Symbolic Protocol Analysis for Monoidal Equational Theories ⋆

Stéphanie Delaune [a], Pascal Lafourcade [b], Denis Lugiez [c], Ralf Treinen [d]

[a] *LORIA, INRIA project Cassis, Nancy, France*

[b] *Information Security Group, Dep. Computer Science, ETH Zürich, Switzerland*

[c] *LIF, Université Aix-Marseille1 & CNRS UMR 6166, France*

[d] *LSV, CNRS UMR 8643, ENS de Cachan & INRIA Futurs, France*

Abstract

We are interested in the design of automated procedures for analyzing the (in)security of cryptographic protocols in the Dolev-Yao model for a bounded number of sessions when we take into account some algebraic properties satisfied by the operators involved in the protocol. This leads to a more realistic model than what we get under the perfect cryptography assumption, but it implies that protocol analysis deals with terms modulo some equational theory instead of terms in a free algebra. The main goal of this paper is to set up a general approach that works for a whole class of monoidal theories which contains many of the specific cases that have been considered so far in an ad-hoc way (*e.g.* exclusive or, Abelian groups, exclusive or in combination with the homomorphism axiom). We follow a classical schema for cryptographic protocol analysis which proves first a locality result and then reduces the insecurity problem to a symbolic constraint solving problem. This approach strongly relies on the correspondence between a monoidal theory E and a semiring $\mathcal{S}_{\mathsf{E}}$ which we use to deal with the symbolic constraints. We show that the well-defined symbolic constraints that are generated by reasonable protocols can be solved provided that unification in the monoidal theory satisfies some additional properties. The resolution process boils down to solving particular quadratic Diophantine equations that are reduced to linear Diophantine equations, thanks to linear algebra results and the well-definedness of the problem. Examples of theories that do not satisfy our additional properties appear to be undecidable, which suggests that our characterization is reasonably tight.

⋆ This work has been partly supported by the RNTL project PROUVÉ 03V360, the ACI-SI Rossignol, the RNTL project POSÉ and by the DGA under grant number 06 60 019 00 470 75 01.

1 Introduction

Cryptographic protocols. Cryptographic protocols are small concurrent programs that use cryptographic primitives like encryption under public or symmetric keys, digital signatures, etc., to ensure confidentiality of the messages exchanged in an insecure environment. To write correct cryptographic protocols has turned out to be a difficult and error-prone task. For instance, a man in the middle attack has been found [Low96] in the infamous Needham-Schroeder protocol [NS78] only seventeen years after the first description of the protocol. This calls for automated tools to help designers to check that their protocol is free of logical flaws, and a lot of progress has been done in this direction. These achievements rely on the so-called Dolev-Yao model [DY81] which assumes that the cryptography is perfect, *i.e.*, one cannot decipher an encrypted message if one does not know the decryption key. In this model, messages are terms of a free algebra, and the deductive power of the attacker, designated later on as the *intruder*, is modeled by a set of deduction rules. In this framework, known as the *formal model* approach, the insecurity problem amounts to deciding whether there is an execution of the protocol that allows the intruder to learn some secret data. The insecurity problem is undecidable when the number of sessions of the protocol is unbounded. Several decidability results have been proved for a bounded number of sessions [MV01,ALV02,RT03], which is the case that we consider in this paper, yielding the realization of effective tools like [AVI]. These results rely on a reduction of the insecurity problem to a symbolic constraint solving problem.

Algebraic properties. The hypothesis of perfect cryptography in the Dolev-Yao model is too strong since protocols use operations that satisfy some algebraic properties used in a crucial way in the protocol or in the encryption/decryption process. For example, this is the case for the DES and for the more recent AES which both rely on the properties of exclusive or. Therefore, a current trend in the formal model approach is to relax the perfect cryptography hypothesis in order to accommodate for these algebraic properties, and several new decidability results have been obtained, for instance in the case of exclusive or (ACUN), Abelian groups (AG), and weak models of modular exponentiation [CKRT03,CLS03,CKR$^+$03,MS05]. A weakness of these approaches is their lack of generality since each new theory requires a new complex proof. This calls for results that are as generic as possible, or for new paradigms. 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 specifically the combinations of these axioms that constitute monoidal theories.

Our contribution. In this paper we propose a general approach to handle *monoidal theories* that covers several cases already studied, and furthermore includes properties of homomorphic operators. A monoidal theory E determines a semiring $\mathcal{S}_{\mathsf{E}}$, that is, an algebraic structure which can be thought of as a ring without subtraction. For instance, the semirings corresponding to the theories ACU, AG and ACUNh are the natural numbers $\mathbb{N}$, the ring of integers $\mathbb{Z}$ and the ring $\mathbb{Z}_2[\mathsf{h}]$ (a.k.a. $\mathsf{GF}(2)[\mathsf{h}]$) of polynomials in the indeterminate h with coefficients from the finite field $\mathbb{Z}_2$. Monoidal theories have been extensively studied by F. Baader and W. Nutt [Nut90,Baa93,BN96] who have provided a complete survey of unification in these theories. We shall rely on these previous results in an essential way since the decidability of unification is a necessary condition for the decidability of protocol insecurity.

If the monoidal theory enjoys some additional properties then our approach provides a decision procedure for protocol insecurity for a bounded number of sessions. This procedure applies to a large class of algebraic theories that generalizes many previous works. The additional properties required involve natural concepts from algebra: (1) unification must be unitary, that is any solvable unification problem has a most general solution, and (2) $\mathcal{S}_{\mathsf{E}}$ must be an Euclidean ring that is either finite or where the Euclidean division has some good properties, and such that linear Diophantine equations are solvable. As far as we know this is the most general result for theories involving AC axioms. Our procedure is inspired by the work of J. Millen and V. Shmatikov for the Abelian group theory [MS05] but it is different in several aspects: it handles monoidal theories, and we have devised a characterization of well-defined systems that relies on classical linear algebra concepts. Furthermore, our resolution procedure for solving quadratic Diophantine equations is different and more general than the procedure of [MS05].

The main steps of our method are sketched as follows. First, we replace the deduction system modeling the intruder capabilities by a new system containing a rule which "compresses" into a single rule sequences of rule applications of the original system involving operators subject to the algebraic laws. This will allow us later to model arbitrary sequences of these operators by linear equations over the semiring $\mathcal{S}_{\mathsf{E}}$. Next we will exploit the fact that any reasonable protocol, i.e. any protocol where participants have a deterministic behavior, will result in a so-called *well-defined* constraint system [MS05]. Thanks to properties of unification in monoidal theories we reduce the solvability of constraint systems (where a constraint denotes existence of a deduction of arbitrary length) to the solvability of one-step constraint systems (where constraints denote exactly one application of a deduction rule), which then are transformed into constraint systems in a signature consisting of constants and operators of the theory E, but without the operations of the Dolev-Yao model like pairing and encryption. Then we prove that if the monoidal theory enjoys some additional properties, such as the finiteness of $\mathcal{S}_{\mathsf{E}}$, then the resolution of

the latter system amounts to solving particular quadratic Diophantine equations in the semiring $\mathcal{S}_{\mathsf{E}}$. Finally, we can thanks to the well-definedness of the constraint system reduce the resolution of this quadratic system to the resolution of a system of linear Diophantine equations, which is decidable.

Our characterization is reasonably tight as shown by the case of the AGh theory: this theory has a decidable unification problem but the associated semiring is neither finite nor an Euclidean ring, and protocol insecurity is in fact undecidable [Del06b].

Applications to cryptographic operators and protocols Properties of cryptographic operators are crucial for the design and the verification of cryptographic protocols for at least two reasons: The design of a protocol can itself make essential use of some algebraic properties, or it may the case that cryptographic operators used for the realization of a protocol "accidentally" enjoy properties which then can be exploited by an attacker. Protocols that are based on the properties of *exclusive or* fall into the first case, like for instance Bull's recursive authentication protocol which was proved correct in a model which abstracts from the algebraic properties [Pau97], but for which later an attack was found when taking account the properties of *exclusive or* [RS98]. An example of a protocol with "accidental" algebraic properties of cryptographic operators is the TMN protocol where the RSA-like asymmetric encryption operation has the properties of Abelian groups with homomorphism. This protocol has a vulnerability based on exactly these algebraic properties [Sim94].

The algebraic theories of *exclusive or*, as of Abelian groups with a homomorphism, are instances of the class of monoidal theories to which our results apply.

Related works. Many results have already been obtained for an exact analysis of cryptographic protocols in presence of algebraic properties for a bounded number of sessions. The theory of exclusive or (ACUN theory) was addressed first [CKRT03,CLS03], followed by the case of modular exponentiation. In this later case decidability results [CKR$^+$03,MS05] and undecidability results [KNW03] have been shown, depending on the accurateness of the axiomatization. The results of [CKRT03,CKR$^+$03] are presented in a very general framework (oracle rules), but these rules are difficult to use and this framework has not been used for other theories than the ones already mentioned. Abelian groups were also treated in [MS05], and homomorphic properties have been dealt with either in isolation [CLT03] or in combination with other properties [DLLT06]. When the algebraic theory enjoys a particular subterm property which can be checked syntactically, protocol insecurity is decidable for a

bounded number of sessions [DJ04,Bau05]. A general approach for handling algebraic properties has been advocated in [CL04], but it relies on the finite variant property which does not hold in the ACUNh case [CD05] (for which we get a decidability result) and requires that the AC case is solved. Surprisingly enough, this simple theory does not fulfill our conditions and its status is still open. Another direction of research is to use a combination algorithm that, given decidability results for disjoint theories, yields a decidability result for the union of the theories [CR05]. This has been extended to non-disjoint properties [CR06], but the requirements on the theories are strong, and the main relevant application so far is modular exponentiation. None of these combination methods are applicable for the class that we deal with.

When we generalize to protocol insecurity for an *un*bounded number of sessions the problem becomes undecidable even without algebraic properties, and even when additional restrictions are imposed on the messages [DLMS04]. Dealing with general algebraic properties like in [BMV05,ZD04] leads to procedures that approximate the behavior of the protocol and/or require strong conditions on the equational theories to get termination and exact analysis. Furthermore, the final verification is often done with an automated theorem prover such as ProVerif [Bla01] for which no termination guarantee holds in general.

Plan of the paper. We recall the links between protocol insecurity and constraint systems in Section 2. After some preliminaries we describe, in Section 4, the Dolev-Yao model and we state the locality theorem which is a prerequisite for the constraint solving procedure. The first part of our procedure for handling protocol insecurity proceeds by several successive simplification steps and is detailed through Section 5 to Section 8. Our first Theorem (Theorem 42) allows us to deal with monoidal theories for which the associated semiring is finite. Finally, in Sections 9 and 10, we show how to reduce the search space of solutions to deal with the case where the associated semiring is infinite (Theorem 62). Section 11 summarizes our decidability results. The last two Sections 12 and 13 show how this general framework can be instantiated by specific equational theories, and discuss why it does not apply to certain other equational theories.

2 Protocol Insecurity as a Constraint Solving Problem

We briefly recall on a simple example how protocol insecurity is reduced to constraint solving. For more details the reader is referred to [MV01] for instance.

A cryptographic protocol is defined by a set of programs (or *roles*) which may be executed by agents which are distributed over a network. In the simplest case these programs are linear sequences of *receive* and *send* instructions on a public communication channel. The attacker may modify the messages sent on the channel using a certain set of *intruder capabilities*. The fact that all messages may be modified by the attacker is often expressed by saying that *the attacker is the network*.

The most basic property of cryptographic protocols is the so-called *secrecy* property, which states that for any number of agents executing the roles, for any possible interlacing of the program execution, and for any modifications of the messages by the attacker (according to his deduction capabilities) the intruder is not able to deduce a certain message which is supposed to remain secret.

In the case of a bounded number of sessions, *i.e.* a bounded number of role instances running in parallel, there is only a bounded number of symbolic traces, each of which represents an interleaving of the execution of the parallel role instances. Every message received during the execution of a role is a message that can be deduced using the intruder deduction capabilities from the messages sent before on the communication channel. The idea of the algorithm is to guess a symbolic trace in which the messages are represented by terms containing variables. This symbolic trace corresponds to a concrete execution trace if the variables can be instantiated in such a way that at every moment a message received by an agent can in fact be deduced by the intruder from the messages seen before.

Let $\{m\}_K$ denotes the encryption of m by the key K and let $+$ denote some binary operation on messages. Let us consider the toy protocol

$$A \to B : \{N_a\}_K$$
$$B \to A : \{N_b\}_K$$

which is used by roles A and B to share a temporary secret, say $\{N_a + N_b\}_K$, that can be used once for some latter transaction. The protocol involves a permanent symmetric key K shared by A and B and nonces N_a, N_b.

The protocol is a sequence of receive-send actions $0 \to \{N_a\}_K, \{x\}_K \to \{N_b\}_K$ (the initial 0 serves to kick off the protocol).

The fact that the execution of a single session of the protocol is insecure is

described by the following sequence of deduction constraints:

$$T \Vdash 0$$
$$T, \{N_a\}_K \Vdash \{x\}_K$$
$$T, \{N_a\}_K, \{N_b\}_K \Vdash \{N_a + N_b\}_K$$

where T is the initial knowledge of the intruder, say $T = \{0\}$ in this example. The last deduction step states that the secret is revealed and the protocol is insecure if the constraint system has a solution.

The procedure to solve these constraints system returns an instantiation of the variables, for instance $\{x \mapsto N_a\}$ which satisfies the ground deducibility constraint system

$$T \vdash 0$$
$$T, \{N_a\}_K \vdash \{N_a\}_K$$
$$T, \{N_a\}_K, \{N_b\}_K \vdash \{N_a + N_b\}_K$$

where $\vdash$ is the relation that describes the attacker deduction capabilities as a proof system. This latter system is satisfiable for instance if the operator $+$ is the *exclusive or* and if the encryption by K is an homomorphism over the operator $+$. These algebraic properties define monoidal theories and our goal is to provide a solution for protocol insecurity in these theories.

To achieve this goal, we follow a classical approach:

(1) Prove a locality result required for the satisfiability of ground deducibility system. This means that if $T \vdash u$ holds, then there is a proof consisting only of subterms of T and u for an appropriate notion of subterms and for a variant of the proof system (that relies on solving linear equations in monoidal theories).
(2) Give a decision procedure for solving so called well-defined constraints system in monoidal theories. The first step is to reduce the deduction constraints to a system of particular quadratic Diophantine equations, and the second one is to solve these Diophantine equations in an ad-hoc way. These two steps can be done successfully when the monoidal theory E enjoys some additional properties.

The most difficult part of this work deals with part (2) and presents:

- A procedure for solving constraint systems and the conditions required on the equational theory E allowing us to apply it. Those conditions are summarized in Section 11 (Theorems 42 and 62).
- The proofs concerning soundness, completeness and termination of our procedure are stated and proved along the description of the procedure.

3 Preliminaries

3.1 Terms

We use classical notations and terminology from [DJ90,BS01] on terms, unification and rewrite systems. We write $\mathcal{T}(\mathcal{F}, \mathcal{X})$ for the set of terms. For our purpose, the set $\mathcal{F}$ is partitioned into a subset $\mathcal{PF}$ of *private* function symbols, and a subset $\mathcal{VF}$ of *visible* or *public* function symbols. We also assume that $\mathcal{VF}$ contains at least the function symbols $\langle \_, \_ \rangle$, $\{\_\}_\_$. The set of variables occurring in a term t is denoted by $vars(t)$.

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. Note that the result of such a replacement is uniquely determined. A replacement $[x \mapsto t]$ is also a substitution.

3.2 Equational Theories and Contexts

An equational theory E is a set of equations (*i.e.* a set of unordered pairs of terms). We denote by $sig(\mathsf{E})$ the set of all function symbols occurring in E. Given two terms s and t such that $s, t \in \mathcal{T}(sig(\mathsf{E}), \mathcal{X})$, we write $t =_\mathsf{E} s$ if the equation $t = s$ is an equational consequence of E.

It is well known that $=_\mathsf{E}$ is a $sig(\mathsf{E})$-congruence, and that we can define, for any set $\mathcal{X}$, the quotient algebra $\mathcal{T}(sig(\mathsf{E}), \mathcal{X})/\mathsf{E}$, the elements of which are congruence classes of $\mathcal{T}(sig(\mathsf{E}), \mathcal{X})$ under the relation $=_\mathsf{E}$. See for instance [MT92] for details.

An E-*context* is a λ-term $\lambda y_1, \ldots, y_n.t$ with $t \in \mathcal{T}(sig(\mathsf{E}), \{y_1, \ldots, y_n\})$, also written $t[y_1, \ldots, y_n]$. The application of $t[y_1, \ldots, y_n]$ to arguments $u_1, \ldots, u_n$ is written $t[u_1, \ldots, u_n]$.

3.3 Monoidal Equational Theories

In this paper, we are particularly interested in the class of monoidal equational theories introduced by W. Nutt. [Nut90].

Definition 1 (monoidal theory) *An equational theory* E *is called* monoidal *if it satisfies the following properties:*

(1) The signature $sig(\mathsf{E})$ contains a binary function symbol $+$ and a constant symbol 0, and all other function symbols in $sig(\mathsf{E})$ are unary.
(2) The symbol $+$ is associative-commutative with unit 0. In other words, we have that $x + (y + z) =_{\mathsf{E}} (x + y) + z$, $x + y =_{\mathsf{E}} y + x$ and $x + 0 =_{\mathsf{E}} x$.
(3) Every unary function symbol $\mathsf{h} \in sig(\mathsf{E})$ is an endomorphism for $+$ and 0, i.e. $\mathsf{h}(x + y) =_{\mathsf{E}} \mathsf{h}(x) + \mathsf{h}(y)$ and $\mathsf{h}(0) =_{\mathsf{E}} 0$.

Example 2 *Suppose "+" is a binary function symbol and 0 is nullary. Moreover assume that the others symbols (e.g. $-$, h) are unary symbols. The equational theories below are monoidal.*

- *The theory* ACU *which consists of:*
  · *Associativity, Commutativity* (AC) $(x+y)+z = x+(y+z)$, $x+y = y+x$,
  · *Unit* (U) $x + 0 = x$.
- *The theories* ACUI *and* ACUN *(also called* exclusive or theory*):*
  the axioms (AC) *and* (U) *with in addition Idempotency* (I) $x + x = x$ *or Nilpotency* (N) $x + x = 0$
- *The theory* AG *of so-called* Abelian groups*:*
  AG *is generated by the identities* (AC), (U) *and* $x + -(x) = 0$ (Inv).
- *The theories* ACUh, ACUIh, ACUNh, AGh*: these equational theories correspond to the equational theories 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* $\mathsf{h}(0) = 0$.

Note that there are two homomorphisms in the theory AGh, namely $-$ and h. These two homomorphisms commute, that is $\mathsf{h}(-x) =_{\mathsf{AGh}} -(\mathsf{h}(x))$. More examples of monoidal equational theories can be found in [Nut90].

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 $\cdot$ the *addition* and the *multiplication* of the semiring. The elements 0 and 1 are called *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 $\alpha + (-\beta)$.

For any monoidal theory E there exists a corresponding semiring $\mathcal{S}_{\mathsf{E}}$ [Nut90]. We can rephrase the definition of $\mathcal{S}_{\mathsf{E}}$ as follows. Its universe is $\mathcal{T}(sig(\mathsf{E}), \{\mathbf{1}\})/\mathsf{E}$,

that is the set of equivalence classes of E-terms possibly containing the new constant $\mathbf{1}$ under equivalence by the equational axioms E. The constant 0 and the sum $+$ of the semiring are defined as in the algebra $\mathcal{T}(sig(\mathsf{E}), \{\mathbf{1}\})/\mathsf{E}$. 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.

Example 4 *The universe of the semiring $\mathcal{S}_{\mathsf{ACUN}}$ consists of the two elements 0 and $\mathbf{1}$. We have in $\mathcal{S}_{\mathsf{ACUN}}$ that $0 + \mathbf{1} = \mathbf{1} + 0 = \mathbf{1}$, $0 + 0 = \mathbf{1} + \mathbf{1} = 0$, $0 \cdot 0 = \mathbf{1} \cdot 0 = 0 \cdot \mathbf{1} = 0$, and $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$. Hence, $\mathcal{S}_{\mathsf{ACUN}}$ is isomorphic to the ring $\mathbb{Z}_2$.*

It has been shown [Nut90] that

(1) $\mathcal{S}_{\mathsf{E}}$ is a ring if, and only if, E is a group theory.
(2) $\mathcal{S}_{\mathsf{E}}$ is commutative if, and only if, E has commuting homomorphisms, that is if $\mathsf{h}_1(\mathsf{h}_2(x)) =_{\mathsf{E}} \mathsf{h}_2(\mathsf{h}_1(x))$ for any two homomorphisms h_1 and h_2.

Note that any E with no more than one homomorphism has commuting homomorphisms.

Example 5 *The semiring $\mathcal{S}_{\mathsf{AGh}}$ is isomorphic to $\mathbb{Z}[\mathsf{h}]$, the commutative ring of polynomials in the indeterminate h with integer coefficients. Note that AGh is a group theory and has commuting homomorphisms.*

We denote by $\phi_{\mathbf{1}} \colon \mathcal{T}(sig(\mathsf{E}), \{\mathbf{1}\})/\mathsf{E} \to \mathcal{S}_{\mathsf{E}}$ the function which maps any term $t \in \mathcal{T}(sig(\mathsf{E}), \{\mathbf{1}\})/\mathsf{E}$ to t considered as an element of the semiring $\mathcal{S}_{\mathsf{E}}$. We often choose for convenience of presentation some semiring $\mathcal{S}'_{\mathsf{E}}$ which is isomorphic to $\mathcal{S}_{\mathsf{E}}$, and also use $\phi_{\mathbf{1}}$ for the corresponding function from $\mathcal{T}(sig(\mathsf{E}), \{\mathbf{1}\})/\mathsf{E}$ to $\mathcal{S}'_{\mathsf{E}}$. In case of a finite set X of p generators (*i.e.* variables) we generalize this construction and obtain a function which assigns to any term a tuple in $\mathcal{S}^p_{\mathsf{E}}$, that is a tuple of p elements from $\mathcal{S}_{\mathsf{E}}$. For $X = \{c_1, \ldots, c_p\}$ we define the function $\phi_X \colon \mathcal{T}(sig(\mathsf{E}), X)/\mathsf{E} \to \mathcal{S}^p_{\mathsf{E}}$ as follows: any term $t \in \mathcal{T}(sig(\mathsf{E}), X)/\mathsf{E}$ has a unique decomposition $t = t_1 + \ldots + t_p$ with $t_i \in \mathcal{T}(sig(\mathsf{E}), \{c_i\})/\mathsf{E}$, and we define $\phi_X(t) = (\phi_{c_1}(t_1), \ldots, \phi_{c_p}(t_p))$.

