =_{\mathsf{E}} N)\phi_1$ and $(M \neq_{\mathsf{E}} N)\phi_2$ (or the converse). Thanks to Lemma 4 and the fact that the frames are saturated, we can assume that $M, N \in \mathcal{T}(\Sigma, dom(\phi_1))$. Let $X_M = \psi_{dom(\phi_1)}(M)$ and $X_N = \psi_{dom(\phi_1)}(N)$. We have that

- $X_M \cdot A_1 = X_N \cdot A_1$. Indeed, we have that $M\sigma_1 =_{\mathsf{E}} N\sigma_1$. Hence $\psi_B(M\sigma_1) = \psi_{\mathcal{B}}(N\sigma_1)$. By Lemma 2, we have $\psi_{dom(\phi_1)}(M) \cdot \psi_{\mathcal{B}}(\phi_1) = \psi_{dom(\phi_1)}(M) \cdot \psi_{\mathcal{B}}(\phi_1)$, *i.e.* $X_M \cdot A_1 = X_N \cdot A_1$.
- $X \cdot A_2 \neq Y \cdot A_2$ can be established in a similar way. □

Going further. Thanks to Theorem 2, we give a way to decide static equivalence in monoidal equational theories provided we can decide whether two sets of linear equations over $\mathcal{S}_{\mathsf{E}}$ have the same set of solutions. Actually, when $\mathcal{S}_{\mathsf{E}}$ is a ring or when we can extend the semiring $\mathcal{S}_{\mathsf{E}}$ into a ring $\mathcal{R}_{\mathsf{E}}$, the static equivalence problem is equivalent to the problem of deciding whether the following equality holds.

$$\{Z \in \mathcal{R}_{\mathsf{E}}^{\ell} \mid Z \cdot A_1 = 0\} = \{Z \in \mathcal{R}_{\mathsf{E}}^{\ell} \mid Z \cdot A_2 = 0\}$$

When $\mathcal{R}_{\mathsf{E}}$ is a commutative ring, it is equivalent to deciding whether $\mathsf{Ker}(A_1) = \mathsf{Ker}(A_2)$, where $\mathsf{Ker}(M)$ denotes the kernel of the matrices M, *i.e.* the set $\{X \mid M \cdot X = 0\}$.

The ring associated to a given monoidal theory E, denoted by $\mathcal{R}_{\mathsf{E}}$, is equal to $\mathcal{S}_{\mathsf{E}}$ when E is a group theory. Otherwise, it might be possible to extend the equational theory E with a new unary symbol $-$ and the law $x + -(x) = 0$ in order to obtain a theory E' that is consistent with E, *i.e.* for all $u, v \in \mathcal{S}_{\mathsf{E}}$ such that $u =_{\mathsf{E}'} v$, we have also that $u =_{\mathsf{E}} v$. In such a case, the ring $\mathcal{R}_{\mathsf{E}}$ is the semiring $\mathcal{S}_{\mathsf{E}'}$ associated to E' as explained in Section 4.1.

Example 9. We have seen that the semiring associated to AG is isomorphic to $\mathbb{Z}$ which is a commutative ring. Hence, we have that $\mathcal{R}_{\mathsf{E}}$ is isomorphic to $\mathbb{Z}$. The associated semiring to the monoidal equational theory ACU is isomorphic to $\mathbb{N}$ whereas its associated ring is $\mathbb{Z}$.

Note that the transformation described above does not allow us to associate a ring to any semiring. For instance, if we consider the theory ACUI and the theory E' obtained by the transformation described above, we have that $0 =_{\mathsf{E}'} (\mathbf{1} + \mathbf{1}) + -(\mathbf{1}) =_{\mathsf{E}'} \mathbf{1} + (\mathbf{1} + -(\mathbf{1})) =_{\mathsf{E}'} \mathbf{1}$ whereas this equality does not hold in ACUI.