Example 6 *Taking into account that the semiring $\mathcal{S}_{\mathsf{AGh}}$ is (isomorphic to) $\mathbb{Z}[\mathsf{h}]$, we have that*

$$\phi_{\{c_1,c_2,c_3\}}(c_1 + c_1 + \mathsf{h}(c_3) + \mathsf{h}^3(c_3)) = (2, 0, \mathsf{h}^3 + \mathsf{h})$$

where $\mathsf{h}^n(t)$ ($n \geq 1$) stands for n applications of the function h to the term t.

If we have additional free constant symbols from some set C in the signature then we can decompose any term $t \in \mathcal{T}(sig(\mathsf{E}) \cup C, \{c_1, \ldots, c_p\})$ in a unique way as $t = t_1 + \ldots + t_p + t^0$ with $t_i \in \mathcal{T}(sig(\mathsf{E}), \{c_i\})/\mathsf{E}$ and $t^0 \in \mathcal{T}(sig(\mathsf{E}) \cup C, \emptyset)$.

Example 7 *If $C = \{a, b\}$ then the decomposition of the term $t = a + c_1 + \mathsf{h}(\mathsf{h}(c_3)) + b$ is $t = t_1 + t_2 + t_3 + t^0$ where $t_1 = c_1$, $t_2 = 0$, $t_3 = \mathsf{h}(\mathsf{h}(c_3))$, $t^0 = a + b$.*

Definition 8 (operation $\odot$) *Let p be an element of $\mathcal{S}_{\mathsf{E}}$ and t be a term in $\mathcal{T}(\mathcal{F}, \{c_1, \ldots, c_p\})$. The product of p by t, denoted $p \odot t$ is the uniquely defined term such that $\phi_{\{c_i\}}(p \odot t) = p \cdot \phi_{\{c_i\}}(t)$ for any i.*

Example 9 *In case of the equational theory* AGh *we have that, using the usual abbreviations:*

$$\left(\Sigma_{i=1}^{n} \alpha_i \mathsf{h}^i\right) \odot \left(\Sigma_{j=1}^{m} t_j\right) = \Sigma_{i=1}^{n} \Sigma_{j=1}^{m} \alpha_i \mathsf{h}^i(t_j)$$

For instance,

$$(h^2 + 2h) \odot (c_1 + c_3 + \mathsf{h}(c_3)) = \mathsf{h}^2(c_1) + 2\mathsf{h}(c_1) + \mathsf{h}^3(c_3) + 3\mathsf{h}^2(c_3) + 2\mathsf{h}(c_3)$$

4 The Attacker Model

4.1 The Inference System

The deduction capabilities of an intruder are modeled by the now classical *Dolev-Yao model* [DY81]. We extend the intruder capabilities by equational reasoning modulo a set E of equational axioms which is assumed to satisfy $sig(\mathsf{E}) \subseteq (\mathcal{VF} \setminus \{\langle \_, \_ \rangle, \{\_\}_\_\})$. This inference system, denoted $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$, is formally defined in Figure 1.

$$\textsf{Unpairing (UL)}\ \frac{T \vdash \langle u, v \rangle}{T \vdash u} \qquad \textsf{Compose (C)}\ \frac{T \vdash u_1 \ \ldots \ T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)}\ \text{with } f \in \mathcal{VF}$$

$$\textsf{Unpairing (UR)}\ \frac{T \vdash \langle u, v \rangle}{T \vdash v} \qquad \textsf{Decryption (D)}\ \frac{T \vdash \{u\}_v \quad T \vdash v}{T \vdash u}$$

$$\textsf{Equality (Eq)}\ \frac{T \vdash u}{T \vdash v} \quad u =_{\mathsf{E}} v$$

Figure 1. Inference System $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$.

The intended meaning of a *sequent* $T \vdash u$ is that the intruder is able to deduce the term $u \in \mathcal{T}(\mathcal{F}, \mathcal{X})$ from the finite set of terms $T \subseteq \mathcal{T}(\mathcal{F}, \mathcal{X})$. As in the standard Dolev-Yao model, the intruder can compose new terms (C) from known terms, he can also decompose pairs (UL, UR) and decrypt ciphertexts,

provided that he can deduce the decryption key (D). Finally, we relax the *perfect cryptography assumption* by taking into account the algebraic properties of the cryptographic primitives through the rule (Eq).

Definition 10 (proof tree) *Given an inference system $\mathcal{I}$, a* proof tree *P of a sequent $T \vdash u$ is a finite tree such that*

- *every leaf of P labeled with $T \vdash v$ is such that $v \in T$,*
- *for every node of P labeled with $T \vdash v$ having n children ($n \geq 0$) labeled with $T \vdash v_1, \ldots, T \vdash v_n$, there is an instance $\dfrac{T \vdash v_1 \quad \ldots \quad T \vdash v_n}{T \vdash v}\,(\mathsf{R})$ of an inference rule of $\mathcal{I}$. If this node labeled with $T \vdash v$ is the root of P then we say that P* ends *with an instance of* (R).
- *the root of P is labeled with $T \vdash u$.*

We say that u is deducible from *T in $\mathcal{I}$ or shortly that $T \vdash u$ in $\mathcal{I}$.*

Note that the terms in the proof are not necessarily ground. The *size* of a proof P, denoted by $|P|$, is the number of nodes in P. A proof P of $T \vdash u$ is *minimal* if there is no proof P' of $T \vdash u$ such that $|P'| < |P|$.

Example 11 *Let $T = \{\{a + \mathsf{h}(\mathsf{h}(b))\}_k,\ k,\ b + \mathsf{h}(b)\}$. The proof P below is a proof of $T \vdash a + b$ in $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUNh})$.*

$$\dfrac{\dfrac{\dfrac{T \vdash \{a + \mathsf{h}(\mathsf{h}(b))\}_k \quad T \vdash k}{T \vdash a + \mathsf{h}(\mathsf{h}(b))}\,(\mathsf{D}) \qquad \dfrac{T \vdash b + \mathsf{h}(b)}{T \vdash \mathsf{h}(b + \mathsf{h}(b))}\,(\mathsf{C}) \qquad T \vdash b + \mathsf{h}(b)}{T \vdash a + \mathsf{h}(\mathsf{h}(b)) + \mathsf{h}(b + \mathsf{h}(b)) + b + \mathsf{h}(b)}\,(\mathsf{C})}{T \vdash a + b}\,(\mathsf{Eq})$$

4.2 Factors and Subterms

A main idea of our procedure consists in separating inference steps involving operators subject to the equational theory E from steps involving only standard Dolev-Yao operators, and then to analyze these steps separately. We hence need some notation that allows us to distinguish the parts of a term belonging to either class of operators.

A term t is *standard* if it is a variable or if it is headed with a function symbol $f \notin sig(\mathsf{E})$. In case of the theory $\mathsf{E} = \mathsf{ACUNh}$, for instance, the terms x, $\langle a, b + c\rangle$ and $\{\mathsf{h}(a)\}_b$ are standard whereas $\mathsf{h}(a)$ and $a + b$ are not.

Definition 12 (factors) *Let t be a term in normal form. We have $t = C[t_1, \ldots, t_n]$ for some standard terms $t_1, \ldots, t_n$ and an E-context C. The set $Fact_{\mathsf{E}}(t)$ of* factors *of t is defined by $Fact_{\mathsf{E}}(t) = \{t_1, \ldots, t_n\}$.*

Example 13 *Let* $\mathsf{E} = \mathsf{ACUNh}$*,* $t_1 = \langle a, b + c\rangle$ *and* $t_2 = \langle a, b\rangle + c$*, we have that* $Fact_{\mathsf{E}}(t_1) = t_1$ *and* $Fact_{\mathsf{E}}(t_2) = \{\langle a, b\rangle, c\}$*. Note that* $Fact_{\mathsf{E}}(t) = \{t\}$ *for any term* t *that is standard.*

Definition 14 (subterms) *The set* $St_{\mathsf{E}}(t)$ *of* subterms *of* t *is the smallest set such that:*

- $t \in St_{\mathsf{E}}(t)$,
- *if* $f(t_1, \ldots, t_n) \in St_{\mathsf{E}}(t)$ *with* $f \notin sig(\mathsf{E})$ *then* $t_1, \ldots t_n \in St_{\mathsf{E}}(t)$,
- *if* $s \in St_{\mathsf{E}}(t)$ *is not standard, i.e. headed with* $f \in sig(\mathsf{E})$ *then we have that* $Fact_{\mathsf{E}}(s) \subseteq St_{\mathsf{E}}(t)$.

These notations are extended as expected to sets of terms. The set $Fact_{\mathsf{E}}(T)$ (resp. $St_{\mathsf{E}}(T)$) is the union of the sets $Fact_{\mathsf{E}}(t)$ (resp. $St_{\mathsf{E}}(t)$) for all terms t occurring in T. Note that, by definition, the factors of any term are necessarily standard. Subterms of a term, however, can be either standard or non-standard.

Example 15 *Let* $\mathsf{E} = \mathsf{ACUNh}$*,* $t_1 = \mathsf{h}^2(a) + b + c$*,* $t_2 = \mathsf{h}(\langle a, b\rangle) + c$ *and* $t_3 = \langle a + b + c, d\rangle$*. We have* $Fact_{\mathsf{E}}(t_1) = \{a, b, c\}$*,* $St_{\mathsf{E}}(t_1) = \{t_1, a, b, c\}$*,* $Fact_{\mathsf{E}}(t_2) = \{\langle a, b\rangle, c\}$*, and* $St_{\mathsf{E}}(t_2) = \{t_2, \langle a, b\rangle, a, b, c\}$*,* $Fact_{\mathsf{E}}(t_3) = \{t_3\}$*, and* $St_{\mathsf{E}}(t_3) = \{t_3, a + b + c, d, a, b, c\}$.

Now, we introduce a notion that will be used in Section 7. Intuitively, a substitution is non-collapsing w.r.t. to a set of terms T if it does not introduce any new equalities between terms in T. This notion will be useful since at one moment in our procedure we will guess all the pairs of non-variable subterms of the problem that will be rendered equal by the solution (provided that a solution exists). After this non-deterministic guessing step we will make use of the assumption that the solution does not render any more subterms equal, that is that the solution is in fact non-collapsing.

Definition 16 (non-collapsing) *A substitution* σ *is* non-collapsing *w.r.t. a set* $T \subseteq \mathcal{T}(\mathcal{F}, \mathcal{X})$ *of terms if for all* $u, v \in St_{\mathsf{E}}(T) \setminus \mathcal{X}$ *such that* $u\sigma =_{\mathsf{E}} v\sigma$*, we have* $u =_{\mathsf{E}} v$.

Example 17 *Let* $\mathsf{E} = \mathsf{ACUNh}$ *and* $T = \{\mathsf{h}(a), \mathsf{h}(\langle a, b\rangle), \mathsf{h}(x)\}$*. We have that* $St_{\mathsf{E}}(T) \setminus \mathcal{X} = T \cup \{\langle a, b\rangle, a, b\}$*. Let* $\sigma_1 = \{x \mapsto a\}, \sigma_2 = \{x \mapsto \langle a, b\rangle\}$*,* $\sigma_3 = \{x \mapsto \langle b, a\rangle\}$ *and* $\sigma_4 = \{x \mapsto b\}$*. The substitutions* σ_1 *and* σ_2 *are collapsing since* $\mathsf{h}(a)\sigma_1 =_{\mathsf{E}} \mathsf{h}(x)\sigma_1$ *and* $\mathsf{h}(\langle a, b\rangle)\sigma_2 =_{\mathsf{E}} \mathsf{h}(x)\sigma_2$*, whereas* $\mathsf{h}(a) \neq_{\mathsf{E}} \mathsf{h}(x)$ *and* $\mathsf{h}(\langle a, b\rangle) \neq_{\mathsf{E}} \mathsf{h}(x)$*. The substitutions* σ_3 *and* σ_4 *are non-collapsing w.r.t.* T.

In the remainder, we assume that the equational theory E can be represented by $\mathcal{R}_\mathsf{E}$, an AC-convergent rewriting system, and we will denote by $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_\mathsf{E})$ the inference system described in Figure 2 and by $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_\mathsf{E})$ the inference system made up of the inference rule $(\mathsf{M_E})$ only. One step in our algorithm will be to separate a proof in the original inference system into a combination of $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_\mathsf{E})$-proofs and of $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_\mathsf{E})$-proofs.

$$\textsf{Unpair. (UL)}\ \frac{T \vdash \langle u, v\rangle}{T \vdash u} \qquad \textsf{Comp. (C}^-\textsf{)}\ \frac{T \vdash u_1\ \ldots\ T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)}\ f \in \mathcal{VF} \setminus sig(\mathsf{E})$$

$$\textsf{Unpair. (UR)}\ \frac{T \vdash \langle u, v\rangle}{T \vdash v} \qquad \textsf{Decrypt. (D)}\ \frac{T \vdash \{u\}_v \quad T \vdash v}{T \vdash u}$$

$$\textsf{Context (M}_\mathsf{E}\textsf{)}\ \frac{T \vdash u_1 \quad \ldots \quad T \vdash u_n}{T \vdash u}\quad \text{where } u = C[u_1, \ldots, u_n]{\downarrow_{\mathcal{R}_\mathsf{E}}} \text{ and } C \text{ is an } \mathsf{E}\text{-context}$$

Figure 2. Inference System $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_\mathsf{E})$.

Equivalence modulo AC is easy to decide, so we omit the equality rule for AC and just work with equivalence classes modulo AC. When the rewriting system is clear from the context, we write $u{\downarrow}$ instead of $u{\downarrow_{\mathcal{R}_\mathsf{E}}}$. More generally, along this paper, we consider implicitly that terms are always kept in normal form, hence we write u (resp. $u\sigma$) instead of $u{\downarrow}$ (resp. $u\sigma{\downarrow}$). This implicit assumption will help us to simplify notation, since otherwise we would have to use equivalence modulo E when applying an inference rule, when computing subterms and factors, and so on.

Example 18 *Let* $\mathsf{E} = \mathsf{ACUNh}$ *and consider the rewriting system* $\mathcal{R}_\mathsf{E}$ *obtained by orienting from left to right the equation* (U), (N) *and* (h) *and by adding the consequence* $\mathsf{h}(0) \to 0$. *Let* $u_1 = a + \mathsf{h}(a)$, $u_2 = \mathsf{h}^3(a) + b$, $C[x_1] = x_1 + \mathsf{h}(x_1) + \mathsf{h}^2(x_1)$ *and* $C'[x_1, x_2] = x_1 + \mathsf{h}(x_1) + \mathsf{h}^2(x_1) + x_2$. *We have that* $C[u_1]{\downarrow_\mathcal{R}} = a + \mathsf{h}^3(a)$ *and* $C'[u_1, u_2]{\downarrow_\mathcal{R}} = a + b$.

The deductive systems $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$ and $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_\mathsf{E})$ deal with symmetric encryption only. However, it is not difficult to design a similar deduction system for asymmetric encryption and to extend the result of this paper to this new inference system. The lemma below states that the systems $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$ and $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_\mathsf{E})$ are equivalent in deductive power.

Lemma 19 *Let $T \subseteq \mathcal{T}(\mathcal{F},\mathcal{X})\downarrow$ and $u \in \mathcal{T}(\mathcal{F},\mathcal{X})\downarrow$. We have:*

$$T \vdash u \text{ in } (\mathcal{I}_{\mathsf{DY}}, \mathsf{E}) \Leftrightarrow T \vdash u \text{ in } (\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$$

PROOF.
($\Leftarrow$) Let P be a proof tree of $T \vdash u$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$. It is easy to obtain a proof tree of $T \vdash u$ in $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$ by replacing normalization steps by some instances of the rule (Eq).

($\Rightarrow$) Let P be a proof tree of $T \vdash u$ in $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$. Let P' be the proof obtained by normalizing all the terms and by removing the application of the rule (Eq). We can show by induction on P that the tree P' obtained is a proof tree of $T \vdash u\downarrow$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$, *i.e.* of $T \vdash u$, since $u = u\downarrow$. □

We now come to the notion of one-step deducibility, that is of deducibility in at most one inference step. This is an important notion, in fact one essential step in analyzing $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ will be reducing deducibility to one-step-deducibility.

Definition 20 (R-one-step deducible) *A term u is* R-one-step deducible *from a set of terms T in any of the following cases:*

- *$T \vdash u$ is a proof of $T \vdash u$ (i.e., $u \in T$),*
- *there exists some terms $u_1, \ldots, u_n$ such that $\dfrac{T \vdash u_1 \quad \ldots \quad T \vdash u_n}{T \vdash u}\,(\mathsf{R})$ is a proof tree of $T \vdash u$.*

Given an inference system $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$, we say that u is *one-step deducible* from T if u is R-one-step deducible from T for some inference rule $\mathsf{R} \in (\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$. We say also that u is DY-*one-step deducible* from T if $\mathsf{R} \in \{\mathsf{C}^-, \mathsf{UL}, \mathsf{UR}, \mathsf{D}\}$. Note that the rule M_{E} does not appear in this set.

Given a set of terms T and a term u, it is easy to decide if u is DY-one-step deducible from T. This can be done in polynomial time since each DY inference rule has a finite set of premises.

One-step deducibility is more difficult to decide in case of the rule M_{E}. However, in the case of monoidal equational theories we will see that M_{E}-one-step deducibility problems can be reduced to solvability of linear equations over the associated semiring. This has already been used for particular equational theories such as ACUN, AG, ACUNh and AGh (see for instance [Che03,Del06a]).

Example 21 *Consider the equational theory $\mathsf{E} = \mathsf{ACUNh}$, $s = a_1 + \mathsf{h}^2(a_1)$ and $T = \{a_1 + \mathsf{h}(a_1) + \mathsf{h}^2(a_1), a_2 + \mathsf{h}^2(a_1), \mathsf{h}(a_2) + \mathsf{h}^2(a_1)\}$ with a_1, a_2 standard terms. The problem of deciding whether s is M_{E}-one-step deducible from T amounts*

to decide whether the following system of equations has a solution over $\mathbb{Z}_2[\mathsf{h}]$.

$$\begin{pmatrix} 1+\mathsf{h}+\mathsf{h}^2 & \mathsf{h}^2 & \mathsf{h}^2 \\ 0 & 1 & \mathsf{h} \end{pmatrix} \cdot Y = \begin{pmatrix} 1+\mathsf{h}^2 \\ 0 \end{pmatrix}$$

The vector $Y = (1+\mathsf{h}, \mathsf{h}, 1)$ *is a solution. Hence,* s *is* $\mathsf{M_E}$*-one-step deducible by using the* E*-context* $x_1 + \mathsf{h}(x_1) + \mathsf{h}(x_2) + x_3$ *where* x_i *is used to denote the* i^{th} *term of* T.

The notion of a decomposition proof will be useful in Subsection 4.4.

Definition 22 (decomposition proof) *A proof tree* P *of* $T \vdash u$ *in* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ *is a* decomposition proof *in any of the following cases:*

- $|P| = 1$,
- P *ends with an instance of a decomposition rule (i.e.* $(\mathsf{UL}, \mathsf{UR}, \mathsf{D})$*),*
- P *ends with an instance of* $(\mathsf{M_E})$ *and* u *is a standard term.*

Example 23 *Let* $\mathsf{E} = \mathsf{ACUNh}$ *and* $T = \{a + \mathsf{h}(a),\ b\}$. *The proof* P *below is a proof of* $T \vdash a + \mathsf{h}(\mathsf{h}(\mathsf{h}(a))) + \mathsf{h}(b)$. *It is made up of an instance of the rule* $(\mathsf{M_E})$ *with* $C = y_1 + \mathsf{h}(y_1) + \mathsf{h}(\mathsf{h}(y_1)) + \mathsf{h}(y_2)$.

$$\frac{T \vdash a + \mathsf{h}(a) \qquad T \vdash b}{T \vdash a + \mathsf{h}(\mathsf{h}(\mathsf{h}(a))) + \mathsf{h}(b)}\ (\mathsf{M_E})$$

Since $a + \mathsf{h}(\mathsf{h}(\mathsf{h}(a))) + \mathsf{h}(b)$ *is not standard,* P *is not a decomposition proof. We have* $|P| = 3$ *and* $a + \mathsf{h}(\mathsf{h}(\mathsf{h}(a))) + \mathsf{h}(b)$ *is* $\mathsf{M_E}$*-one-step deducible from* T *but is not* DY*-one-step deducible from* T *since* $\mathsf{M_E} \notin \{\mathsf{C}^-, \mathsf{UL}, \mathsf{UR}, \mathsf{D}\}$.

4.4 Locality

Now, we can define the notion of locality. This notion, first introduced by McAllester [McA93], allows us to focus on proof trees that involve only some particular terms. This is the foundation of reducing deducibility to one-step deducibility since it allows us, given only the hypotheses and the result of a proof, to guess the intermediate proof steps.

Definition 24 (local inference system) *We say that* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ *is local if each minimal proof tree* P *of* $T \vdash u$ *contains only terms in* $St_{\mathsf{E}}(T \cup \{u\})$. *If moreover* P *is a decomposition proof, then* P *contains only terms in* $St_{\mathsf{E}}(T)$.

This notion of locality has already been studied for numerous inference systems. In particular, some existing results establish locality of the inference system $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ for the equational theories ACUN, AG (see [Che03]) and ACUNh, AGh (see [Del06a]). Actually, we have the following lemma.

Lemma 25 (locality lemma) *Let* E *be an equational theory and* $\mathcal{R}_{\mathsf{E}}$ *be an* AC*-convergent rewriting system representing* E*. If* $sig(\mathsf{E}) \cap \{\langle \_, \_ \rangle, \{\_\}_\_\} = \emptyset$*, then the inference system* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ *is local.*

PROOF. Let T be a set of terms and u a term. Let P be a minimal proof of $T \vdash u$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$. By induction on P, we prove that:

(1) P only contains terms in $St_{\mathsf{E}}(T \cup \{u\})$,
(2) if P is a decomposition proof, then P contains only terms in $St_{\mathsf{E}}(T)$.

We consider all possible cases for the last inference rule of P and we conclude by applying the induction hypothesis (1) or (2). We omit the cases (UL), (UR), (C^-) and (D) which are straightforward. The most interesting case is when the last inference is (M_{E}). We have the following derivation:

$$\dfrac{P_1 \left\{ \dfrac{\cdots}{T \vdash u_1} \right. \quad \cdots \quad P_n \left\{ \dfrac{\cdots}{T \vdash u_n} \right.}{T \vdash C[u_1, \ldots, u_n]} \, (\mathsf{M}_{\mathsf{E}})$$

By (1), each P_i only contains terms in $St_{\mathsf{E}}(T \cup \{u_i\})$. Hence, in order to prove claim (1) we have to show that every u_i is in $St_{\mathsf{E}}(T \cup \{u\})$.

- If u_i is not a standard term (*i.e.* u_i headed with $f \in sig(\mathsf{E})$) then P_i is a decomposition proof since the rule (C^-) only produces standard terms. Furthermore, by minimality of the proof, P_i cannot end on M_{E} since otherwise on could merge the two M_{E} rules. Hence, $u_i \in St_{\mathsf{E}}(T)$ by (2).
- If u_i is standard then let us assume that $u_i \notin St_{\mathsf{E}}(T \cup \{u\})$. This means that $u_i \in Fact_{\mathsf{E}}(u_j)$ for some $j \neq i$. The term u_j must be standard since otherwise we have $u_i = u_j$, and we contradict the minimality of P since a smaller proof could be obtained by replacing the subproof P_i of u_i by a proof of 0. Hence, by induction hypothesis (2) applied to P_j, we deduce that $u_i \in St_{\mathsf{E}}(T)$.

In order to show claim (2) let u be standard. We have $u \in St_{\mathsf{E}}(u_i)$ for some u_i that is not standard. Hence $u_i \in St_{\mathsf{E}}(T)$ and P only contains terms in $St_{\mathsf{E}}(T)$. □

5 Constraint Systems

5.1 Constraint Generation

As mentioned in Section 2, verifying security of a protocol amounts to a non-deterministic guessing of the symbolic trace plus the resolution of a system of *deducibility constraints*.

Definition 26 (deducibility constraint) *A* constraint *(resp. one-step constraint) is a sequent of the form* $T \Vdash u$ *(resp.* $T \Vdash_1 u$*) where* T *is a finite subset of* $\mathcal{T}(\mathcal{F}, \mathcal{X})$ *and* $u \in \mathcal{T}(\mathcal{F}, \mathcal{X})$*. We call* T *(resp.* u*) the* hypothesis set *(resp. the* target*) of the constraint. A* system of constraints *is a sequence of constraints. Given an inference system* $\mathcal{I}$*, a solution of a constraint system* $\mathcal{C}$ *is a substitution* σ *such that:*

- *for every* $T \Vdash u \in \mathcal{C}$*, there exists a proof of* $T\sigma \vdash u\sigma$ *in* $\mathcal{I}$*,*
- *for every* $T \Vdash_1 u \in \mathcal{C}$*,* $u\sigma$ *is one-step deducible from* $T\sigma$ *in* $\mathcal{I}$*.*

Given an inference system $\mathcal{I}$*, we say that a constraint system* $\mathcal{C}$ *is satisfiable if it has a solution w.r.t.* $\mathcal{I}$*.*

5.2 Well-Defined Constraint Systems

The definition stated below is due to J. Millen and V. Shmatikov. In [MS05] they show that "reasonable" protocols, in which legitimate protocol participants only execute deterministic steps (up to the generation of random nonces) always lead to a well-defined constraint system. In the following we will only consider well-defined protocols. This allows us to restrict our attention to well-defined constraint systems.

Definition 27 (well-defined) *A system* $\mathcal{C} = \{T_1 \Vdash u_1, \ldots, T_n \Vdash u_k\}$ *of constraints is* well-formed *if:*

(1) monotonicity*:* $0 \in T_0$ *and for all* $i < k$*, we have that* $T_i \subseteq T_{i+1}$*,*
(2) origination*:* $\forall i \leq k$*,* $\forall x \in vars(T_i)$*,* $\exists j < i$ *such that* $x \in vars(u_j)$*.*

We say that $\mathcal{C}$ *is* well-defined *if for every substitution* θ*,* $\mathcal{C}\theta{\downarrow}$ *is well-formed.*

This notion of well-definedness is defined in a similar way on systems of one-step constraints. Note that this notion depends on the equational theory under consideration.

Example 28 *The constraint system* $\mathcal{C}_1$*, described below, is not well-defined*

w.r.t. the equational theory $\mathsf{E} = \mathsf{ACUN}$. *Indeed, the application of the substitution* $\theta = \{x_2 \to x_1\}$ *on* $\mathcal{C}_1$ *yields a constraint system which is not well-formed.*

$$\mathcal{C}_1 := \begin{cases} 0, a & \Vdash x_1 + x_2 \\ 0, a, x_1 & \Vdash x_3 \end{cases} \qquad \mathcal{C}_1\theta := \begin{cases} 0, a & \Vdash 0 \\ 0, a, x_1 & \Vdash x_3 \end{cases}$$

The following constraint system $\mathcal{C}_2$*, however, is well-defined:*

$$\mathcal{C}_2 := \begin{cases} 0, a & \Vdash \langle x_1, x_2 \rangle \\ 0, a, x_1 & \Vdash x_3 \end{cases}$$

The remainder of this paper deals with the design of a procedure to solve well-defined constraints systems under some additional restrictions on the theory E, and to the proofs of soundness, completeness and termination.

Our procedure proceeds by several successive simplification steps. The steps described in Sections 6 and 7 allow us to reduce our problem to the satisfiability of constraint systems in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$. Note that, in the case of the empty equational theory, the inference system $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ is empty. Hence, as a consequence, we have that a well-defined constraint system is satisfiable in $(\mathcal{I}_{\mathsf{DY}}, \emptyset)$ if, and only if, the empty constraint system can be obtained by applying the (non-deterministic) procedure described in Sections 6 and 7.

Then, in Section 8, we reduce the satisfiability of constraint systems in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ to the satisfiability of constraint systems over a signature containing only symbols of $sig(\mathsf{E})$ and constants. After this step, we establish our first Theorem (Theorem 42) allowing us to deal with monoidal theories for which the associated semiring is finite. Finally, in Sections 9 and 10, we show how to reduce the search space of solutions to deal with the case where the associated semiring is infinite.

6 Existence of Conservative Solutions

The completeness of our decision procedure is ensured by the existence of a *conservative* solution (Lemma 30), which means intuitively that the solution does not introduce any new structure structural elements that are not already present in the constraint system. Moreover, conservative solutions allow us to lift the notion of locality (see Lemma 34 below).

Definition 29 (conservative) *Let* $\mathcal{C}$ *be a constraint system and* σ *a substitution,* σ *is* conservative *w.r.t.* $\mathcal{C}$ *if and only if for all* $x \in vars(\mathcal{C})$*, we*

have $Fact_{\mathsf{E}}(x\sigma) \subseteq (St_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C}))\sigma$.

Lemma 30 *Assume that* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ *is a local inference system. Let* $\mathcal{C}$ *be a well-defined constraint system. If there exists a solution* σ *to* $\mathcal{C}$ *in* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ *then there exists a conservative one.*

The proof of Lemma 30 is rather classical [RT03,MS05] and is detailed in Appendix A.

We will use this lemma in order to show the completeness of several steps of our algorithm (see Lemma 35 and Lemma 39 in Section 7, and Lemma 41 in Section 8).

Example 31 *Let* $\mathsf{E} = \mathsf{ACUNh}$. *Consider the following well-defined constraint system* $\mathcal{C}$*:*

$$0, a, \mathsf{h}(b) \quad \Vdash \mathsf{h}(x)$$
$$0, a, \mathsf{h}(b), x \Vdash \langle a, b\rangle$$

The solution $\sigma = \{x \mapsto \langle a, a\rangle + b\}$ *is not conservative w.r.t.* $\mathcal{C}$. *Indeed* $Fact_{\mathsf{E}}(\langle a, a\rangle + b) = \{\langle a, a\rangle, b\}$, *and* $\langle a, a\rangle$ *does not belong to* $(St_{\mathsf{E}}(\mathcal{C}) \setminus \{x\})\sigma$ *which is equal to* $\{0, \mathsf{h}(b), b, \mathsf{h}(\langle a, a\rangle + b), \langle a, b\rangle, a\}$. *However, as it is said in Lemma 30, there is a conservative solution:* $\{x \mapsto b\}$.

Proposition 32 *Let* t *be a term and* σ *a substitution. We have:*

$$St_{\mathsf{E}}(t\sigma) \subseteq St_{\mathsf{E}}(t)\sigma \cup \bigcup_{x \in vars(t)} St_{\mathsf{E}}(x\sigma)$$

The proof is straightforward. Obviously, the proposition above can be extended to any set of terms. Note, however, that the inclusion may be strict.

Example 33 *Let* $\mathsf{E} = \mathsf{ACUNh}$, $t = x + y$ *and* $\sigma = \{x \mapsto a; y \mapsto a\}$. *We have* $St_{\mathsf{E}}(t\sigma) = \{0\}$ *whereas* $St_{\mathsf{E}}(t)\sigma \cup St_{\mathsf{E}}(\{x\sigma, y\sigma\}) = \{0, a\}$.

The following lemma states a lifting of the Locality Lemma 25 to the solutions of constraint systems.

Lemma 34 *Assume that* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ *is a local inference system. Let* σ *be a conservative solution of* $\mathcal{C} = \{C_1, \ldots, C_k\}$. *For each* $i \leq k$, *there exists a proof* P_i *of* $C_i\sigma$ *which involves only terms in* $St_{\mathsf{E}}(\mathcal{C})\sigma$.

The proof is given in Appendix A.

7 From Satisfiability in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ to Satisfiability in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$

We reduce the satisfiability of a constraint system in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ to the satisfiability of a constraint system in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$ in two steps :

(1) Firstly, we reduce our problem to the satisfiability of one-step constraints in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ (Lemma 35).
(2) Secondly, we reduce the satisfiability of one-step constraint systems to the satisfiability of constraint systems in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$ (Lemma 39).

To perform these two steps, some conditions on the equational theory E are required. These conditions are formally stated in each lemma.

The non-deterministic algorithm described below allows us to reduce the satisfiability of a system of constraints to the satisfiability of a system of one-step constraints. First, we guess among the subterms of $\mathcal{C}$ those which are going to be deduced by the intruder and insert all deducible subterms in the constraint system. The completeness of this step of the procedure is essentially due to the existence of a conservative solution (Lemma 30) and the lifting locality lemma (Lemma 34). In the resulting constraint system, every constraint can be solved by application of a single inference rule.

```
Input: C = {T_1 ⊩ u_1, ... , T_k ⊩ u_k}.
Output: C'.
Algorithm:
  choose S ⊆ St_E(C).
  for all s ∈ S, choose j(s) ∈ {1, ..., k}.
  C' := ∅.
  S_0 := ∅ .
  for i = 1 to k do
     let S_i := {s | j(s) = i}.
     choose a total ordering on S_i (S_i = {s_i^1, ... , s_i^ki}).
     for j = 1 to ki do
     T := T_i ∪ S_0 ∪ ... ∪ S_{i-1} ∪ {s_i^1, ... , s_i^{j-1}}.
        C' := C' ∪ {T ⊩_1 s_i^j}.
     end
     C' := C' ∪ {T ⊩_1 u_i}.
  end
  return C'.
```

Algorithm 3. From constraints to one-step constraints.

Lemma 35 *Let $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ be a local inference system and $\mathcal{C}$ be a well-defined system of constraints. Let $\mathscr{C}'$ be the set of all constraint systems obtained by applying Algorithm 3 on $\mathcal{C}$ (by considering all the possible choices).*

(1) $\mathscr{C}'$ is a finite set of well-defined systems of one-step constraints.
(2) Let $\mathcal{C}' \in \mathscr{C}'$. If σ is a solution to $\mathcal{C}'$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ then σ is a solution to $\mathcal{C}$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$.
(3) If σ is a conservative solution to $\mathcal{C}$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ then there exists $\mathcal{C}' \in \mathscr{C}'$ such that σ is a solution to $\mathcal{C}'$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$.
(4) For any $\mathcal{C}' \in \mathscr{C}'$, σ is conservative w.r.t. $\mathcal{C}$ if and only if σ is conservative w.r.t. $\mathcal{C}'$.

The proof is given in Appendix C. The essential part of the proof is the completeness assertion stated in item (3). The main idea of the proof is to use the lifting locality Lemma 34 which justifies that we do not loose completeness when we choose the intermediate proof steps from the subterms of the constraint system.

The completeness of the following step of our procedure relies on the notion of a non-collapsing solution (see Definition 16). In order to use completeness assertions for non-collapsing solutions to show overall completeness of our algorithm, we guess the equalities between terms, and for each guess of equations, we compute a finite and complete set of unifiers. Furthermore, we need to ensure that the unifiers obtained do not introduce "new structural elements" not already present in the constraint system. Otherwise, we would have to deal with the new equalities introduced after application of the unifier.

Definition 36 (P-conservative) *Let P be a general unification problem modulo a monoidal theory E. A solution θ to P is called* P-conservative *if*

$$St_{\mathsf{E}}(img(\theta)) \setminus \mathcal{X} \subseteq St_{\mathsf{E}}(P)\theta \cup \{0\}.$$

In other words, θ is P-conservative if
$\forall x \in dom(\theta), \forall v \in St_{\mathsf{E}}(x\theta) \setminus \{\mathcal{X} \cup \{0\}\}, \exists t \in St_{\mathsf{E}}(P)$ such that $v =_{\mathsf{E}} t\theta$.

Definition 37 (unification property) *Let E be an equational theory, we say that E satisfies the* unification property *if there exists an algorithm which for any general unification problem P decides whether it has a solution, and in this case computes a complete and finite set $mgu_{\mathsf{E}}(P)$ of unifiers of P which are P-conservative.*

Proposition 38 *Let E be a monoidal equational theory which is unitary for elementary unification, and such that there is an algorithm to compute solutions of inhomogeneous linear equations over the associated semiring $\mathcal{S}_{\mathsf{E}}$. Then E satisfies the unification property.*

Existence of an algorithm to solve general unification problems under the stated conditions is due to F. Baader and W. Nutt [BN96]. Their algorithm is based on the algebraic characterization of unification in monoidal equational theories [Nut90], and the general combination procedure of [BS96]. A proof that the most-general unifiers obtained in that way are P-conservative is given in Appendix B. Note that several monoidal theories considered in this paper satisfy the hypothesis of Proposition 38 (see Section 12).

Lemma 39 allows us to reduce the satisfiability of a system of one-step constraints in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ to the satisfiability of a constraint system in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$. We first guess a set of equalities between subterms and thus obtain a unification problem. We require that there is a finite and complete set of solutions. We apply the unifier to the constraint system. Then, the one-step constraints that can be solved by the application of a standard inference rule, *i.e.* (D), (UL), (UR) and (C^-) can be determined by syntactic inspection. Hence, we can eliminate all constraints that can be satisfied by a single application of an inference rule other than ($\mathsf{M_E}$). We obtain a constraint system that we have to solve in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$.

Lemma 39 *Let* E *be an equational theory for which general unification is decidable and finitary and let* $\mathcal{C}$ *be a well-defined system of one-step constraints. Let* $\mathcal{P} = \{\bigwedge_{(s_1,s_2)\in S'} s_1 = s_2 \mid S' \subseteq St_E(\mathcal{C})^2\}$. *Let* $R \in \mathcal{P}$ *and* $\theta \in mgu_{\mathsf{E}}(R)$. *Let* $\mathcal{C}_\theta = \{T\theta \Vdash u\theta \mid T \Vdash_1 u \in \mathcal{C}$ *and* $u\theta$ *is not* DY*-one-step deducible from* $T\theta\}$.

(1) There are only finitely many outputs (i.e. possibilities for $\mathcal{C}_\theta$*) for a given input* $\mathcal{C}$. *Each of them is a well-defined system of constraints.*
(2) If there exists $\mathcal{C}_\theta$ *(obtained by the procedure above) which has a solution in* $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$ *then* $\mathcal{C}$ *has a solution in* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$.
(3) If $\mathcal{C}$ *has a conservative solution in* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ *then there exists* $\mathcal{C}_\theta$ *(obtained by the procedure above) which has a solution in* $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$. *Moreover, if* E *satisfies the unification property then* $\mathcal{C}_\theta$ *has a non-collapsing solution.*

Again, the proof is given in Appendix C. The crucial part is the completeness assertion stated in the last item of the lemma. The proof of this step uses the fact that we have covered with the set $\mathcal{P}$ all possible identifications of subterms of the constraint system, and that for each of these identifications there is a finite complete set of unifiers. As a consequence, the solution σ to $\mathcal{C}$ is an instance of one of the unifiers θ, which is in turn a unifier pertaining to the identifications of exactly those terms $u = v$ for which $u\sigma = v\sigma$. We can show (the details are in the proof) that this means that every $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$-proof step on $\mathcal{C}\sigma$ can be imitated on $\mathcal{C}\theta$ (which is in general not a ground system). Hence, only the $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$-constraints of $\mathcal{C}\theta$ remain to satisfy, that is exactly the system $\mathcal{C}_\theta$.

8 Reducing the Signature

In the last section we have seen that the satisfiability of the original constraint system can be reduced to the satisfiability of an $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ constraint system. The latter system, however, still contains "mixed" terms, that is terms that contain both standard and non-standard function symbols. This is a problem since only if the constraint system is "pure" and contains only non-standard function symbols (plus free constant symbols) can we reduce this constraint system into an equation system over $\mathcal{S}_\mathsf{E}$.

This is the subject of this section: We will show in Lemma 41 that we can reduce the satisfiability of constraint systems in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ to the satisfiability of constraint systems over a signature containing only symbols of $sig(\mathsf{E})$ and constants.

Notation. If $\rho : M \to N$ is a replacement, that is a bijection between two finite sets of terms M and N, then we denote for any term t by t^ρ the term obtained by replacing in t any top-most occurrence of a subterm $s \in M$ by $s\rho$. This extends in a natural way to constraint systems, and to substitutions by setting $x(\sigma^\rho) = (x\sigma)^\rho$ for all variables $x \in dom(\sigma)$.

Note that the constraint system obtained after such an abstraction is not necessarily well-defined.

Example 40 *Consider the system $\mathcal{C}$ described below. After application of the abstraction $\rho = [a \mapsto a_1;\ b \mapsto a_2;\ \langle x_1, x_2\rangle \mapsto a_3]$, we obtain the non well-defined system $\mathcal{C}^\rho$ described below.*

$$\mathcal{C} = \begin{cases} a \Vdash \langle x_1, x_2\rangle \\ a, x_1, x_2 \Vdash b \end{cases} \qquad \mathcal{C}^\rho = \begin{cases} a_1 \Vdash a_3 \\ a_1, x_1, x_2 \Vdash a_2 \end{cases}$$

Lemma 41 *Let $\mathcal{C}$ be a constraint system and $F = Fact_\mathsf{E}(\mathcal{C}) \setminus \mathcal{X}$. Let $\mathcal{F}_0$ be a set of new constant symbols of the same cardinality as F and $\rho : F \to \mathcal{F}_0$ a bijection.*

(1) If $\mathcal{C}$ has a non-collapsing solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ then $\mathcal{C}^\rho$ has also a solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$.
(2) If $\mathcal{C}^\rho$ has a solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ then $\mathcal{C}$ has a solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$.

PROOF.

(1) Let σ be a non-collapsing solution to $\mathcal{C}$. For all $v_1, v_2 \in Fact_\mathsf{E}(\mathcal{C}) \setminus \mathcal{X}$ such that $v_1\sigma =_\mathsf{E} v_2\sigma$ we have by definition of non-collapsing solution

that $v_1 =_{\mathsf{E}} v_2$ and hence $v_1^\rho =_{\mathsf{E}} v_2^\rho$. The constraint system $\mathcal{C}\sigma$ is a set of ground constraints that is satisfiable in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$, hence we have also that $(\mathcal{C}\sigma)^\rho$ is satisfiable in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$. Since we have that $(\mathcal{C}\sigma)^\rho = \mathcal{C}^\rho\sigma^\rho$, we easily deduce that σ^ρ is a solution to $\mathcal{C}^\rho$ in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$.

(2) Let σ be a solution to $\mathcal{C}^\rho$ in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$, then $\sigma^{(\rho^{-1})}$ is a solution to $\mathcal{C}$ in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$. □

At this point, we can conclude for monoidal equational theories for which the associated semiring is finite. This allows us to conclude for some equational theories such as ACUN or ACUI (see Section 11) in the following theorem.

Theorem 42 *Let* E *be a monoidal equational theory for which there exists an* AC*-convergent rewriting system such that* $sig(\mathsf{E}) \cap \{\{\_\}_\_, \langle\_,\_\rangle\} = \emptyset$ *and for which the associated semiring* $\mathcal{S}_\mathsf{E}$ *is finite. Then, the problem of deciding whether a well-defined constraint system has a solution in* $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$ *is decidable.*

Note that the theory E is always unitary for unification with constants in case the associated semiring $\mathcal{S}_\mathsf{E}$ is finite [BN96]. We also have a naive algorithm to solve inhomogeneous linear equations over $\mathcal{S}_\mathsf{E}$. This allows us to ensure that E satisfies the unification property (Proposition 38) and gives us an algorithm to verify that some guessed substitution is indeed a solution.

PROOF. By Lemma 25, we have that the inference system $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_\mathsf{E})$ is local. Hence, the procedure described along the first part of this paper allows us to reduce the problem of deciding whether a well-defined constraint system has a solution in $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$ to the problem of deciding whether a constraint system has a solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ on the reduced signature. Indeed, let $\mathcal{C}$ be a well-defined constraint system.