7 Applications and Discussion

In this section we show that several interesting monoidal equational induce a ring or a semiring for which solving linear systems or checking for equalities of sets of solutions of linear systems are decidable. Note that any of these decidability results for deduction and static equivalence can be combined with any existing ones provided the signatures of the equational theories are disjoint [3]. For example, let E be a monoidal equational theory for which deduction and static equivalence are decidable (*e.g.* ACU, ACUNh, ...) then deduction and static equivalence are also decidable for the theory $\mathsf{E}_{\mathsf{enc}} \cup \mathsf{E}$ where $\mathsf{E}_{\mathsf{enc}}$ is defined by the following equations:

$$\mathsf{dec}(\mathsf{enc}(x, y), y) = x, \quad \mathsf{proj}_1(\langle x, y\rangle) = x \quad \text{and} \quad \mathsf{proj}_2(\langle x, y\rangle) = y.$$

Theory ACU. This equational theory is the simplest monoidal theory. The semiring corresponding to this theory is $\mathbb{N}$ whereas its associated ring is $\mathbb{Z}$. This equational theory has been particularly studied. Since the problem of solving linear equations over $\mathbb{N}$ is strongly NP-complete, we obtain that deduction is a NP-complete problem. The problem of static equivalence for this theory has been shown decidable in [1]. Actually thanks to the algebraic characterization given in this paper, this problem can be solved in polynomial time [18].

At first sight, it might seem surprising since it has been shown [1] that deduction in a given theory E can be reduced in polynomial time to static equivalence in E. However, this reduction required the presence of a free function symbol and such a function symbol is not available in the theory ACU. Hence, the polynomial reduction provided in [1] does not apply in this setting.

Theories ACUI and ACUN (Exclusive Or). The semirings corresponding to these equational theories are respectively the Boolean semiring $\mathbb{B}$, which is finite, and the finite field $\mathbb{Z}/2\mathbb{Z}$. The theory ACUN has already been studied in terms of deduction [8, 7] and static equivalence [1]. Deduction and static equivalence are both decidable in polynomial time. As far as we know the theory ACUI has only been studied in term of deduction [10]. Actually, since its associated semiring is finite, we easily deduce that deduction and static equivalence are decidable.

Theory AG (Abelian Groups). The semiring associated to this equational theory is in fact a ring, namely the ring $\mathbb{Z}$ of all integers. There exist several algorithms to compute solutions of linear equations over $\mathbb{Z}$ and to compute a base of the set of solutions (see for instance [18]). Hence, we easily deduce that both problems are decidable in PTIME. Deduction for this theory has already been studied in [8] and [6].

Theories ACUh, ACUNh and AGh. The semiring associated to ACUh is $\mathbb{N}[\mathsf{h}]$, the semiring of polynomial in one indeterminate over $\mathbb{N}$ whereas the ring associated to ACUh is $\mathbb{Z}[\mathsf{h}]$. For the theory ACUNh (resp. AGh) the associated semiring is $\mathbb{Z}/2\mathbb{Z}[\mathsf{h}]$ (resp. $\mathsf{Z}[\mathsf{h}]$). Deduction for these three equational theories have already been studied in [11, 9]. However, results obtained on static equivalence are new.

1. ACUh and AGh: Deciding static equivalence for these both theories is reducible to the problem of deciding whether $\mathsf{Ker}(A) = \mathsf{Ker}(B)$

where A and B are matrices built over $\mathsf{N}[\mathsf{h}]$ in the case of ACUh and $\mathsf{Z}[\mathsf{h}]$ in the case of AGh. This problem has been solved by F. Baader to obtain a unification algorithm for the theory AGh (see [4]). This is done by the help of Gröbner Base methods in a more general settings. Actually, he provides an algorithm even in the case of several commutating homomorphisms.
2. ACUNh: Deciding static equivalence in ACUNh is reducible to the problem of deciding whether $\mathsf{Ker}(A) = \mathsf{Ker}(B)$ where A and B are matrices built over $\mathsf{Z}/2\mathsf{Z}[\mathsf{h}]$. This is achieved in [12] by using an automata-theoretic approach.

Theory ACUIh. The semiring associated to ACUIh is $\mathbb{B}[\mathsf{h}]$. Deduction for this theory has never been studied but is clearly decidable. Indeed, to find a solution to $A \cdot X = b$, it is easy to see that each component of a solution to $A \cdot X = b$ has a degree smaller than the degree of b. Hence, the question of deciding whether there exists X such that $A \cdot X = b$ can be reduced to solving a system of linear equations over $\mathbb{B}$. Theorem 2 does not help us to provide an algorithm to solve static equivalence. Note also that we can not reduced the problem to the problem of deciding whether $\mathsf{Ker}(A) = \mathsf{Ker}(B)$ since, as for ACUI, we are not able to associate a ring to this theory.