Soundness: Let $\mathcal{C}_1$ be a constraint system obtained by applying the first part of our procedure on $\mathcal{C}$. Let $\mathcal{C}_2$ be the constraint system obtained from $\mathcal{C}_1$ by replacing all factors by different constants. Assume that $\mathcal{C}_2$ has a solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ (on the reduced signature). We deduce, thanks to Lemma 41, that $\mathcal{C}_1$ has a solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$, and by Lemma 35 and 39 that $\mathcal{C}$ has a solution in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_\mathsf{E})$.

Completeness: Assume that σ is a solution to $\mathcal{C}$. Thanks to Lemma 30, we can assume that σ is conservative w.r.t. $\mathcal{C}$. Let $\mathscr{C}'$ be the finite set of well-defined one-step constraint systems obtained by applying Algorithm 3 on $\mathcal{C}$. By Lemma 35, we know that there exists $\mathcal{C}' \in \mathscr{C}'$ such that σ is a conservative solution to $\mathcal{C}'$. By Lemma 39, we know that there exists a constraint system $\mathcal{C}_\theta$ which has a non-collapsing solution. Thanks to Lemma 41, we deduce that $\mathcal{C}_\theta^\rho$ has a solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ on the reduced signature.

Now, thanks to the finiteness of $\mathcal{S}_\mathsf{E}$, it is easy to decide if a constraint system $\mathcal{C}$

has a solution in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$ on the reduced signature. Indeed, we can guess (among a finite number of possibilities) the solution σ, *i.e.* the vector $\phi(x\sigma)$ associated to each variable $x \in \mathcal{C}$. Then, it remains to verify that this solution is indeed a solution. □

If the semiring $\mathcal{S}_{\mathsf{E}}$ is infinite then this argument does not apply since then we have a priori an infinite search space. In the next two sections we will show how we can in some cases restrict the search to a finite search space even when the semiring $\mathcal{S}_{\mathsf{E}}$ is infinite.

9 About Well-Defined Constraint Systems

In Section 10, we give an algorithm to solve constraint systems in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$ (when the associated semiring $\mathcal{S}_{\mathsf{E}}$ is not finite) over the reduced signature. However, our algorithm only deals with well-defined constraint systems. Hence, we need to ensure that the constraint systems obtained after abstraction of factors by constants are well-defined. To obtain this result, we first give another characterization of well-definedness (see Section 9.1). Then, we show that the stability of well-definedness by the abstraction is ensured if we consider *factor-preserving* constraint systems (see Section 9.2).

9.1 Another Characterization of Well-Definedness

In this section, we show that on the reduced signature, well-defined constraint systems can be characterized algebraically. For this, we consider an equational theory for which the associated algebraic structure is a commutative ring. Hence in this section (and also in Section 10) $\mathcal{S}_{\mathsf{E}}$ is assumed to be a commutative ring. Moreover, we consider a constraint system $\mathcal{C}$ of the following form:

$$\mathcal{C} = \begin{cases} t_1, \ldots, t_n \Vdash u_1 \\ t_1, \ldots, t_n, t_{n+1} \Vdash u_2 \\ \ldots \\ t_1, \ldots, t_n, t_{n+1}, \ldots, t_{n+k-1} \Vdash u_k \end{cases}$$

where $u_1, \ldots, u_k, t_1, \ldots, t_{n+k-1}$ are terms built on the full signature and on the set of variables $\mathcal{X} = \{x_1, \ldots, x_p\}$. When we say that $\mathcal{C}$ is a constraint system on the reduced signature, this means that the terms involved in $\mathcal{C}$ are in $\mathcal{T}(\mathcal{F}_0 \cup sig(\mathsf{E}), \mathcal{X})$ where $\mathcal{F}_0$ is the set of new constants of the reduced signature.

Input: $\mathcal{C} = \{T_1 \Vdash u_1, \ldots, T_k \Vdash u_k\}$ and $i \leq k$
Output: L

Algorithm:
 L := $\emptyset$;
 for l = 1 to i do
   if $\{\phi_{\mathcal{X}}(u_l)\} \cup \{\phi_{\mathcal{X}}(u_j) \mid j \in L\}$ is independent then $L := L \cup \{l\}$;
 end
return L.

Algorithm 4. Construction of $L_i(\mathcal{C})$ (indexes of defining constraints).

Note that we assume (w.l.o.g) that the hypotheses (*i.e.* $t_1, \ldots t_{n+i}$) of the $i+1^{th}$ constraint contain exactly one term more than the hypotheses of the i^{th} constraint. This can be achieved by duplicating some terms or by adding some constraints.

We need to introduce a notion of dependency. This notion relies on the standard notion used in linear algebra.

Definition 43 (dependent, independent) *Let $\mathcal{S}$ be a commutative ring. Let $\mathcal{V} = \{\vec{v_1}, \ldots, \vec{v_m}\}$ be a subset of $\mathcal{S}^n$. The set $\mathcal{V}$ is* dependent *if there exist $\{\alpha_1, \ldots, \alpha_m\} \subseteq \mathcal{S}$ such that $\alpha_1, \ldots, \alpha_m$ are not all equal to zero and $\alpha_1 \cdot \vec{v_1} + \ldots + \alpha_m \cdot \vec{v_m} = \vec{0}$. Otherwise $\mathcal{V}$ is* independent.

If the set $\mathcal{V}$ is independent and the set $\mathcal{V} \cup \{\vec{v}\}$ is dependent, then we say that the vector $\vec{v}$ is *dependent from* $\mathcal{V}$.

Example 44 *Let $\mathsf{E} = \mathsf{ACUNh}$. Let $t_1 = a + \mathsf{h}(a) + b + x_1 + \mathsf{h}^3(x_1) + \mathsf{h}^2(x_2)$ and $t_2 = \mathsf{h}(a) + \mathsf{h}(x_1) + x_2$. The vectors $\phi_{\mathcal{X}}(t_1)$ and $\phi_{\mathcal{X}}(t_2)$ associated to the terms t_1 and t_2 are:*

$$\phi_{\mathcal{X}}(t_1) = \begin{pmatrix} 1 + \mathsf{h}^3 \\ \mathsf{h}^2 \end{pmatrix} \qquad \phi_{\mathcal{X}}(t_2) = \begin{pmatrix} \mathsf{h} \\ 1 \end{pmatrix}$$

The vectors $\phi_{\mathcal{X}}(t_1)$ and $\phi_{\mathcal{X}}(t_2)$ are independent. Let $t_3 = \mathsf{h}(a)+b+x_1$, $\phi_{\mathcal{X}}(t_3) = (1, 0)$ is dependent of $\{\phi_{\mathcal{X}}(t_1), \phi_{\mathcal{X}}(t_2)\}$ since $\phi_{\mathcal{X}}(t_3) = \phi_{\mathcal{X}}(t_1) + \mathsf{h}^2 \cdot \phi_{\mathcal{X}}(t_2)$.

We denote by $L_i(\mathcal{C})$ the set of indexes obtained by applying Algorithm 4 on $\mathcal{C}, k$. The set $L(\mathcal{C})$ is equal to $L_k(\mathcal{C})$ and it is called the indexes of *defining constraints*. Let $\mathcal{B}_i(\mathcal{C}) = \{\phi_{\mathcal{X}}(u_j) \mid j \in L_i(\mathcal{C})\}$, and $\mathcal{B}(\mathcal{C}) = \mathcal{B}_k(\mathcal{C})$. By construction of $L_i(\mathcal{C})$, the sets $\mathcal{B}_i(\mathcal{C})$ are independent.

Example 45 *Let $\mathsf{E} = \mathsf{ACUNh}$. We consider the constraint system $\mathcal{C}$ described*

below.

$$\mathcal{C} := \begin{cases} \mathsf{h}(a)+a, b+\mathsf{h}^2(a) & \Vdash \mathsf{h}(x_1)+\mathsf{h}^2(x_2) \\ \mathsf{h}(a)+a, b+\mathsf{h}^2(a), x_1+\mathsf{h}(x_2) & \Vdash x_1+a \\ \mathsf{h}(a)+a, b+\mathsf{h}^2(a), x_1+\mathsf{h}(x_2), \mathsf{h}(x_1)+\mathsf{h}(a) & \Vdash \mathsf{h}(x_1)+\mathsf{h}^2(x_2)+x_1+a \end{cases}$$

Let $u_1 = \mathsf{h}(x_1)+\mathsf{h}^2(x_2)$, $u_2 = x_1+a$ *and* $u_3 = \mathsf{h}(x_1)+\mathsf{h}^2(x_2)+x_1+a$. *We have* $\phi_{\mathcal{X}}(u_1) = (\mathsf{h}, \mathsf{h}^2)$, $\phi_{\mathcal{X}}(u_2) = (1,0)$ *and* $\phi_{\mathcal{X}}(u_3) = (1+\mathsf{h}, \mathsf{h}^2)$, $L(\mathcal{C}) = \{1,2\}$ *and* $\mathcal{B}(\mathcal{C}) = \{\phi_{\mathcal{X}}(u_1), \phi_{\mathcal{X}}(u_2)\}$.

Proposition 46 (new characterization of well-definedness) *Let* $\mathcal{C} = \{T_1 \Vdash u_1, \ldots, T_k \Vdash u_k\}$ *be a constraint system on the reduced signature which satisfies the monotonicity property. The system* $\mathcal{C}$ *is well-defined if and only if for all* $i \leq k$, *for all* $t \in T_i$, *the vector* $\phi_{\mathcal{X}}(t)$ *is dependent of* $\mathcal{B}_{i-1}(\mathcal{C})$.

The proof of this proposition (see Appendix D) relies on the following fact:

Fact 47 *Let* $\mathcal{S}$ *be a commutative ring and* A *be an* $n \times m$ *matrix over* $\mathcal{S}$ *such that the* n *row vectors are independent* ($n \leq m$). *There exists* $Q \in \mathcal{S}$ *such that*

$$\forall b \in \mathcal{S}^n, \exists X \in \mathcal{S}^m \quad A \cdot X = Q \cdot b \tag{1}$$

Such a coefficient Q *is computable as a determinant of the matrix obtained by completing* A *with* $m-n$ *independent row vectors.*

Notation. Let $\mathcal{C}$ be a constraint system, we denote by $Q_{max}(\mathcal{C})$ the element of $\mathcal{S}$ associated to the matrix $\mathcal{B}(\mathcal{C})$.

Example 48 *Consider again the constraint system described in Example 45. We have that* $Q_{max}(\mathcal{C}) = \mathsf{h}^2$.

This algebraic characterization of well-defined constraint systems gives us an algorithm to decide if a given constraint system is well-defined (when $\mathcal{S}_{\mathsf{E}}$ is a commutative ring). However, this characterization allows us to deal with constraint systems on the reduced signature only, and seems not to be generalizable on the full signature. We will show later (*cf.* Lemma 55) that we can still obtain one direction of Proposition 46 on the full signature (and not the other one, see Example 57) and we will use this result to obtain a procedure to decide satisfiability of well-defined constraint systems.

Unfortunately, the constraint systems obtained by abstraction on a well-defined constraint system are not necessarily well-defined (see Example 40). To obtain such a result, *i.e.* the stability of well-definedness under abstraction (*cf.* Proposition 52), we need to restrict ourselves to *factor-preserving* constraint systems. However, as it is stated by Lemma 51, this is not a real restriction, since a well-defined constraint, which has a non-collapsing solution, is necessarily factor-preserving.

Definition 49 (factor-preserving) *A constraint system is* factor-preserving *if for all i, $1 \leq i \leq k$, we have that*

$$Fact_{\mathsf{E}}(u_i) \smallsetminus \mathcal{X} \subseteq \bigcup_{j=1}^{j=n+i-1} Fact_{\mathsf{E}}(t_j).$$

Example 50 *The constraint system $\mathcal{C}$ in Example 40 is* not *factor-preserving since the factor $\langle x_1, x_2 \rangle$ does not satisfy the required property.*

Lemma 51 *If a well-defined constraint system $\mathcal{C}$ has a non-collapsing solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ then it is factor-preserving.*

Proposition 52 *Let $\mathcal{C}$ be a well-defined and factor-preserving constraint system. Let $F = Fact_{\mathsf{E}}(\mathcal{C}) \smallsetminus \mathcal{X}$. Let $\mathcal{F}_0$ be a set of new constant symbols of the same cardinality as F and $\rho : F \to \mathcal{F}_0$ a bijection. The system $\mathcal{C}^\rho$ is a well-defined constraint system.*

Before proving this result, we need to introduce some notions and to establish an intermediate lemma (*cf.* Lemma 55).

Definition 53 (non-standard subterms) *The set of* non-standard subterms *$NSt_{\mathsf{E}}(t)$ of a term t is*

$$\begin{array}{lll} NSt_{\mathsf{E}}(f(t_1, \ldots, t_n)) & = \bigcup_{i=1}^{n} NSt_{\mathsf{E}}(t_i) & \text{if } f \notin sig(\mathsf{E}) \\ NSt_{\mathsf{E}}(t) & = \{t\} \cup \bigcup_{s \in Fact_{\mathsf{E}}(t) \smallsetminus \mathcal{X}} NSt_{\mathsf{E}}(s) & \text{otherwise} \end{array}$$

Example 54 *Let t be the term $\mathsf{h}(x_1) + x_2 + \langle x_3, x_4 + x_5 \rangle$. We have that $NSt_{\mathsf{E}}(t) = \{t, x_3, x_4 + x_5\}$.*

Lemma 55 *Let $\mathcal{C} = \{T_1 \Vdash u_1, \ldots, T_k \Vdash u_k\}$ be a factor-preserving and well-defined constraint system (on the full signature) and $1 \leq i \leq k$. We have that: for all $s \in NSt_{\mathsf{E}}(T_i)$, the vector $\phi_{\mathcal{X}}(s)$ is dependent from $\mathcal{B}_{i-1}(\mathcal{C})$.*

This Lemma is proved in Appendix D.

Example 56 *Consider the equational theory* $\mathsf{E} = \mathsf{ACUNh}$ *and the following constraint system* $\mathcal{C}$*:*

$$\mathcal{C} := \begin{cases} 0, a \Vdash x_1 + x_2 \\ 0, a, b \Vdash x_1 \\ 0, a, b, \langle \mathsf{h}(x_1), a\rangle + \langle \mathsf{h}(x_2), a\rangle \Vdash a + b \end{cases}$$

This system is well-defined and factor-preserving. We have $L(\mathcal{C}) = \{1, 2\}$*,* $\phi_{\mathcal{X}}(u_1) = (1, 1)$ *and* $\phi_{\mathcal{X}}(u_2) = (1, 0)$*. We have* $NSt_{\mathsf{E}}(\langle \mathsf{h}(x_1), a\rangle + \langle \mathsf{h}(x_2), a\rangle) = \{\langle \mathsf{h}(x_1), a\rangle + \langle \mathsf{h}(x_2), a\rangle; \mathsf{h}(x_1); \mathsf{h}(x_2)\}$*. The vectors* $(0, 0)$ *(resp.* $(\mathsf{h}, 0)$ *and* $(0, \mathsf{h})$*) are dependent from* $\{(1, 1), (1, 0)\}$*.*

Note that, contrary to what happens on the reduced signature (see Proposition 46), the converse of Lemma 55 is false.

Example 57 *Consider the equational theory* ACUNh *and the following constraint system made up of the constraints* $a \Vdash x + y + \{y\}_k$ *and* $a, x \Vdash a$*. This system is not well-defined* ($\theta = \{x \mapsto y + \{y\}_k\}$)*. However,* $\phi_{\mathcal{X}}(x) = (1, 0)$ *is dependent from* $\{\phi_{\mathcal{X}}(u) \mid u \in \{x + y + \{y\}_k,\ y\}\} = \{(1, 1), (0, 1)\}$*.*

PROOF. (of Proposition 52)
Let $\mathcal{C} = \{T_1 \Vdash u_1, \ldots, T_k \Vdash u_k\}$. By hypothesis, $\mathcal{C}$ is a well-defined and factor-preserving constraint system. By Lemma 55, we know that for all $i \leq k$ and for all $s \in NSt_{\mathsf{E}}(T_i)$, the vector $\phi_{\mathcal{X}}(s)$ is dependent of $\mathcal{B}_{i-1}(\mathcal{C})$. Since for all terms t, we have $\phi_{\mathcal{X}}(t) = \phi_{\mathcal{X}}(t^{\rho})$, we conclude by applying Proposition 46. □

10 Satisfiability in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$ over the Reduced Signature

Now, we have to solve well-defined constraint systems in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$ on the reduced signature. In the remainder, we consider a constraint system $\mathcal{C}$ of the following form:

$$\mathcal{C} = \begin{cases} t_1, \ldots, t_n \Vdash u_1 \\ t_1, \ldots, t_n, t_{n+1} \Vdash u_2 \\ \ldots \\ t_1, \ldots, t_n, t_{n+1}, \ldots, t_{n+k-1} \Vdash u_k \end{cases}$$

with $u_1, \ldots, u_k, t_1, \ldots, t_{n+k-1} \in \mathcal{T}(\mathcal{F}_0 \cup sig(\mathsf{E}), \mathcal{X})$ where $\mathcal{X} = \{x_1, \ldots, x_p\}$.

To deal with the case of an infinite semiring we need to assume that $\mathcal{S}_{\mathsf{E}}$ satisfies some additional properties. In particular, we have to assume that $\mathcal{S}_{\mathsf{E}}$ is an Euclidean ring as defined below.

Definition 58 (Euclidean ring) *An* Euclidean ring *is a commutative ring:*

- *without zero divisors, i.e.*

$$\forall x, y \in \mathcal{S} \text{ if } x \cdot y = 0 \text{ then } x = 0 \text{ or } y = 0$$

- *in which a division algorithm can be defined, i.e. there is a function* $v : \mathcal{S} \setminus \{0\} \to \mathbb{N}$*, called* norm*, that satisfies the following property:*

$$\forall a, b \in \mathcal{S} \text{ with } b \neq 0, \exists q, r \in \mathcal{S} \text{ such that } \begin{cases} a = bq + r, \text{ and} \\ r = 0 \text{ or } v(r) < v(b). \end{cases}$$

Example 59 *The ring* $\mathbb{Z}$ *is an Euclidean ring, where division is defined as the usual integer division with remainder, and the function* v *is the absolute value. For any field* K*, the ring* $K[\mathsf{h}]$ *of polynomials is an Euclidean ring, where* $v(p)$ *is the degree of a polynomial* p*.*

Let E be a monoidal theory. If $t_1, \ldots, t_n \vdash t$ in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$, that is by one step of the inference rule M_{E}, then we call an *instance* of this rule the context C such that $C[t_1, \ldots, t_n] = t$. Recall that, as always, equalities between terms are modulo the equational theory E.

Let $\mathcal{C}$ be a well-defined constraint system in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$ on the reduced signature as given at the beginning of this section. If σ is a solution to $\mathcal{C}$ then we denote by $C_1^\sigma, \ldots, C_k^\sigma$ the instances of the M_{E} rules, that is the contexts such that

$$C_i^\sigma[t_1, \ldots, t_n, t_{n+1}\sigma \ldots, t_{n+i-1}\sigma] = u_i\sigma$$

Note that $t_j\sigma = t_j$ for $j \leq n$ since the $t_1, \ldots, t_n$ are ground. We denote by $\mathcal{Y} = \{y_1, \ldots, y_{n+k-1}\}$ a set of variables disjoint from $\mathcal{X}$ on which the contexts C_i^σ are built. By construction, $vars(C_i^\sigma) \subseteq \{y_1, \ldots, y_{n+i-1}\}$. We also say that $C_1^\sigma, \ldots, C_k^\sigma$ are *witnesses* of the solution σ.

Proposition 60 *Let* E *be a monoidal equational theory for which* $\mathcal{S}_{\mathsf{E}}$ *is an Euclidean ring with norm* v*. If* $\mathcal{C}$ *is satisfiable, then there exists a solution* σ *to* $\mathcal{C}$ *with witnesses* $C_1^\sigma, \ldots, C_k^\sigma$ *satisfying the following condition:*

$$\text{for all } i \in L(\mathcal{C}), \text{ for all } y \in \mathcal{Y}, v(\phi_y(C_i^\sigma)) = 0 \text{ or } v(\phi_y(C_i^\sigma)) < v(Q_{max}(\mathcal{C})).$$

Note that if we view the constraint system $\mathcal{C}$ as an equation system over the semiring $\mathcal{S}_{\mathsf{E}}$ then what we obtain is a *quadratic* equation system since we have on the left-hand side of the equation system products between terms corresponding to the instances of the rule $(\mathsf{M}_{\mathsf{E}})$ (*i.e.*, the witnesses C_i^σ) on the

one hand, and terms corresponding to the messages (*i.e.*, the instances of the terms t_i) on the other hand. The idea of the proof is that we can re-balance a solution σ when C_i^σ is too big in the following sense: If C_i^σ is the context applied to a term t_i then we can shift a chunk of the solution to t_i, that is we make C_i^σ smaller and $t_i\sigma$ larger. The fact that $\mathcal{S}_{\mathsf{E}}$ is an Euclidean ring makes this shifting operation possible, and by exploiting the fact that the constraint system is well-defined we can assure that this shifting does not change the evaluation of the left-hand side of the equation system. The complete proof of this proposition is given in Appendix E.

Input: $\mathcal{C} = \{t_1, \ldots, t_n \Vdash u_1; \ \ldots \ ; t_1, \ \ldots, \ t_n, \ \ldots, t_{n+k-1} \Vdash u_k\}$
Output: Yes/No

Algorithm:
  for all $i \in L(\mathcal{C})$ do
    for all $j := 1$ to $n + i - 1$ do
      choose the value of $\phi_{y_i}(C_i)$ among $\{e \in \mathcal{S}_{\mathsf{E}} | v(e) < v(Q_{max}(\mathcal{C}))\} \cup \{0\}$

  $\mathcal{U} := \emptyset$
  for all $i \in L(\mathcal{C})$ do $\mathcal{U} := \mathcal{U} \cup \{C_i[t_1, \ \ldots, \ t_{n+i-1}] = u_i\}$

  if $\mathcal{U}$ has no solution return No

  let θ a solution to $\mathcal{U}$
  for all $i \notin L(\mathcal{C})$ do
    if $u\theta$ is not M_{E}-one-step deducible from $T\theta$
    return No

  return Yes

Algorithm 5. Satisfiability of a well-defined constraint system in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$.

Proposition 61 *Let* E *be a monoidal equational theory that is unitary for elementary unification, and such that* $\mathcal{S}_{\mathsf{E}}$ *is an Euclidean ring with norm* v *with*

$$\textit{for any } q \in \mathcal{S}_{\mathsf{E}}, \textit{ the set } \{e \in \mathcal{S}_{\mathsf{E}} \mid v(e) < v(q)\} \textit{ is finite}$$

and such that there is an algorithm to compute solutions of inhomogeneous linear equation over $\mathcal{S}_{\mathsf{E}}$*. Then algorithm 5 allows us to decide the satisfiability of a well-defined constraint system* $\mathcal{C}$ *(on the reduced signature) in* $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$*.*

11 Main Results

We have already stated and proved the following result.

Theorem 42 *Let* E *be a monoidal equational theory for which there exists an* AC*-convergent rewriting system such that* $sig(\mathsf{E}) \cap \{\{\_\}\_, \langle \_, \_ \rangle\} = \emptyset$ *and for which the associated semiring* $\mathcal{S}_{\mathsf{E}}$ *is finite. Then, the problem of deciding whether a well-defined constraint system has a solution in* $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$ *is decidable.*

Now, we can go further since in some cases, we can deal with monoidal equational theory for which the associated semiring is not finite.

Theorem 62 *Let* E *be a monoidal equational theory for which there exists an* AC*-convergent rewriting system such that* $sig(\mathsf{E}) \cap \{\{\_\}\_, \langle \_, \_ \rangle\} = \emptyset$*, and such that:*

(1) the associated semiring $\mathcal{S}_{\mathsf{E}}$ *is an Euclidean ring and the function* v *used in the Euclidean division algorithm satisfies the following condition:*
for any $q \in \mathcal{S}_{\mathsf{E}}$*, the set* $\{e \in \mathcal{S}_{\mathsf{E}} \mid v(e) < v(q)\}$ *is finite.*
(2) the theory E *is unitary for elementary unification, and there is an algorithm to compute solutions of inhomogeneous linear equations over the associated semiring* $\mathcal{S}_{\mathsf{E}}$*.*

Then, the problem of deciding whether a well-defined constraint system has a solution in $(\mathcal{I}_{\mathsf{DY}}, \mathsf{E})$ *is decidable.*

PROOF. First, the procedure described along the first part of this paper allows us to reduce the problem of deciding whether a well-defined constraint system has a solution in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ to the problem of deciding whether a well-defined constraint system has a solution in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$ on the reduced signature. This is similar to the proof of Theorem 42. However, note that we obtain a well-defined constraint system after abstraction thanks to Lemma 51 and Proposition 52.

Second, thanks to Proposition 61, we know that the problem of deciding whether a well-defined constraint system has a solution in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$ on the reduced signature is decidable. □

The complexity of the insecurity problem for these theories is not settled yet, and probably depends on the particular equational theory under consideration. Although the proofs of correctness are complicated, the algorithm itself is simple enough: apart from the guessing steps, the most complex operations

are unification and the resolution of a system of linear equations. Therefore, the whole process may be in NP at least for the monoidal theories E such that the semiring $\mathcal{S}_{\mathsf{E}}$ is finite, provided one uses structure sharing, like it is the case in the empty equational theory.

12 Application to Particular Monoidal Theories

In this section we show that several interesting monoidal equational theories satisfy the conditions allowing us to apply either Theorem 42 or Theorem 62. A summary is given in Figure 6.

12.1 The Theories $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUI})$ *and* $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUN})$ *(Exclusive Or)*

These equational theories are made up of the axioms (AC) and (U) with in addition $x+x = x$ (I) or $x+x = 0$ (N). The semirings corresponding to these equational theories are respectively the Boolean semiring $\mathbb{B}$, which is finite, and the finite field $\mathbb{Z}_2$. Theorem 42 allows us to conclude that the problem whether a well-defined constraint system has a solution in $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUI})$ (resp. $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUN})$) is decidable.

12.2 The Theory $(\mathcal{I}_{\mathsf{DY}}, \mathsf{AG})$ *(Abelian Groups)*

This well-known equational theory is made up of the axioms (AC) and (U) with in addition $x + -(x) = 0$ (Inv). The semiring associated to this equational theory is in fact a ring, namely the ring $\mathbb{Z}$ of all integers. This ring is an Euclidean ring. We can define the function v as $|n|$, the absolute value of n. Hence we have the property that the set $\{e \in \mathbb{Z} \mid v(e) < v(q)\}$ is finite, for any $q \in \mathbb{Z}$. Moreover, it is a well-known result [BS01] that elementary unification modulo AG is unitary. Lastly, there exist several algorithms to compute solutions of linear equations over $\mathbb{Z}$ (see for instance [Sch86]). Hence, Theorem 62 allows us to conclude that the problem of deciding whether a well-defined constraint system has a solution in $(\mathcal{I}_{\mathsf{DY}}, \mathsf{AG})$ is decidable.

12.3 The Theory $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUNh})$

This equational theory is made up of the axioms of ACUN with in addition $\mathsf{h}(x + y) = \mathsf{h}(x) + \mathsf{h}(y)$. The semiring associated to ACUNh is $\mathbb{Z}_2[\mathsf{h}]$, the ring of polynomials in one indeterminate over $\mathbb{Z}_2$. As $\mathbb{Z}_2$ is a field, we have that

$\mathbb{Z}_2[\mathsf{h}]$ is an Euclidean ring. The norm we consider for polynomials is the degree, and thus, the extra condition on v is satisfied. Elementary unification modulo ACUNh has been shown unitary in [LLT06] and the authors also provide an algorithm to compute solutions of linear equations over $\mathbb{Z}_2[\mathsf{h}]$. Hence, by applying Theorem 62, we conclude that the problem of deciding whether a well-defined constraint system has a solution in $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUNh})$ is decidable.

13 Monoidal Theories Not Covered by Our Results

In this section, we briefly discuss some equational theories which do not fulfill all the required conditions allowing us to apply Theorem 42 or Theorem 62.

13.1 The Theory $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUh})$

The equational theory ACUh is known to have an undecidable unification problem [Nar96]. This result had been obtained by using the fact that solvability of linear equations over the semiring $\mathbb{N}[\mathsf{h}]$ is undecidable. Hence, Theorem 62 can not be applied. It is not surprising that our theorem can not handle this case since it is well-known that decidability of unification is a necessary condition for decidability of the security property of protocols [CDL06].

13.2 The Theory $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACUIh})$

The equational theory ACUIh is made up of the axioms of ACUI with in addition $\mathsf{h}(x + y) = \mathsf{h}(x) + \mathsf{h}(y)$ and $\mathsf{h}(0) = 0$. The semiring associated to ACUIh is $\mathbb{B}[\mathsf{h}]$, the semiring of polynomial in one indeterminate over $\mathbb{B}$. This semiring is neither finite nor a ring. Moreover, elementary unification is of type 0 [BS01], *i.e.* a minimal complete set of unifiers does not always exists. However, general unification is decidable, as a consequence of the fact that solvability of unification problems with constants is decidable [BS01] and of the combination result obtained in [BS96].

13.3 The Theory $(\mathcal{I}_{\mathsf{DY}}, \mathsf{AGh})$

Contrary to the equational theory ACUh, the equational theory AGh is known to have a decidable unification problem [Baa93]. The semiring corresponding to this equational theory is the ring $\mathbb{Z}[\mathsf{h}]$. However, this ring is neither finite, nor an Euclidean ring. Hence, we can not apply neither Theorem 42,

nor Theorem 62. Actually, it has recently been shown [Del06b] that the problem of deciding whether a well-defined constraint system has a solution, is undecidable for this equational theory.

13.4 The Theory $(\mathcal{I}_{\mathsf{DY}}, \mathsf{ACU})$

This equational theory, which is the simplest monoidal equational theory, seems to be challenging. The semiring corresponding to this equational theory is the semiring $\mathbb{N}$ which is neither finite nor a ring. Hence our results do not allow us to conclude. Actually, decidability of the problem whether a well-defined constraint system modulo the theory ACU has a solution is still open. The problem has so far only been partially solved [BCD07].

13.5 Monoidal Theories with Several Homomorphisms

Another issue is to consider several homomorphic symbols that may or may not commute (besides the *inversion* operation of Abelian Groups). In the non-commuting case, unification is solved by a Gröbner basis approach in non-commutative algebra [Baa93] and this question is likely to be difficult. The commutative case seems more tractable, but there is not yet any decidability result for this case.

Theory E	$\mathcal{S}_{\mathsf{E}}$	Properties of $\mathcal{S}_{\mathsf{E}}$	Element. Unificat.	Constraints
ACUI	$\mathbb{B}$	finite semiring	unitary	decidable
ACUN	$\mathbb{Z}_2$	finite semiring	unitary	decidable
AG	$\mathbb{Z}$	Euclidean ring	unitary	decidable
ACUNh	$\mathbb{Z}_2[\mathsf{h}]$	Euclidean ring	unitary	decidable
ACUh	$\mathbb{N}[\mathsf{h}]$	semiring	undecidable	undecidable
ACUIh	$\mathbb{B}[\mathsf{h}]$	semiring	type 0	?
AGh	$\mathbb{Z}[\mathsf{h}]$	commutative ring	unitary	undecidable
ACU	$\mathbb{N}$	semiring	unitary	?

Figure 6. Summary of some results.

References

[ALV02] R. Amadio, D. Lugiez, and V. Vanackère. On the symbolic reduction of processes with cryptographic functions. *Theoretical Computer Science*, 290:695–740, 2002.

[AVI] AVISPA Project. The AVISPA tool. Available at http://www.avispa-project.org/.

[Baa93] F. Baader. Unification in commutative theories, Hilbert's basis theorem and Gröbner bases. *Journal of the ACM*, 40(3):477–503, 1993.

[Bau05] M. Baudet. Deciding security of protocols against off-line guessing attacks. In *Proc. 12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 16–25, Alexandria, Virginia, USA, 2005. ACM Press.

[BCD07] Sergiu Bursuc, Hubert Comon-Lundh, and Stéphanie Delaune. Associative-commutative deducibility constraints. In Wolfgang Thomas and Pascal Weil, editors, *Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS'07)*, volume 4393 of *Lecture Notes in Computer Science*, pages 634–645, Aachen, Germany, February 2007. Springer.

[Bla01] B. Blanchet. An efficient cryptographic protocol verifier based on Prolog rules. In *Proc. 14th IEEE Computer Security Foundations Workshop (CSFW'01)*, pages 82–96. IEEE Comp. Soc., 2001.

[BMV05] D. Basin, S. Mödersheim, and L. Viganò. Algebraic intruder deductions. In *Proc. 12th International Conference on Logic Programming and Automated Reasoning (LPAR'06)*, volume 3835 of *LNAI*, pages 549–564. Springer-Verlag, 2005.

[BN96] 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.

[BS96] F. Baader and K.U. Schulz. Unification in the union of disjoint equational theories: Combining decision procedures. *Journal of Symbolic Computation*, 21:211–243, 1996.

[BS01] F. Baader and W. Snyder. Unification theory. In Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, volume 1, chapter 8, pages 447–533. Elsevier, 2001.

[CD05] H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In *Proc. 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *LNCS*, pages 294–307, Nara (Japan), 2005. Springer.

[CDL06] V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.

[Che03] Y. Chevalier. *Résolution de problèmes d'accessibilité pour la compilation et la validation de protocoles cryptographiques*. PhD thesis, Université Henri Poincaré, Nancy (France), 2003.

[CKR+03] Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, and L. Vigneron. 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.

[CKRT03] Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with XOR. In *Proc. 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03)*, pages 261–270, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.

[CL04] H. Comon-Lundh. Intruder theories (ongoing work). In *Proc. 7th International Conference on Foundations of Software Science and Computation Structures (FOSSACS'04)*, volume 2987 of *LNCS*, pages 1–4, Barcelona (Spain), 2004. Springer.

[CLS03] H. Comon-Lundh and V. Shmatikov. Intruder deductions, constraint solving and insecurity decision in presence of exclusive or. In *Proc. 18th Annual IEEE Symposium on Logic in Computer Science (LICS'03)*, pages 271–280, Ottawa (Canada), 2003. IEEE Comp. Soc. Press.

[CLT03] H. Comon-Lundh and R. Treinen. Easy intruder deductions. In *Verification: Theory & Practice, Essays Dedicated to Zohar Manna on the Occasion of His 64th Birthday*, volume 2772 of *LNCS*, pages 225–242. Springer, 2003.

[CR05] Y. Chevalier and M. Rusinowitch. Combining intruder theories. In *Proc. 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *LNCS*, pages 639–651, Lisbon (Portugal), 2005. Springer.

[CR06] Y. Chevalier and M. Rusinowitch. Hierarchical combination of intruder theories. In *Proc. 17th International Conference on Term Rewriting and Applications, (RTA'06)*, volume 4098 of *LNCS*, pages 108–122. Springer, 2006.

[Del06a] S. Delaune. Easy intruder deduction problems with homomorphisms. *Information Processing Letters*, 97(6):213–218, 2006.

[Del06b] Stéphanie Delaune. An undecidability result for AGh. *Theoretical Computer Science*, 368(1-2):161–167, December 2006.

[DJ90] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 6. Elsevier and MIT Press, 1990.

[DJ04] S. Delaune and F. Jacquemard. A decision procedure for the verification of security protocols with explicit destructors. In *Proc. 11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 278–287, Washington, D.C., USA, 2004. ACM Press.

[DLLT06] S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In *Proc. 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) — Part II*, volume 4052 of *LNCS*, pages 132–141, Venice (Italy), 2006. Springer.

[DLMS04] N. Durgin, P. Lincoln, J. Mitchell, and A. Scedrov. Multiset rewriting and the complexity of bounded security protocols. *Journal of Computer Security*, 2004.

[DY81] D. Dolev and A.C. Yao. On the security of public key protocols. In *Proc. 22nd Symposium on Foundations of Computer Science*, pages 350–357, Nashville (USA, Tennessee), 1981. IEEE Comp. Soc. Press.

[KNW03] D. Kapur, P. Narendran, and L. Wang. An E-unification algorithm for analyzing protocols that use modular exponentiation. In *Proc. 14th International Conference on Rewriting Techniques and Applications (RTA'03)*, LNCS, pages 165–179. Springer, 2003.

[LLT06] P. Lafourcade, D. Lugiez, and R. Treinen. ACUNh: Unification and disunification using automata theory. In *Proc. 20th International Workshop on Unification (UNIF'06)*, pages 6–20, Seattle (USA, Washington), 2006.

[Low96] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. *Software - Concepts and Tools*, 17(3):93–102, 1996.

[McA93] D. A. McAllester. Automatic recognition of tractability in inference relations. *Journal of the ACM*, 40(2):284–303, 1993.

[MM82] A. Martelli and U. Montanari. An efficient unification algorithm. *ACM Transactions on Programming Languages and Systems*, 4(2):258–282, 1982.

[MS05] J. Millen and V. Shmatikov. Symbolic protocol analysis with an Abelian group operator or Diffie-Hellman exponentiation. *Journal of Computer Security*, 13(3):515–564, 2005.

[MT92] K. Meinke and J. V. Tucker. Universal algebra. In S. Abramsky, Dov M.Gabbay, and T. S. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 1, pages 189–411. Oxford Science Publications, 1992.

[MV01] 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)*, pages 166–175. ACM, 2001.

[Nar96] P. Narendran. Solving linear equations over polynomial semirings. In *Proc. 11th Annual IEEE Symposium on Logic in Computer Science (LICS'96)*, pages 466–472, New Brunswick, New Jersey, 1996. IEEE Comp. Soc. Press.

[NS78] R. Needham and M. Schroeder. Using encryption for authentification in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.

[Nut90] W. Nutt. Unification in monoidal theories. In *Proc. 10th International Conference on Automated Deduction, (CADE'90)*, volume 449 of *LNCS*, pages 618–632, Kaiserslautern (Germany), 1990. Springer.

[Pau97] L. Paulson. The inductive approach to verifying protocols. In *10th IEEE Computer Scurity Foundations Workshop*, pages 84–95, 1997.

[RS98] P. Ryan and S. Schneider. An attack on a recursive authentication protocol. A cautionary tale. *Information Processing Letters*, 65(1):7–10, January 1998.

[RT03] 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.

[Sch86] A. Schrijver. *Theory of Linear and Integer Programming.* Wiley, 1986.

[Sim94] G.J. Simmons. Cryptoanalysis and protocol failures. *Communications of the ACM*, 37(11):56–65, 1994.

[ZD04] R. Zunino and P. Degano. Handling exp, $\times$ (and timestamps) in protocol analysis. In *Proc. 9th International Conference on Foundations of Software Science and Computation Structures, (FOSSACS'06)*, volume 3921 of *LNCS*, pages 413–427. Springer, 2004.

Appendix A Conservative Solutions

Definition 63 (decomposed) *Let P be a proof of $T \vdash u$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$. We say that a standard term v is decomposed in P if:*

- *either $v = \langle u_1, u_2 \rangle$ and P contains an instance of (UL) or (UR) whose premise is labeled with $T \vdash \langle u_1, u_2 \rangle$.*
- *or $v = \{u_1\}_{u_2}$ and P contains an instance of (D) whose premises are labeled with $T \vdash \{u_1\}_{u_2}$ and $T \vdash u_2$.*

The following proposition has been proved in [RT03] for the standard Dolev-Yao model. The proof of [RT03] can be transferred in a straightforward way to our intruder model which comprises in addition to the standard rules the

rule ($\mathsf{M_E}$). It will be used in Lemma 30 to ensure the existence of a proof of $T \vdash u$ which respects some conditions.

Proposition 64 *Let P be a proof of $T \vdash u$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ and P' be a minimal proof of $T \vdash \gamma$. Moreover, assume that P' ends with an instance of (C^-). Then, there exists a proof of $T \vdash u$ in which γ is never decomposed.*

PROOF. The proof can be done by induction on the number of instances of inference rules in P which decompose γ. Base case: If there is no such instance then P is the expected proof. Assume there are $n+1$ instances of inference rules in P which decompose γ. We can distinguish two cases depending on whether γ is a pair (*i.e.* $\langle \gamma_1, \gamma_2 \rangle$) or a ciphertext (*i.e.* $\{\gamma_1\}_{\gamma_2}$). In the first case, this means that there exists an instance of (UL) (or (UR)) whose premise is $\langle \gamma_1, \gamma_2 \rangle$ and conclusion is γ_1 (or γ_2). From P', we can easily extract a proof P_1 of $T \vdash \gamma_1$ (resp. P_2 of $T \vdash \gamma_2$). Note that P_1 (resp. P_2) does not decompose γ by minimality of P'. Hence, such a proof can be plugged to replace the subproof of $T \vdash \gamma_1$ (resp. $T \vdash \gamma_2$) in P which decompose γ. The second case where $\gamma = \{\gamma_1\}_{\gamma_2}$ is similar. We obtain a proof of $T \vdash u$ which contains less instances of inference rules which decompose γ than P. Hence we can apply the induction hypothesis to conclude. □

Remember that we consider implicitly that terms are kept in normal forms, hence we write $u\sigma$ instead of $u\sigma{\downarrow}$.

Lemma 30 *Assume that $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ is a local inference system. Let $\mathcal{C}$ be a well-defined constraint system. If there exists a solution σ to $\mathcal{C}$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ then there exists a conservative one.*

PROOF.

We assume given a linear well-founded ordering $\prec$ on standard terms of $\mathcal{T}(\mathcal{F}, \mathcal{X})$ such that a special public constant 0 is minimal w.r.t. $\prec$. We shall use below the multi-set extension $\ll$ of $\prec$ to multi-sets of standard ground terms. For sake of notation, given two solutions σ_1 and σ_2 of a constraint system, we write $\sigma_1 \ll \sigma_2$ if and only if $Fact_{\mathsf{E}}(img(\sigma_1)) \ll Fact_{\mathsf{E}}(img(\sigma_2))$. Let σ be a minimal (w.r.t. $\ll$) solution to $\mathcal{C}$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$.

We reason by contradiction to show that σ is conservative w.r.t. $\mathcal{C}$. Assume that there exists $x \in vars(\mathcal{C})$ and $v_x \in Fact_{\mathsf{E}}(x\sigma)$ such $v_x \notin (St_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C}))\sigma$ *i.e.* for all $t \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \setminus \mathcal{X}$ with $t\sigma =_{\mathsf{E}} v_x$, we have $t \notin St_{\mathsf{E}}(\mathcal{C})$. We will show that under this condition there exists a smaller solution σ' of $\mathcal{C}$. Let

$\mathcal{C} = \{C_1, \ldots, C_k\}$ and for each $i \leq k$, let $T_i \Vdash u_i$ be the constraint C_i and $C_i\sigma$ be the constraint obtained from C_i by instantiating (and normalizing) all the terms with σ.

Fact 65 *If $v_x \in St_{\mathsf{E}}(s\sigma)$ for some $s \in T_i$ $(i \leq k)$, then there exists $j < i$ such that $v_x \in St_{\mathsf{E}}(u_j\sigma)$.*

We show this result by contradiction. Assume that $v_x \in St_{\mathsf{E}}(s\sigma)$ for some $s \in T_i$ $(i \leq k)$, and that for all $j < i$, we have $v_x \notin St_{\mathsf{E}}(u_j\sigma)$. Let z be a fresh variable, and ρ be the replacement $\{v_x \mapsto z\}$. Let $\theta := \sigma\rho$. We are going to show that $\mathcal{C}\theta$ is not well-formed, leading to a contradiction with the fact that $\mathcal{C}$ is well-defined. Firstly, since $v_x \notin (St_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C}))\sigma$, we have $(\mathcal{C}\sigma)\rho = \mathcal{C}(\sigma\rho)$ $(= \mathcal{C}\theta)$. By hypothesis, $v_x \in St_{\mathsf{E}}(T_i\sigma)$, hence $z \in vars(T_i\theta)$. However, for all $j < i$, we have $z \notin vars(u_j\theta)$ since $v_x \notin St_{\mathsf{E}}(u_j\sigma)$.