Theory E	$\mathcal{S}_\mathsf{E}$	$\mathcal{R}_\mathsf{E}$	Deduction	Static Equivalence
ACU	$\mathbb{N}$	$\mathbb{Z}$	NP-complete	decidable [1], PTIME (*new*)
ACUI	$\mathbb{B}$	–	decidable [10]	decidable (*new*)
ACUN	$\mathbb{Z}/2\mathbb{Z}$		PTIME [7]	decidable [1], PTIME (*new*)
AG	$\mathbb{Z}$		PTIME [6]	PTIME (*new*)
ACUh	$\mathbb{N}[\mathsf{h}]$	$\mathbb{Z}[\mathsf{h}]$	NP-complete [11]	decidable (*new*)
ACUIh	$\mathbb{B}[\mathsf{h}]$	–	decidable (*new*)	?
ACUNh	$\mathbb{Z}/2\mathbb{Z}[\mathsf{h}]$		PTIME [9]	decidable (*new*)
AGh	$\mathbb{Z}[\mathsf{h}]$		PTIME [9]	decidable (*new*)
$\mathsf{AGh}_1 \ldots \mathsf{h}_\mathsf{n}$	$\mathbb{Z}[\mathsf{h}_1, \ldots, \mathsf{h}_n]$		decidable (*new*)	decidable (*new*)

8 Conclusion

We have proposed a general schema for deciding deduction and static equivalence algorithms. This schema has to be filled with procedures for linear equations in order to yield complete algorithms. Such algorithms strongly depend on the structure of the semiring. In this paper, we have mentioned and used several existing results of Algebra. But Algebra can still provide useful techniques that allow us to deduce some new results. Moreover, efficient existing tools for solving algebraic problems can also be used to implement our algorithms.

Acknowledgment. We wish to thank Daniel Lazard for fruitful discussions.

References

1. M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 387(1-2):2–32, November 2006.
2. M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. 28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115, London (UK), 2001. ACM.
3. M. Arnaud, V. Cortier, and S. Delaune. Combining algorithms for deciding knowledge in security protocols. In *Proc. of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07)*, LNAI, Liverpool, UK, 2007. Springer. To appear.
4. F. Baader. Unification in commutative theories, Hilbert's basis theorem, and Gröbner bases. *Journal of the ACM*, 40(3):477–503, 1993.
5. F. Baader and W. Nutt. Combination problems for commutative/ monoidal theories or How algebra can help in equational unification. *Applicable Algebra Engineering Communication and Computing*, 7(4):309–337, 1996.
6. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. Deciding the security of protocols with Diffie-Hellman exponentiation and product in exponents. In *Proc. 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS'03)*, volume 2914 of *LNCS*, pages 124–135, Mumbai (India), 2003. Springer-Verlag.
7. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with XOR. In *Proc. 18th IEEE Symposium on Logic in Computer Science (LICS'03)*, pages 261–270, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.
8. H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *Proc. 18th IEEE Symposium on Logic in Computer Science (LICS'03)*, pages 271–280, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.
9. S. Delaune. Easy intruder deduction problems with homomorphisms. *Information Processing Letters*, 97(6):213–218, Mar. 2006.
10. S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis for monoidal equational theories. Research Report LSV-06-17, Laboratoire Spécification et Vérification, ENS Cachan, France, Nov. 2006. 47 pages.
11. P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for AC-like equational theories with homomorphisms. In *Proc. 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *LNCS*, pages 308–322, Nara (Japan), 2005. Springer.

12. P. Lafourcade, D. Lugiez, and R. Treinen. ACUNh: Unification and disunification using automata theory. In *Proc. 20th Int. Workshop on Unification (UNIF'06)*, pages 6–20, Seattle, Washington, USA, Aug. 2006.
13. G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *Proc. 2nd Int. Workshop on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'96)*, volume 1055 of *LNCS*, Berlin (Germany), 1996. Springer-Verlag.
14. J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *Proc. 8th ACM Conference on Computer and Communications Security (CCS'01)*. ACM Press, 2001.
15. W. Nutt. Unification in monoidal theories. In *Proc. 10th Int. Conference on Automated Deduction, (CADE'90)*, volume 449 of *LNCS*, pages 618–632, Kaiserslautern (Germany), 1990. Springer.
16. L. C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6(1-2):85–128, 1998.
17. M. Rusinowitch and M. Turuani. Protocol insecurity with a finite number of sessions, composed keys is NP-complete. *Theoretical Computer Science*, 1-3(299):451–475, 2003.
18. A. Schrijver. *Theory of Linear and Integer Programming.* Wiley, 1986.