This allows us to define: $m = \min\{j \mid v_x \in St_{\mathsf{E}}(u_j\sigma)\}$.

Fact 66 *There exists P' a proof tree of $T_m\sigma \vdash v_x$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ which ends with an instance of (C^-).*

By hypothesis, there exists a minimal proof P of $T_m\sigma \vdash u_m\sigma$. Firstly, we show that there exists in P a node labeled with $T_m\sigma \vdash v_x$. If P contains a node labeled by $T_m\sigma \vdash v_x$, then it is the expected node. Otherwise, we can find recursively a path in P, from the root up to one leaf, where every node which is labeled by $T_m\sigma \vdash u$ is such that $v_x \in St_{\mathsf{E}}(u)$. Thanks to Fact 65, the existence of such a path leads to a contradiction with the minimality of m. Secondly, by definition of m and thanks to the fact that the inference system $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ is local, the subproof P' of P labeled with $T_m\sigma \vdash v_x$ can not be a decomposition proof (otherwise $v_x \in St_{\mathsf{E}}(T_m\sigma)$). Since v_x is necessarily a standard term, this implies that P' ends with an instance of (C^-).

Now, we let δ be the replacement $\{v_x \mapsto 0\}$. We will show that $\sigma' := \sigma\delta$ is also a solution of $\mathcal{C}$, which is a contradiction since $\sigma' \ll \sigma$ (v_x is a standard term since it is a factor, hence $0 \prec v_x$). For this purpose, we have to build a proof of each $C_i\sigma'$, $i \leq l$. We distinguish two cases.

(1) Case $i < m$: By definition of m, $v_x \notin St_{\mathsf{E}}(C_i\sigma)$. In this case, $(C_i\sigma)\delta = C_i\sigma = C_i\sigma'$, *i.e.* σ' is a solution to C_i.
(2) Case $i \geq m$: In the remainder, we are going to show that $\sigma' = \sigma\delta$ is also a solution to $C_i = T_i \Vdash u_i$.

Firstly, we may note that $C_i(\sigma\delta) = (C_i\sigma)\delta$ since by hypothesis $v_x \notin (St_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C}))\sigma$. By hypothesis σ is a solution to C_i in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$, this means that we have a proof P of $T_i\sigma \vdash u_i\sigma$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$. Moreover, Fact 66 ensures the

existence of a proof of $T_i\sigma \vdash v_x$ which ends with (C^-) in P. σ' is a solution of $\mathcal{C}_i$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$, it is obvious for $i = m$ and we extend the result for $i > m$ by well-definedness of $\mathcal{C}$ (stability by any substitution that $\mathcal{C}$ is well-formed). Now, we can apply Proposition 64 to obtain a proof P_i of $T_i\sigma \vdash u_i\sigma$ in which v_x is never decomposed. We shall build from P_i a proof P'_i of $(T_i\sigma)\delta \vdash (u_i\sigma)\delta$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ by replacing every subtree ended by $\dfrac{T_i\sigma \vdash v_1 \dots T_i\sigma \vdash v_n}{T_i\sigma \vdash v_x}\,(\mathsf{C}^-)$ with a leaf labeled with $T_i\sigma \vdash v_x$ and then by applying δ to every term of the tree obtained.

Fact 67 *P'_i is a proof of $(T_i\sigma)\delta \vdash (u_i\sigma)\delta$.*

To prove this, we have to show that for every node in P'_i labeled with $T_i\sigma\delta \vdash v_0$ and with n sons labeled respectively by $T_i\sigma\delta \vdash v_1, \dots T_i\sigma\delta \vdash v_n$, the inference $\dfrac{T_i\sigma\delta \vdash v_1 \dots T_i\sigma\delta \vdash v_n}{T_i\sigma\delta \vdash v_0}$ is an instance of an inference rule of Figure 2.

We distinguish several cases:

- If the inference is a leaf added by the replacement of an instance of (C^-) in the construction of P'_i given above, then we have $v_0 = 0$, hence $v_0 \in T_i\sigma\delta$.
- If the inference is not a leaf added by the replacement, then we have a "corresponding" inference in P_i. This means that there exists $\dfrac{T_i\sigma \vdash u_1 \dots T_i\sigma \vdash u_n}{T_i\sigma \vdash u_0}$ an inference step in P_i such that $v_i = u_i\delta$ for each $0 \leq i \leq n$. Since, by construction of P'_i we know that v_x is never decomposed in P_i and the conclusion of an instance of (C^-) can not be v_x, we can show by case analysis on the inference rule, that when we apply δ on the inference above, we retrieve another instance of the same inference rule. □

Proposition 32 *Let t be a term and σ a substitution. We have:*

$$St_{\mathsf{E}}(t\sigma) \subseteq St_{\mathsf{E}}(t)\sigma \cup \bigcup_{x \in vars(t)} St_{\mathsf{E}}(x\sigma)$$

PROOF. This can be easily proved by structural induction on t. If t is a constant or a variable, it is obvious. Now, assume that t is a standard term, *i.e.* $t = f(t_1, \dots, t_n)$ with $f \in \mathcal{F} \setminus sig(\mathsf{E})$. Note that, in such a case, we have

that $t\sigma = f(t_1\sigma, \ldots, t_n\sigma)$ is also a standard term. We have:

$$\begin{aligned} St_{\mathsf{E}}(t\sigma) &= \{t\sigma\} \cup \textstyle\bigcup_{i=1}^{n} St_{\mathsf{E}}(t_i\sigma) \\ &\subseteq \{t\sigma\} \cup \textstyle\bigcup_{i=1}^{n} (St_{\mathsf{E}}(t_i)\sigma \cup \bigcup_{x \in vars(t_i)} St_{\mathsf{E}}(x\sigma)) \text{ by induction hypothesis} \\ &\subseteq St_{\mathsf{E}}(f(t_1, \ldots, t_n))\sigma \cup \textstyle\bigcup_{x \in vars(\{t_1, \ldots, t_n\})} St_{\mathsf{E}}(x\sigma) \\ &\subseteq St_{\mathsf{E}}(t)\sigma \cup \textstyle\bigcup_{x \in vars(t)} St_{\mathsf{E}}(x\sigma) \end{aligned}$$

If t is not a standard term, then we have $t = C[t_1, \ldots, t_n]$ for some standard terms $t_1, \ldots, t_n$ and an E-context C, and we can do the same reasoning as before. □

Lemma 34 *Assume that $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ is a local inference system. Let σ be a conservative solution of $\mathcal{C} = \{C_1, \ldots, C_k\}$. For each $i \leq k$, there exists a proof P_i of $C_i\sigma$ which involves only terms in $St_{\mathsf{E}}(\mathcal{C})\sigma$.*

PROOF. Since the system $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ is local, we know that for each i there exists a minimal proof P_i of $T_i\sigma \vdash u_i\sigma$ which only involves terms in $St_{\mathsf{E}}(\mathcal{C}\sigma)$. Thanks to Proposition 32, we have $St_{\mathsf{E}}(\mathcal{C}\sigma) \subseteq St_{\mathsf{E}}(\mathcal{C})\sigma \cup \bigcup_{x \in vars(\mathcal{C})} St_{\mathsf{E}}(x\sigma)$. Hence, we obtain:

$$\begin{aligned} St_{\mathsf{E}}(\mathcal{C}\sigma) &\subseteq St_{\mathsf{E}}(\mathcal{C})\sigma \cup \textstyle\bigcup_{x \in vars(\mathcal{C})} St_{\mathsf{E}}(x\sigma) \\ &\subseteq (St_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C}))\sigma \cup \textstyle\bigcup_{x \in vars(\mathcal{C})} St_{\mathsf{E}}(x\sigma) \quad \text{since } x\sigma \in St_{\mathsf{E}}(x\sigma) \\ &\subseteq \bar{S}(\mathcal{C})\sigma \quad \text{since } \sigma \text{ is conservative w.r.t. } \mathcal{C} \end{aligned}$$

where $\bar{S}(\mathcal{C}) = \{C[t_1, \ldots, t_n] \mid \forall i.\ t_i \in St_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C}) \text{ and } C \text{ is an } \mathsf{E}\text{-context}\}$

Hence, each node $T_i\sigma \vdash v$ of P_i is such that $v \in \bar{S}(\mathcal{C})\sigma$. Now, it remains to show that each node is actually in $St_{\mathsf{E}}(\mathcal{C})$. To establish this, we first show that all the nodes involved in an inference other than $(\mathsf{M}_{\mathsf{E}})$ satisfy this condition. Let $\dfrac{T_i\sigma \vdash u_1 \ldots T_i\sigma \vdash u_n}{T_i\sigma \vdash u_0}$ be an inference in P_i which is an instance of some rule other than $(\mathsf{M}_{\mathsf{E}})$, say that (C^-). We have to show that for all $j \in \{0, \ldots n\}$, we have $u_j \in St_{\mathsf{E}}(\mathcal{C})\sigma$. Since $u_0 \in \bar{S}(\mathcal{C})$ and u_0 is headed with $f \in \mathcal{VF} \setminus sig(\mathsf{E})$, we have that $u_0 \in St_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C})$. Hence, we deduce that $u_0, u_1, \ldots, u_n \in St_{\mathsf{E}}(\mathcal{C})$.

Then, we have to deal with the instance of $(\mathsf{M}_{\mathsf{E}})$. By minimality of P_i, an instance of a rule $(\mathsf{M}_{\mathsf{E}})$ must not be followed by another instance of $(\mathsf{M}_{\mathsf{E}})$ (we could otherwise merge the two instances). Hence, for each premise $T_i\sigma \vdash u$ of an instance of $(\mathsf{M}_{\mathsf{E}})$, either $T_i\sigma \vdash u$ is the conclusion of an instance of another

inference rule than (M_E), or we have $u \in T_i\sigma$. Furthermore, the conclusion $T_i\sigma \vdash u$ of an instance of (M_E) is either the premise of an instance of another inference rule than (M_E), or we have $u = u_i\sigma$. This allows us to conclude. □

Appendix B About General Unification in Monoidial Theories

In this section we show a technical property of most general solutions of general unification problems:

Proposition 38 *Let* E *be a monoidal equational theory which is unitary for elementary unification, and such that there is an algorithm to compute solutions of inhomogeneous linear equations over the associated semiring* $\mathcal{S}_\mathsf{E}$*. Then* E *satisfies the unification property.*

In order to show that proposition, we first need some additional lemmas. In this section, we denote by Σ_1 the signature of the equational theory E, and by Σ_2 the set of function symbols not in Σ_1 (that is, the free function symbols and constants). We denote by E_1 the equational theory E, and by E_2 the empty equational theory.

A *unification problem with linear constant restrictions* in an equational theory E is a triple $(P, C, <)$ where C is a set of new constants not contained in $sig(\mathsf{E})$, P is a set of equations over the signature $sig(\mathsf{E}) \cup C$, and $<$ is a linear order on $C \cup vars(P)$. A substitution σ is a solution to $(P, C, <)$ if σ is a solution to P with the additional property that c is not a subterm of $x\sigma$ whenever $c < x$.

Lemma 68 *Let* E *be a monoidal equational theory that is unitary for elementary unification, and such that there is an algorithm to compute solutions of inhomogeneous linear equations over the associated semiring* $\mathcal{S}_\mathsf{E}$*.*

There is an algorithm which for any unification problem $(P, C, <)$ *with linear constant restrictions decides whether it has a solution, and in this case computes a complete and finite set* $mgu_\mathsf{E}(P, C, <)$ *of solutions to* $(P, C, <)$ *which are* P*-conservative.*

In difference to Proposition 38, Lemma 68 is only about unification problems with linear constant restrictions.

PROOF. An algorithm to compute solutions of unification problems with linear constant restrictions is given in [BN96]. We just have to show that all

solutions obtained by their algorithm are P-conservative. To this end let θ be a substitution returned by the algorithm, $x \in dom(\theta)$ and $v \in St_{\mathsf{E}}(x\theta) \setminus \mathcal{X}$. According to our definition of subterms (see Definition 12), we have to consider two cases:

(1) $v = x\theta$. In this case we simply choose $t = x$.
(2) v is a constant. In this case, the constant v is either 0 or is already a subterm of P. □

Lemma 69 *There is an algorithm which for any unification problem with linear constant restrictions $(P, C, <)$ over the signature Σ_2 decides whether it has a solution, and in this case computes a most general unifier which is P-conservative.*

PROOF. We use the algorithm of A. Martelli and U. Montanari [MM82] which is trivial to extend to linear constant restrictions. Here we follow the presentation of that algorithm in [BS01]. The algorithm consists of 6 transformation rules which rewrite pairs of the form $P\,;S$ where P is a unification problem and S a solved form. We denote by σ_S the substitution derived from a solved form S. Given a unification problem P we start on the pair $P\,;\emptyset$. The transformation system has the property that $vars(P') \cap dom(\sigma_{S'}) = \emptyset$ and also that $dom(\sigma_{S'}) \cap img(\sigma_{S'}) = \emptyset$ for every reachable pair $P'\,;S'$. If we can reach a pair $\emptyset\,;S'$ then $\sigma_{S'}$ is the most general unifier of P.

It is now sufficient to show by induction on the length of the rewrite sequence $P\,;\emptyset \to^* P'\,;S'$ that

$$St_{\mathsf{E}}(P') \cup St_{\mathsf{E}}(img(\sigma_{S'})) \subseteq St_{\mathsf{E}}(P)\sigma_{S'}$$

This is obviously the case when the length is one. Otherwise we consider the last rule used in the rewrite sequence. The assertion is trivially true for the rules (Symbol Clash) and (Occurs Check), and obvious for the rule (Orient) since this latter rule does not change the set of terms in $P\,;S$. Furthermore, the assertion is obviously true for the rules (Trivial) and (Decomposition) since these rules only restrict the set of subterms of the unification problem and do not change the solved form.

It remains the case of the rule (Variable Elimination):

$$\{x = t\} \cup P'\,;S' \;\to\; P'[x \mapsto t]\,;S'[x \mapsto t] \cup \{x = t\} \quad \text{if } x \notin vars(t)$$

Let S'' be $S'[x \mapsto t] \cup \{x = t\}$ and $v \in St_{\mathsf{E}}(P'[x \mapsto t]) \cup St_{\mathsf{E}}(img(\sigma_{S''}))$. There are two cases:

(1) $v \in St_{\mathsf{E}}(t)$:
By induction hypothesis, we have that $v = s\sigma_{S'}$ for some $s \in St_{\mathsf{E}}(P)$.

We have that $x \notin vars(t)$ by the side condition of the rule, and as a consequence $x \notin vars(v)$. Furthermore, we have that $\sigma_{S''} = \sigma_{S'}[x \mapsto t]$. Hence, we have that $v = s\sigma_{S'} = s\sigma_{S''}$.

(2) $v = v'[x \mapsto t]$ for some $v' \in St_{\mathsf{E}}(P') \cup St_{\mathsf{E}}(img(\sigma_{S'}))$:
By induction hypothesis we have that $v' = s\sigma_{S'}$ for some $s \in St_{\mathsf{E}}(P)$. Hence, we have that $v = v'[x \mapsto t] = s\sigma_{S'}[x \mapsto t] = s\sigma_{S''}$. □

PROOF of Proposition 38. We show that all substitutions returned by the combination algorithm of [BS96] are P-conservative. We recall here only the features of that combination algorithm that are essential for us:

Given a general unification problem P we obtain by a non-deterministic procedure two unification problems P_1 and P_2, together with a linear order $<$ on $V := vars(P_1) \cup vars(P_2)$, and a partition of V into $V_1 \uplus V_2$. This yields two unification problems with linear constant restrictions $(P_i, V_{3-i}, <)$ for $i = 1, 2$. Let σ_i be a solution of $(P_i, V_{3-i}, <)$ for $i = 1, 2$.

A substitution σ is constructed by induction on the order $<$:

- If $x \in V_i$ is minimal in the order $<$ then $x\sigma := x\sigma_i$.
- Otherwise, with $x \in V_i$, let $x\sigma := x\sigma_i\sigma$. In fact, the linear constant restrictions guarantee that $y < x$ for all $y \in vars(x\sigma_i)$, and hence that the expression $x\sigma_i\sigma$ is well-defined.

Note that in particular $\sigma_i\sigma = \sigma$ for $i = 1, 2$. The substitution σ is not yet a solution to P. However, the solution σ' finally obtained satisfies $img(\sigma') = img(\sigma)$. Hence, for our purpose it is sufficient to show by induction on the order $<$ that

$$\forall x \in V, St_{\mathsf{E}}(x\sigma) \setminus \mathcal{X} \subseteq St_{\mathsf{E}}(P)\sigma \cup \{0\}$$

Let $x \in V_i$, and assume that the assertion is true for all variables y with $y < x$. Let $v \in St_{\mathsf{E}}(x\sigma) \setminus \mathcal{X}$. By construction of σ, this means that $v \in St_{\mathsf{E}}(x\sigma_i\sigma) \setminus \mathcal{X}$. By Proposition 32, there are two cases:

(1) $v \in St_{\mathsf{E}}(x\sigma_i)\sigma \setminus \mathcal{X}$. We may even assume that $v \in (St_{\mathsf{E}}(x\sigma_i) \setminus \mathcal{X})\sigma$ since otherwise we have that $v \in \mathcal{X}\sigma$, and hence the second case applies.
By Lemmas 68 and 69 we know that $St_{\mathsf{E}}(x\sigma_i) \setminus \mathcal{X} \subseteq St_{\mathsf{E}}(P)\sigma_i \cup \{0\}$. As a consequence, $(St_{\mathsf{E}}(x\sigma_i) \setminus \mathcal{X})\sigma \subseteq (St_{\mathsf{E}}(P)\sigma_i \cup \{0\})\sigma = St_{\mathsf{E}}(P)\sigma \cup \{0\}$, where the last equation is due to $\sigma_i\sigma = \sigma$.

(2) $v \in St_{\mathsf{E}}(y\sigma)$ for some $y < x$.
In this case we conclude by applying the induction hypothesis. □

Appendix C From Satisfiability in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ to Satisfiability in $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$

Lemma 35 *Let $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ be a local inference system and $\mathcal{C}$ be a well-defined system of constraints. Let $\mathscr{C}'$ be the set of all constraint systems obtained by applying Algorithm 3 on $\mathcal{C}$ (by considering all the possible choices).*

(1) $\mathscr{C}'$ is a finite set of well-defined systems of one-step constraints.
(2) Let $\mathcal{C}' \in \mathscr{C}'$. If σ is a solution to $\mathcal{C}'$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ then σ is a solution to $\mathcal{C}$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$.
(3) If σ is a conservative solution to $\mathcal{C}$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ then there exists $\mathcal{C}' \in \mathscr{C}'$ such that σ is a solution to $\mathcal{C}'$ in $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$.
(4) For any $\mathcal{C}' \in \mathscr{C}'$, σ is conservative w.r.t. $\mathcal{C}$ if and only if σ is conservative w.r.t. $\mathcal{C}'$.

PROOF.

(1) Algorithm 3 is non-deterministic and at each step there are only finitely many possibilities to consider. Hence, $\mathscr{C}'$ is finite. By construction, each constraint system in $\mathscr{C}'$ is a one-step constraint system. Now, let $\mathcal{C}'$ be a one-step constraint system in $\mathscr{C}'$. The monotonicity of $\mathcal{C}'$ is due to the monotonicity of $\mathcal{C}$ and the construction of $\mathcal{C}'$. To complete the proof of well-definedness of $\mathcal{C}'$ we observe that each term which appears in a hypothesis set of a constraint is either a term introduced by the algorithm (*i.e.* a term in S) or a term issuing from a hypothesis set of a constraint in $\mathcal{C}$. In the first case, this means that the term appears previously in the target of a constraint by construction. As a consequence,if there were a substitution θ that makes well-definedness fail for $\mathcal{C}'$ then this same θ would make well-definedness fail for $\mathcal{C}$, which contradicts the assumption. Hence in both cases we conclude that $\mathcal{C}'$ is well-defined thanks to the well-definedness of $\mathcal{C}$.

(2) For each constraint $T_i \Vdash u_i \in \mathcal{C}$, there exists $T_i \cup S_1 \cup \ldots \cup S_i \ \Vdash_1 \ u_i \in \mathcal{C}'$. Since σ is a solution to $\mathcal{C}'$ (by hypothesis), this means that $u_i\sigma$ is one-step deducible from $T_i\sigma \cup S_1\sigma \cup \ldots \cup S_i\sigma$. By construction of $\mathcal{C}'$, we can show that each term in $S_j\sigma$ is deducible by using only terms in $T_j\sigma$. Intuitively, each proof is obtained by stacking "one-step" proofs in correct order. From this, we easily deduce that $u_i\sigma$ is deducible from $T_1\sigma \cup \ldots \cup T_i\sigma$ which is equal to $T_i\sigma$ thanks to the monotonicity of $\mathcal{C}$.

(3) By hypothesis, for each constraint $T_i \Vdash u_i \in \mathcal{C}$, there exists a proof P_i of $T_i\sigma \vdash u_i\sigma$. Since σ is conservative and $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ is local, thanks to Lemma 34, we can assume that the proof trees P_i involve only terms in $St_{\mathsf{E}}(\mathcal{C})\sigma$. Let $S'_i = \{s \in St_{\mathsf{E}}(\mathcal{C}) \mid T_i\sigma \vdash s\sigma\}$. In other words, S'_i contains all the subterms of $\mathcal{C}$ whose instance by σ is deducible at step i (*i.e.* by using the terms in T_i). Note that, thanks to the monotonicity of $\mathcal{C}$, we

have $S'_i \subseteq S'_{i+1}$ for all $1 \leq i < k$.

Now, let $S_1 = S'_1$ and $S_i = S'_i \setminus (S'_1 \cup \ldots \cup S'_{i-1})$ for $i \geq 2$. S_i contains all the subterms of $\mathcal{C}$ whose instance by σ is deducible at step i and not before. Finally, for each i, we order the elements in S_i such that: for all $s, s' \in S_i$ such that $T_i\sigma \vdash s\sigma$ is the root of a subproof of a minimal proof of $T_i\sigma \vdash s'\sigma$, then $s \prec_i s'$. Hence for each $s \in S_i$, we have that $s\sigma$ is one-step deducible from $S_1\sigma \cup \ldots \cup S_{i-1}\sigma \cup \{s'\sigma \mid s' \prec_i s \text{ and } s' \in S_i\}$. It remains to show that $u_i\sigma$ is one-step deducible from $T_i\sigma \cup S_1\sigma \cup \ldots \cup S_i\sigma$. By definition of the S_j and thanks to the fact that $u_i\sigma$ is deducible at least at step i, we know that $u_i \in S_1 \cup \ldots \cup S_i$. So, we easily deduce that $u_i\sigma \in T_i\sigma \cup S_1\sigma \cup \ldots \cup S_i\sigma$. Hence, the result holds.

(4) Let $\mathcal{C}' \in \mathscr{C}'$. We have $St_{\mathsf{E}}(\mathcal{C}') = St_{\mathsf{E}}(\mathcal{C})$. Hence σ is conservative w.r.t. $\mathcal{C}$ if and only if σ is conservative w.r.t. $\mathcal{C}'$. □

Lemma 39 *Let* E *be an equational theory for which general unification is decidable and finitary and let* $\mathcal{C}$ *be a well-defined system of one-step constraints. Let* $\mathcal{P} = \{\bigwedge_{(s_1,s_2)\in S'} s_1 = s_2 \mid S' \subseteq St_E(\mathcal{C})^2\}$. *Let* $R \in \mathcal{P}$ *and* $\theta \in mgu_{\mathsf{E}}(R)$. *Let* $\mathcal{C}_\theta = \{T\theta \Vdash u\theta \mid T \Vdash_1 u \in \mathcal{C}$ *and* $u\theta$ *is not* DY*-one-step deducible from* $T\theta\}$.

(1) There are only finitely many outputs (i.e. possibilities for $\mathcal{C}_\theta$*) for a given input* $\mathcal{C}$. *Each of them is a well-defined system of constraints.*

(2) If there exists $\mathcal{C}_\theta$ *(obtained by the procedure above) which has a solution in* $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$ *then* $\mathcal{C}$ *has a solution in* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$.

(3) If $\mathcal{C}$ *has a conservative solution in* $(\mathcal{I}_{\mathsf{DY}}, \mathcal{R}_{\mathsf{E}})$ *then there exists* $\mathcal{C}_\theta$ *(obtained by the procedure above) which has a solution in* $(\mathcal{I}_{\mathsf{M_E}}, \mathcal{R}_{\mathsf{E}})$. *Moreover, if* E *satisfies the unification property then* $\mathcal{C}_\theta$ *has a non-collapsing solution.*

PROOF.

(1) $\mathcal{P}$ is a finite set of equation systems since $St_{\mathsf{E}}(\mathcal{C})$ is finite. Each system of equations represents a unification problem and has a finite complete set of unifiers since E is finitary for general unification. Let θ be such a unifier. Let $\mathcal{C}_\theta$ be a constraint system obtained by using the substitution θ. We have to show that $\mathcal{C}_\theta\sigma$ is well-formed for every substitution σ. Let $\mathcal{C}' = \mathcal{C}\theta\sigma$. Thanks to the well-definedness of $\mathcal{C}$, we deduce that $\mathcal{C}'$ is well-formed. It remains to show that the constraints that we need to remove to obtain $\mathcal{C}_\theta$ from $\mathcal{C}'$ do not change anything regarding well-definedness. In other words, we need to show that a removed constraint $T\theta \Vdash_1 u\theta$ does not introduce a variable for the first time, *i.e.* there exists $x \in vars(u\theta)$ and $x \notin vars(T\theta)$. By hypothesis, such a constraint $T\theta \Vdash_1 u\theta$ is such that $u\theta$ is DY-one-step deducible from $T\theta$. Hence $vars(u\theta) \subseteq vars(T\theta)$.

(2) Let $\mathcal{C}_\theta$ be the constraint system obtained from $\mathcal{C}$ by applying the transformation described in Lemma 39 with the substitution θ. Let θ' be a solution to $\mathcal{C}_\theta$. We are going to show that $\theta\theta'$ is a solution to $\mathcal{C}$. Let $T \Vdash_1 u \in \mathcal{C}$. Either $u\theta$ is DY-one-step-deducible from $T\theta$ (without any instantiation) or $T\theta \Vdash u\theta \in \mathcal{C}'$. In both case, this means that $u\theta\theta'$ is one-step deducible from $T\theta\theta'$. Hence $\theta\theta'$ is a solution of $\mathcal{C}$.

(3) Let σ be a conservative solution to $\mathcal{C}$. Let

$$R = \{(s_1, s_2) \mid s_1, s_2 \in St_{\mathsf{E}}(\mathcal{C}) \text{ and } s_1\sigma =_{\mathsf{E}} s_2\sigma\}$$

Let $\theta \in mgu_{\mathsf{E}}(R)$ such that θ is more general than σ. Then, let θ' be the substitution such that $\theta\theta' =_{\mathsf{E}} \sigma$. Let

$$\mathcal{C}_\theta = \{T\theta \Vdash u\theta \mid T \Vdash_1 u \in \mathcal{C} \text{ and } u\theta \text{ is not } \mathsf{DY}\text{-one-step deducible from } T\theta\}.$$

We are going to show that θ' is a solution to $\mathcal{C}_\theta$, *i.e.* $u\theta'$ is $\mathsf{M_E}$-one-step deducible from $T\theta'$ for each constraint in $\mathcal{C}_\theta$. Let $T \Vdash_1 u \in \mathcal{C}$ such that $u\sigma$ is DY-one-step deducible from $T\sigma$. We are going to show that $u\theta$ is DY-one-step deducible from $T\theta$. Hence, the constraints that remain in $\mathcal{C}_\theta$ are those that can be solved by using ($\mathsf{M_E}$). If $u\sigma \in T\sigma$, this means that there exists $t \in T$ such that $t\sigma = u\sigma$. Hence, we have $t\theta = u\theta$ since $t, u \in St_{\mathsf{E}}(\mathcal{C})$. Hence $u\theta \in T\theta$, and so $u\theta$ is one-step deducible from $T\theta$. Otherwise, $u\sigma$ is one-step deducible from $T\sigma$ by using an inference rule among (C^-), (UL), (UR) or (D).
In the first case, *i.e.* (C^-), we have $u\sigma = f(v_1, \ldots, v_n)$ for some $v_i \in T\sigma$ and $f \in \mathcal{VF} \setminus sig(\mathsf{E})$. Hence, for every $i \leq n$ there exists $v'_i \in T$ such that $v_i = v'_i\sigma$. There are two possibilities:

- If u is not a variable, then $u = f(u'_1, \ldots, u'_n)$, we have $u'_i, v'_i \in St_{\mathsf{E}}(\mathcal{C})$ and $u'_i\sigma = v'_i\sigma$ for each $i \leq n$. Hence, we deduce that $u'_i\theta = v'_i\theta$ and $u\theta$ is DY-one-step deducible from $T\theta$.
- If u is a variable then (since σ is conservative w.r.t. $\mathcal{C}$) there exists $t \in St_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C})$ such that $u\sigma =_{\mathsf{E}} t\sigma$. Hence $t = f(t_1, \ldots, t_n)$ for some $t_i \in St_{\mathsf{E}}(\mathcal{C})$. We can deduce that $t_i = v'_i$. Hence $u\theta$ is DY-one-step deducible from $T\theta$.

The others cases (UR), (UL) and (D) are similar.

Finally, if E satisfies the unification property then we can show that θ' is non-collapsing w.r.t. $\mathcal{C}_\theta$. Let $u, v \in St_{\mathsf{E}}(\mathcal{C}_\theta) \setminus \mathcal{X}$. Hence, by Proposition 32, we have $u, v \in St_{\mathsf{E}}(\mathcal{C})\theta \cup \bigcup_{x \in vars(\mathcal{C})} St_{\mathsf{E}}(x\theta)$. Thanks to the fact that E satisfies the unification property (*cf.* Definition 37) there exist $u_1, v_1 \in St_{\mathsf{E}}(\mathcal{C})$ such that $u = u_1\theta$ and $v = v_1\theta$. Assuming that $u\theta' =_{\mathsf{E}} v\theta'$, we obtain that $u_1\theta\theta' =_{\mathsf{E}} v_1\theta\theta'$, hence we have $u_1\sigma =_{\mathsf{E}} v_1\sigma$ and by definition of R we have that $(u_1, v_1) \in R$. Finally, by construction of θ, we deduce that $u_1\theta = v_1\theta$, *i.e.* $u =_{\mathsf{E}} v$. Hence, we deduce that θ' is non-collapsing w.r.t. $\mathcal{C}_\theta$. □

Appendix D About Well-Defined Constraint Systems

Proposition 46 (new characterization of well-definedness) *Let $\mathcal{C} = \{T_1 \Vdash u_1, \ldots, T_k \Vdash u_k\}$ be a constraint system on the reduced signature which satisfies the monotonicity property. The system $\mathcal{C}$ is well-defined if and only if for all $i \leq k$, for all $t \in T_i$, the vector $\phi_{\mathcal{X}}(t)$ is dependent of $\mathcal{B}_{i-1}(\mathcal{C})$.*

PROOF. ($\Leftarrow$) We have to show that for every substitution θ, $\mathcal{C}\theta$ satisfies the origination property. Let θ be a substitution and t be a term which appears in an hypothesis set T_i of $\mathcal{C}$ such that $t\theta$ contains a variable Z. As explained at the end of Section 3, we denote by t^0 (resp. u_j^0) the constant part of the term t (resp u_j^0). We have to show that $Z \in vars(u_{i'}\theta)$ for some $i' < i$. Let $L_{i-1}(\mathcal{C}) = \{i_1, \ldots, i_n\}$. By hypothesis, we know that there exists $\alpha \in \mathcal{S}_{\mathsf{E}}$ ($\alpha \neq 0$) and $\alpha_{i_1}, \ldots, \alpha_{i_n} \in \mathcal{S}_{\mathsf{E}}$ such that:

$$
\begin{aligned}
& \alpha \cdot \phi_{\mathcal{X}}(t) = \sum_{j \in L_{i-1}(\mathcal{C})} \alpha_j \cdot \phi_{\mathcal{X}}(u_j) \\
\Rightarrow \quad & \alpha \odot (t - t^0) = \sum_{j \in L_{i-1}(\mathcal{C})} \alpha_j \odot (u_j - u_j^0) \\
\Rightarrow \quad & \alpha \odot (t\theta - t^0) = \sum_{j \in L_{i-1}(\mathcal{C})} \alpha_j \odot (u_j\theta - u_j^0) \\
\Rightarrow \quad & \alpha \odot t\theta = \sum_{j \in L_{i-1}(\mathcal{C})} \alpha_j \odot (u_j\theta - u_j^0) + \alpha \odot t^0
\end{aligned}
$$

Hence, since $Z \in vars(t\theta)$, we deduce that $Z \in vars(u_{i'}\theta)$ for some $i' \leq i$.

($\Rightarrow$) Assume that there exists $1 \leq i \leq k$ and $t \in T_i$ such that $\phi_{\mathcal{X}}(t)$ is independent of $\mathcal{B}(\mathcal{C}_{i-1}(\mathcal{C}))$. Let $L_{i-1}(\mathcal{C}) = \{i_1, \ldots, i_n\}$. Let A be the matrix whose rows is made up of the vectors $\phi_{\mathcal{X}}(u_{i_1}), \ldots, \phi_{\mathcal{X}}(u_{i_n})$ and $\phi_{\mathcal{X}}(t)$, and b be the column vector $(0, \ldots, 0, 1)$. By Fact 47, there exists $Q \in \mathcal{S}_{\mathsf{E}}$ such that $A \cdot Y = Q \cdot b$ has a solution in $\mathcal{S}_{\mathsf{E}}^p$.

Let $(c_1, \ldots, c_p)$ be a solution to this system of equations. Let Z be a fresh variable and θ be the substitution defined by $X_{i'} \mapsto c_{i'} \odot Z$ for $1 \leq i' \leq p$. By construction of θ, we have $u_i\theta = u_i^0$ for each $i \in L$ such that $i \leq j$ and we have $t_{n+j}\theta = Q \odot Z + t_{n+j}^0$ (remember that t_{n+j} is the term added in the hypothesis set of the $j + 1^{\text{th}}$ constraint – *cf.* beginning of Section 9). In other words, we have found a substitution θ such that Z appears for the first time in an hypothesis set of $\mathcal{C}\theta$. This contradicts the well-definedness of $\mathcal{C}$. $\square$

Lemma 51 *If a well-defined constraint system $\mathcal{C}$ has a non-collapsing solution in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$ then it is factor-preserving.*

PROOF. Let $\mathcal{C} = \{T_1 \Vdash u_1, \ldots, T_k \Vdash u_k\}$ be a well-defined constraint system and σ a non-collapsing solution to $\mathcal{C}$ in $(\mathcal{I}_{\mathsf{M}_\mathsf{E}}, \mathcal{R}_\mathsf{E})$. Firstly, we show that for all $i \leq k$:

(1) $Fact_\mathsf{E}(u_i\sigma) \subseteq (Fact_\mathsf{E}(T_i) \setminus \mathcal{X})\sigma$, and
(2) for all $x \in vars(u_i)$ such that for all $j < i$ we have $x \notin vars(u_j)$, the following property is satisfied:

$$Fact_\mathsf{E}(x\sigma) \subseteq (Fact_\mathsf{E}(T_i) \setminus \mathcal{X})\sigma.$$

Base case. Since T_1 is a set of ground terms, we have $Fact_\mathsf{E}(u_1\sigma) \subseteq Fact_\mathsf{E}(T_1)$ and $Fact_\mathsf{E}(T_1) = (Fact_\mathsf{E}(T_1) \setminus \mathcal{X})\sigma$. This allows us to conclude about (1). Now, let $x \in vars(u_1)$. If $x \in Fact_\mathsf{E}(u_1)$ then $Fact_\mathsf{E}(x\sigma) \subseteq Fact_\mathsf{E}(u_1\sigma)$ and we conclude thanks to (1). Otherwise, there exists $f \in Fact_\mathsf{E}(u_1)$ such that $x \in vars(f)$. Then, we have $f\sigma = t_g$ with $t_g \in St_\mathsf{E}(T_1)$. This contradicts the fact that σ is non-collapsing.
Induction step. Let $i > 1$. We have $Fact_\mathsf{E}(u_i\sigma) \subseteq Fact_\mathsf{E}(T_i)\sigma$. Assume that there exists $f \in Fact_\mathsf{E}(u_i\sigma)$ and $x \in Fact_\mathsf{E}(T_i)$ such that $f = x\sigma$. By induction hypothesis, we know that: $Fact_\mathsf{E}(x\sigma) \subseteq (Fact_\mathsf{E}(T_i) \setminus \mathcal{X})\sigma$. We conclude about (1). Now, assume that there exists $x \in vars(u_i\sigma)$ such that $x \notin vars(u_j\sigma)$ for all $j < i$. Since $\mathcal{C}$ is a well-defined constraint system, we have $x \notin vars(T_i)$. We deduce that $x \in Fact_\mathsf{E}(u_i)$ since σ is non-collapsing. Hence, we have that $Fact_\mathsf{E}(x\sigma) \subseteq Fact_\mathsf{E}(u_i\sigma)$ and we conclude thanks to (1).

Now, we have to show that $\mathcal{C}$ satisfies (1) and (2) implies that $\mathcal{C}$ is factor-preserving. Let i be such that $1 \leq i \leq k$. We have that

$$(Fact_\mathsf{E}(u_i) \setminus \mathcal{X})\sigma \subseteq Fact_\mathsf{E}(u_i\sigma) \cup \bigcup_{x \in vars(u_i)} Fact_\mathsf{E}(x\sigma)$$

Thanks to (1) and (2), we deduce that $(Fact_\mathsf{E}(u_i) \setminus \mathcal{X})\sigma \subseteq (Fact_\mathsf{E}(T_i) \setminus \mathcal{X})\sigma$. Since σ is non-collapsing, we have that $Fact_\mathsf{E}(u_i) \setminus \mathcal{X} \subseteq Fact_\mathsf{E}(T_i) \setminus \mathcal{X}$ and hence $Fact_\mathsf{E}(u_i) \setminus \mathcal{X} \subseteq Fact_\mathsf{E}(T_i)$. This allows us to conclude. □

Lemma 55 *Let $\mathcal{C} = \{T_1 \Vdash u_1, \ldots, T_k \Vdash u_k\}$ be a factor-preserving and well-defined constraint system (on the full signature) and $1 \leq i \leq k$. We have that: for all $s \in NSt_\mathsf{E}(T_i)$, the vector $\phi_\mathcal{X}(s)$ is dependent from $\mathcal{B}_{i-1}(\mathcal{C})$.*

PROOF. We proceed by induction on i.

Base case: $i = 1$. Let $s \in NSt_{\mathsf{E}}(T_1)$. Since T_1 is ground, we deduce that s is ground, and hence $\phi_{\ell_{\mathcal{X}}}(s) = (0, \ldots, 0)$. This allows us to conclude.

Induction step: Let $1 < i \leq k$. By contradiction, we suppose that there is a $s \in NSt(T_i)$ such that $\{\phi_{\mathcal{X}}(s)\} \cup \mathcal{B}_{i-1}$ is independent. We will now construct a substitution θ witnessing the fact that $\mathcal{C}$ is not well-defined.

By Fact 47 there is some $Q \in \mathcal{S}_{\mathsf{E}}, Q \neq 0$, and a vector $(c^{x_1}, \ldots, c^{x_p}) \in (\mathcal{S}_{\mathsf{E}})^p$ such that

$$\begin{pmatrix} \phi_{x_1}(u_1) & \ldots & \phi_{x_p}(u_1) \\ \vdots & & \vdots \\ \phi_{x_1}(u_{i-1}) & \ldots & \phi_{x_p}(u_{i-1}) \\ \phi_{x_1}(s) & \ldots & \phi_{x_p}(s) \end{pmatrix} \cdot \begin{pmatrix} c^{x_1} \\ \vdots \\ c^{x_p} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ Q \end{pmatrix} \qquad (\star)$$

where only those row vectors $\phi_{\mathcal{X}}(u_j)$ appear in the matrix for which $j \in L$. We define the substitution θ in the following way:

$$x_i \mapsto x_i + c^{x_i} \odot z$$

for any $1 \leq i \leq p$.

We are going to establish that:

- for all $j < i$, we have $z \notin vars(u_j\theta)$ (*cf.* Fact 71),
- $z \in vars(T_i\theta)$ (*cf.* Fact 72)

Fact 70 *For all $j < i$, for all $t \in T_j$, we have $z \notin vars(t\theta)$.*

Let $j < i$. We show that for all $t \in NSt_{\mathsf{E}}(T_j)$, we have $Z \notin vars(t\theta)$.

Base case: If $Fact_{\mathsf{E}}(t) \subseteq \mathcal{X} \cup \mathcal{T}(\mathcal{F})$ (In other words, the factors of t are either variables or ground terms), we have that

$$t = \phi_{x_1}(t) \odot x_1 + \ldots + \phi_{x_p}(t) \odot x_p + t^0.$$

By induction hypothesis (of Lemma 55), we know that $\phi_{\ell_{\mathcal{X}}}(t)$ is dependant of $\mathcal{B}_{i-1}(\mathcal{C})$. We deduce that $t\theta = t^0$. Hence we conclude that $Z \notin vars(t\theta)$.

Induction step: We distinguish two cases.

(1) The term t is a standard term. There exists a $\{\mathcal{F} \setminus sig(\mathsf{E})\}$-context C and some non-standard terms (or variables) $t_1, \ldots, t_n \in NSt_{\mathsf{E}}(t)$ such

that $t = C[t_1, \ldots, t_n]$. In such a case, we have $t\theta = C[t_1\theta, \ldots, t_n\theta]$ and we conclude by applying the induction hypothesis on $t_1, \ldots, t_n$.

(2) The term t is a non-standard term. In such a case t is of the form:

$$t = \sum_{i=1}^{p}(\phi_{x_i}(t) \odot x_i) + \sum_{f \in Fact_{\mathsf{E}}(t) \setminus \mathcal{X}} (\phi_f(t) \odot f)$$

By definition of θ, we have:

$$\begin{aligned} t\theta &= \sum_{i=1}^{p}(\phi_{x_i}(t) \odot x_i\theta) + \sum_{f \in Fact_{\mathsf{E}}(t) \setminus \mathcal{X}} (\phi_f(t) \odot f\theta) \\ &= \underbrace{\sum_{i=1}^{p}(\phi_{x_i}(t) \odot x_i)}_{t_1} + \underbrace{\sum_{i=1}^{p}((\phi_{x_i}(t) \cdot c^{x_i}) \odot Z)}_{t_2} + \underbrace{\sum_{f \in Fact_{\mathsf{E}}(t) \setminus \mathcal{X}} (\phi_f(t) \odot f\theta)}_{t_3} \end{aligned}$$

Firstly, we have $z \notin vars(t_1)$. By induction hypothesis (of Fact 70), we have that $z \notin vars(t_3)$. By induction hypothesis (of Lemma 55), $\phi_{\mathcal{X}}(t)$ is dependant of $\mathcal{B}_{j-1}(\mathcal{C})$, and hence of $\mathcal{B}_{i-1}(\mathcal{C})$. Let $\{i_1, \ldots, i_n\} = \{\ell \in L \mid \ell < i\}$. There exists $\alpha, \alpha_{i_1}, \ldots, \alpha_{i_n} \in \mathbb{Z}_2[\mathsf{h}]$ such that $\alpha \neq 0$ and:

$$\alpha \cdot \phi_{\mathcal{X}}(t) = \alpha_{i_1} \cdot \phi_{\mathcal{X}}(u_{i_1}) + \ldots + \alpha_{i_n} \cdot \phi_{\mathcal{X}}(u_{i_n})$$

$$\Rightarrow \quad \alpha \cdot \sum_{i=1}^{p}(\phi_{x_i}(t) \cdot c^{x_i}) = \alpha_{i_1} \cdot \sum_{i=1}^{p}(\phi_{x_i}(u_{i_1}) \cdot c^{x_i}) + \ldots + \alpha_{i_n} \cdot \sum_{i=1}^{p}(\phi_{x_i}(u_{i_n}) \cdot c^{x_i})$$

$$\Rightarrow \quad \alpha \cdot \sum_{i=1}^{p}(\phi_{x_i}(t) \cdot c^{x_i}) = \alpha_{i_1} \cdot 0 + \ldots + \alpha_{i_n} \cdot 0 \qquad \text{thanks to } (\star)$$

$$\Rightarrow \quad \alpha \cdot \sum_{i=1}^{p}(\phi_{x_i}(t) \cdot c^{x_i}) = 0$$

Hence, we have $\sum_{i=1}^{p}(\phi_{x_i}(t) \cdot c^{x_i}) = 0$. We deduce that $z \notin vars(t_2)$. Hence, we obtain that for all $j < i$, for all $t \in NSt_{\mathsf{E}}(T_j)$, we have $z \notin vars(t\theta)$.

Let $t \in T_j$. If t is a non-standard term, we have $t \in NSt_{\mathsf{E}}(t)$ and we conclude. Otherwise, there exists a $\{\mathcal{F} \setminus sig(\mathsf{E})\}$-context C and some non-standard terms $t_1, \ldots, t_n \in NSt_{\mathsf{E}}(t)$ such that $t = C[t_1, \ldots, t_n]$. We apply Fact 70 on $t_1, \ldots, t_n$ and we conclude.

Fact 71 *For all $j < i$, we have $z \notin vars(u_j\theta)$.*

Assume that there exists $j < i$ such that $z \in vars(u_j\theta)$. If $j \in L_{i-1}(\mathcal{C})$ then

$\sum_{i=1}^{p}(\phi_{x_i}(u_j)\cdot c^{x_i}) = 0$ by construction of θ, and if $j \notin L_{i-1}(\mathcal{C})$, we also have $\sum_{i=1}^{p}(\phi_{x_i}(u_j)\cdot c^{x_i}) = 0$ since by construction of $L_{i-1}(\mathcal{C})$, $\phi_{\mathcal{X}}(u_j)$ is dependant of $\mathcal{B}_{i-1}(\mathcal{C})$. Hence, we deduce that there exists $f \in Fact_{\mathsf{E}}(u_j\theta) \setminus \mathcal{X}$ such that $z \in vars(f)$, and there exists $f' \in Fact_{\mathsf{E}}(u_j)$ such that $z \in vars(f'\theta)$. Since $\mathcal{C}$ is factor-preserving, we deduce that there exists $j' \leq j$ such that $f' \in Fact_{\mathsf{E}}(T_{j'})$. Lemma 73, stated and proved below, ensures that for all $f'' \in Fact_{\mathsf{E}}(T_{j'})$ such that $f' \neq f''$, we have $f'\theta \neq f''\theta$. Hence, $z \in vars(T_{j'}\theta)$, which contradicts Fact 70.

Fact 72 *We have $z \in vars(T_i\theta)$.*

The term s has the following form:

$$s = \sum_{i=1}^{p}(\phi_{x_i}(s) \odot x_i) + \sum_{f \in Fact_{\mathsf{E}}(s) \setminus \mathcal{X}} (\phi_f(s) \odot f).$$

By definition of θ, we know that:

$$s\theta = \sum_{i=1}^{p}(\phi_{x_i}(s) \odot x_i) + \underbrace{\sum_{i=1}^{p}((\phi_{x_i}(s)\cdot c^{x_i}) \odot z)}_{=Q\odot z} + \sum_{f \in Fact_{\mathsf{E}}(s) \setminus \mathcal{X}} (\phi_f(s) \odot f\theta).$$

We deduce that $z \in vars(s\theta)$. If $s \in T_i$, we conclude that $z \in vars(T_i\theta)$. Otherwise, there exists $f \in Fact_{\mathsf{E}}(T_i) \setminus \mathcal{X}$ such that $s \in NSt_{\mathsf{E}}(f)$. Lemma 73 ensires that the factor $f\theta$ can not disappear. Hence, we deduce that $z \in vars(f\theta)$, and $z \in vars(T_i\theta)$.

Hence, we have $z \in vars(T_i\theta)$ and $z \notin vars(u_j\theta)$ for all $j < i$, which contradicts the fact that $\mathcal{C}$ is a well-defined constraint system. □

In the proof above, we use the following lemma in order to ensure that different factors can not become equal after application of the substitution θ that we have chosen. We formally state and prove this lemma below.

Lemma 73 *Let z be a fresh variable and θ a substitution of the form $x \mapsto x + c^x \odot z$ for all $x \in \mathcal{X}$, where $c^x \in \mathcal{S}_{\mathsf{E}}$ for all $x \in \mathcal{X}$. If $t_1 \neq_{\mathsf{E}} t_2$, then $t_1\theta \neq_{\mathsf{E}} t_2\theta$.*

PROOF. We show this result by induction on the size of the terms t_1 and t_2. The base case is trivial. We distinguish several cases:

- If t_1 and t_2 are standard terms, we have $t_1 = f_1(t_1^1, \ldots, t_1^n)$ and $t_2 = f_2(t_2^1, \ldots, t_2^m)$. If $f_1 \neq f_2$ then we conclude that $t_1\theta \neq t_2\theta$. Otherwise, we

have $n = m$ and there exists $i < n$ such that $t_1^i \neq t_2^i$. By induction hypothesis, we know that $t_1^i\theta \neq t_2^i\theta$, and we deduce that $t_1\theta = f_1(t_1^1\theta, \ldots, t_1^n\theta) \neq f_2(t_2^1\theta, \ldots, t_2^n\theta) = t_2\theta$.

- If t_1 is a standard term and t_2 a non-standard term, we have $t_1 = f_1(t_1^1, \ldots, t_1^n)$ and $t_2 = \sum_{s \in Fact_{\mathsf{E}}(t_2)}(\phi_s(t_2) \odot s)$. The set $Fact_{\mathsf{E}}(t_2)$ contains at least two elements. By induction hypothesis, we know that for all $s_1, s_2 \in Fact_{\mathsf{E}}(t_2)$ such that $s_1 \neq s_2$, we have $s_1\theta \neq s_2\theta$. Hence, $t_2\theta$ is not a standard term whereas $t_1\theta$ is a standard term. This allows us to conclude.
- If t_1 and t_2 are both non-standard terms. Let $F = Fact_{\mathsf{E}}(t_1) \cup Fact_{\mathsf{E}}(t_2)$ and $x_1, \ldots, x_p$ the variables of t_1 and t_2. The terms t_1 and t_2 can be decomposed in the following way:

$$t_1 = \sum_{i=1}^{p}(\phi_{x_i}(t_1) \odot x_i) + \sum_{f \in F \setminus \mathcal{X}}(\phi_f(t_1) \odot f)$$
$$t_2 = \sum_{i+1}^{p}(\phi_{x_i}(t_2) \odot x_i) + \sum_{f \in F \setminus \mathcal{X}}(\phi_f(t_2) \odot f)$$

By definition of θ, we have that:

$$t_1\theta = \sum_{i=1}^{p}(\phi_{x_i}(t_1) \odot x_i) + \sum_{i=1}^{p}((\phi_{x_i}(t_1) \cdot c^{x_i}) \odot z) + \sum_{f \in F \setminus \mathcal{X}}(\phi_f(t_1) \odot f\theta)$$
$$t_2\theta = \sum_{i=1}^{p}(\phi_{x_i}(t_2) \odot x_i) + \sum_{i=1}^{p}((\phi_{x_i}(t_2) \cdot c^{x_i}) \odot z) + \sum_{f \in F \setminus \mathcal{X}}(\phi_f(t_2) \odot f\theta)$$

By hypothesis, we know that $t_1 \neq_{\mathsf{E}} t_2$. We distinguish two cases. Either there exists i $(1 \leq i \leq p)$ such that $\phi_{x_i}(t_1) \neq \phi_{x_i}(t_2)$. In such a case, we obtain that $t_1\theta \neq_{\mathsf{E}} t_2\theta$. Or, there exists $f \in F \setminus \mathcal{X}$ such that $\phi_f(t_1) \neq \phi_f(t_2)$. By induction hypothesis, for all $f, f' \in F \setminus \mathcal{X}$ such that $f \neq f'$, we have $f\theta \neq_{\mathsf{E}} f'\theta$. Hence, we obtain $t_1\theta \neq_{\mathsf{E}} t_2\theta$. □

Appendix E Satisfiability in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$ over the Reduced Signature

Proposition 60 *Let E be a monoidal equational theory for which $\mathcal{S}_{\mathsf{E}}$ is an Euclidean ring with norm v. If $\mathcal{C}$ is satisfiable, then there exists a solution σ to $\mathcal{C}$ with witnesses $C_1^\sigma, \ldots, C_k^\sigma$ satisfying the following condition:*

for all $i \in L(\mathcal{C})$, for all $y \in \mathcal{Y}$, $v(\phi_y(C_i^\sigma)) = 0$ or $v(\phi_y(C_i^\sigma)) < v(Q_{max}(\mathcal{C}))$.

PROOF. Let σ be a solution to $\mathcal{C}$ with witnesses $C_1^\sigma, \ldots, C_k^\sigma$. Moreover, we assume that we have chosen the solution and the contexts for which the

required condition is violated (if it is) for $\phi_{y_M}(C_N^\sigma)$ with (N, M) the biggest one (lexicographic order). In other words, if σ' with contexts $C_1^{\sigma'}, \ldots, C_k^{\sigma'}$ is a solution to $\mathcal{C}$, then there exists N' and M' with $(N', M') \preceq (N, M)$ such that $v(\phi_{y_{M'}}(C_{N'}^{\sigma'})) \not\leq v(Q_{max}(\mathcal{C}))$ and $v(\phi_{y_{M'}}(C_{N'}^{\sigma'})) \neq 0$.

In the following we construct, from σ, a solution σ' with witnesses $C_1^{\sigma'}, \ldots, C_k^{\sigma'}$. This solution fulfills the required condition for all $(i, j) \preceq (N, M)$. This contradicts the way we have chosen σ and $C_1^\sigma, \ldots, C_k^\sigma$. Hence, the result. The construction of σ' and the contexts $C_1^{\sigma'}, \ldots, C_k^{\sigma'}$ will be in four steps. Finally, we will prove that this is indeed a solution to $\mathcal{S}$.

(1) $\phi_{y_j}(C_i^{\sigma'}) = \phi_{y_j}(C_i^\sigma)$ for all $(i, j) \prec (N, M)$.

(2) Let $K, r \in \mathcal{S}_{\mathsf{E}}$ such that $v(r) < v(Q_{max}(\mathcal{C}))$ or $r = 0$ and $\phi_{y_M}(C_N^\sigma) = r + K \cdot Q_{max}(\mathcal{C})$. Let $\phi_{y_M}(C_N^{\sigma'}) = r$.

(3) Definition of $x\sigma'$ for $x \in vars(\mathcal{C})$.
Let $L(\mathcal{C}) = \{i_1, \ldots, i_\ell\}$. Our goal is to find σ' such that:
- for each $i \in L \setminus \{N\}$, $u_i\sigma - u_i\sigma' = 0$
- $u_N\sigma - u_N\sigma' = K \cdot Q_{max} \odot t_M\sigma$

To do this, we have to solve the following matrix equation (expressing equalities between terms), where the value of a variable x'_i corresponds to $x_i\sigma - x_i\sigma'$:

$$\begin{pmatrix} \phi_{x_1}(u_{i_1}) & \phi_{x_2}(u_{i_1}) & \ldots & \phi_{x_p}(u_{i_1}) \\ \vdots & & & \\ \phi_{x_1}(u_N) & \phi_{x_2}(u_N) & \ldots & \phi_{x_p}(u_N) \\ \vdots & & & \\ \phi_{x_1}(u_{i_\ell}) & \phi_{x_2}(u_{i_\ell}) & \ldots & \phi_{x_p}(u_{i_\ell}) \end{pmatrix} \odot \begin{pmatrix} x'_1 \\ \vdots \\ \vdots \\ x'_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ K \cdot Q_{max} \odot t_M\sigma \\ \vdots \\ 0 \end{pmatrix} \quad \text{(E.1)}$$

This can be achieved by solving the system of equations described below where the unknowns w_i take their value in $\mathcal{S}_{\mathsf{E}}$:

$$\begin{pmatrix} \phi_{x_1}(u_{i_1}) & \phi_{x_2}(u_{i_1}) & \ldots & \phi_{x_p}(u_{i_1}) \\ \vdots & & & \\ \phi_{x_1}(u_N) & \phi_{x_2}(u_N) & \ldots & \phi_{x_p}(u_N) \\ \vdots & & & \\ \phi_{x_1}(u_{i_\ell}) & \phi_{x_2}(u_{i_\ell}) & \ldots & \phi_{x_p}(u_{i_\ell}) \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ \vdots \\ \vdots \\ w_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ K \cdot Q_{max} \\ \vdots \\ 0 \end{pmatrix} \quad \text{(E.2)}$$

Thanks to Fact 47 the equation (E.2) has a solution $(c_1, \ldots, c_p)$. As a consequence, $(c_1 \odot t_M\sigma, \ldots, c_p \odot t_M\sigma)$ is a solution to (E.1).

This allows us to define σ' on $vars(\mathcal{C})$ by:

$$x_i\sigma' = x_i\sigma - c_i \odot t_M\sigma \qquad \text{for all } i \text{ such that } 1 \leq i \leq p.$$

(4) Definition of $\phi_{y_q}(C_i^{\sigma'})$ for $(i,q) \succ (N,M)$.
We define $\phi_{y_q}(C_i^{\sigma'})$ in the following way:

$$\phi_{y_q}(C_i^{\sigma'}) = \begin{cases} \phi_{y_q}(C_i^{\sigma}) + \sum_{j=n+N}^{n+i-1} \left(\sum_{l=1}^{p} \phi_{x_l}(t_j) \cdot c_l \right) \cdot \phi_{y_j}(C_i^{\sigma}) & \text{if } q = M, i > N \\ \phi_{y_q}(C_i^{\sigma}) & \text{if } q \neq M \end{cases}$$

We have to verify that σ' is a solution to $\mathcal{C}$ and also that the contexts $C_1^{\sigma'}, \ldots, C_k^{\sigma'}$ are witnesses of this fact. First we can note that

$$t_j\sigma = t_j\sigma' \qquad \text{for } 1 \leq j < n+N \tag{E.3}$$

This is a direct consequence of the fact that $u_i\sigma = u_i\sigma'$ for $1 \leq i < N$ and of the well-definedness of $\mathcal{C}$.

Now, we proceed to the verification constraint by constraint by distinguishing three cases:

(1) Case $i < N$: This is immediate by (E.3) and the fact that $u_i\sigma = u_i\sigma'$ for $1 \leq i < N$.
(2) Case $i = N$: We notice that by construction:

$$r = \phi_{y_M}(C_N^{\sigma}) - K \cdot Q_{max}(\mathcal{C}) \tag{E.4}$$

Hence, let $\theta = \{y_1 \mapsto t_1, \ldots, y_{n+k-1} \mapsto t_{n+k-1}\}$, we have

$$C_N^{\sigma'}\theta\sigma' = \sum_{j=1}^{n+N-1} \phi_{y_j}(C_N^{\sigma'}) \odot t_j\sigma' \qquad \text{since } vars(C_N^{\sigma'}) \subseteq \{y_1, \ldots, y_{N-1}\}$$

$$= \sum_{j=1}^{M-1} \phi_{y_j}(C_N^{\sigma'}) \odot t_j\sigma' + \phi_{y_M}(C_N^{\sigma'}) \odot t_M\sigma' + \sum_{j=M+1}^{n+N-1} \phi_{y_j}(C_N^{\sigma'}) \odot t_j\sigma'$$

By definition $\phi_{y_M}(C_N^{\sigma'}) = r$

$$= \sum_{j=1}^{M-1} \phi_{y_j}(C_N^{\sigma}) \odot t_j\sigma + r \odot t_M\sigma + \sum_{j=M+1}^{n+N-1} \phi_{y_j}(C_N^{\sigma}) \odot t_j\sigma$$

(E.3) and $\phi_{y_j}(C_N^{\sigma}) = \phi_{y_j}(C_N^{\sigma'})$ for $j \neq M$

$$= \sum_{j=1}^{M-1} \phi_{y_j}(C_N^{\sigma}) \odot t_j\sigma + (\phi_{y_M}(C_N^{\sigma}) - K \cdot Q_{max}(\mathcal{C})) \odot t_M\sigma + \sum_{j=M+1}^{n+N-1} \phi_{y_j}(C_N^{\sigma}) \odot t_j\sigma$$

$$= \sum_{j=1}^{n+N-1} \phi_{y_j}(C_N^{\sigma}) \odot t_j\sigma - K.Q_{max}(\mathcal{C}) \odot t_M\sigma$$

$$= C_N^{\sigma}\theta\sigma - K \cdot Q_{max}(\mathcal{C}) \odot t_M\sigma$$

$$= u_N\sigma - K.Q_{max}(\mathcal{C}) \odot t_M\sigma \qquad \text{since } \sigma \text{ is a solution to } \mathcal{C}$$

$$= u_N\sigma' \qquad \text{by definition of } \sigma'.$$

(3) Case $i > N$: We consider the i^{th} constraint of $\mathcal{C}$, *i.e.* $t_1, t_2, \ldots, t_{n+i-1} \Vdash u_i$. Note that, using $x_i\sigma' = x_i\sigma - c_i \odot t_M\sigma$, we get that:

$$\begin{aligned} t_j\sigma' &= \sum_{v \in Fact_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C})} \phi_v(t_j) \odot v\sigma' + \sum_{v \in vars(\mathcal{C})} \phi_v(t_j) \odot v\sigma' \\ &= \sum_{v \in Fact_{\mathsf{E}}(\mathcal{C}) \setminus vars(\mathcal{C})} (\phi_v(t_j) \odot v) \\ &\quad + \sum_{l=1}^{p} (\phi_{x_l}(t_j) \odot x_l\sigma) - \sum_{l=1}^{p} (c_l \cdot \phi_{x_l}(t_j) \odot t_M\sigma) \\ &= t_j\sigma - \sum_{l=1}^{p} (c_l \cdot \phi_{x_l}(t_j) \odot t_M\sigma) \end{aligned} \qquad \text{(E.5)}$$

Hence, we have:

$$C_i^{\sigma'}\theta\sigma' = \sum_{j=1}^{n+i-1} \phi_{y_j}(C_i^{\sigma'}) \odot t_j\sigma' \qquad \text{since } vars(C_i^{\sigma'}) \subseteq \{y_1, \ldots, y_{N+i-1}\}$$

$$= \sum_{j=1}^{M-1} \phi_{y_j}(C_i^{\sigma'}) \odot t_j\sigma' + \phi_{y_M}(C_i^{\sigma'}) \odot t_M\sigma' + \sum_{j=M+1}^{n+N-1} \phi_{y_j}(C_i^{\sigma'}) \odot t_j\sigma' + \sum_{j=n+N}^{n+i-1} \phi_{y_j}(C_i^{\sigma'}) \odot t_j\sigma'$$

$$= \sum_{j=1}^{M-1} \phi_{y_j}(C_i^{\sigma}) \odot t_j\sigma + \phi_{y_M}(C_i^{\sigma'}) \odot t_M\sigma + \sum_{j=M+1}^{n+N-1} \phi_{y_j}(C_i^{\sigma}) \odot t_j\sigma + \sum_{j=n+N}^{n+i-1} \phi_{y_j}(C_i^{\sigma}) \odot t_j\sigma'$$

(E.3) and $\phi_{y_j}(C_i^{\sigma}) = \phi_{y_j}(C_N^{\sigma'})$ for $j \neq M$

$$= \sum_{j=1}^{M-1} \phi_{y_j}(C_i^{\sigma}) \odot t_j\sigma + \left(\phi_{y_M}(C_i^{\sigma}) + \sum_{j=n+N}^{n+i-1} (\sum_{l=1}^{p} \phi_{x_l}(t_j) \cdot c_l) \cdot \phi_{y_j}(C_i^{\sigma})\right) \odot t_M\sigma + \sum_{j=M+1}^{n+N-1} \phi_{y_j}(C_i^{\sigma}) \odot t_j\sigma + \sum_{j=n+N}^{n+i-1} \phi_{y_j}(C_i^{\sigma}) \cdot \left(t_j\sigma - \sum_{l=1}^{p} (\phi_{x_l}(t_j) \cdot c_l \odot t_M\sigma)\right) \tag{E.5}$$

$$= \sum_{j=1}^{n+i-1} \phi_{y_j}(C_i^{\sigma}) \odot t_j\sigma$$

$$= C_i^{\sigma}\theta\sigma$$

$$= u_i\sigma \qquad \text{since } \sigma \text{ is a solution to } \mathcal{C}$$

$$= u_i\sigma' \qquad \text{since } u_i\sigma = u_i\sigma' \text{ for } i > N.$$

Hence, we conclude that σ' is a solution to $\mathcal{C}$. By construction of σ', we have $v(\phi_{y_j}(C_i^{\sigma'})) < v(Q_{\max}(\mathcal{C}))$ or $v(\phi_{y_j}(C_i^{\sigma'})) = 0$ for all $(i, j) \preceq (N, M)$. Hence we obtain a contradiction and we conclude. □

Proposition 61 *Let* E *be a monoidal equational theory that is unitary for elementary unification, and such that* $\mathcal{S}_{\mathsf{E}}$ *is an Euclidean ring with norm* v *with*

$$\textit{for any } q \in \mathcal{S}_{\mathsf{E}}\textit{, the set } \{e \in \mathcal{S}_{\mathsf{E}} \mid v(e) < v(q)\} \textit{ is finite}$$

and such that there is an algorithm to compute solutions of inhomogeneous linear equation over $\mathcal{S}_{\mathsf{E}}$*. Then algorithm 5 allows us to decide the satisfiability of a well-defined constraint system* $\mathcal{C}$ *(on the reduced signature) in* $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$*.*

PROOF. Algorithm 5 is clearly sound. Now, it remains to show that it is also complete. Assume that $\mathcal{C}$ has a solution in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$. By Proposition 60, we know that if there exists a solution to $\mathcal{C}$ then there exists a solution σ to $\mathcal{C}$ with witnesses $C_1, \ldots, C_k$ satisfying the following condition:

$$\text{for all } i \in L(\mathcal{C}), \text{ for all } y \in \mathcal{Y},\ v(\phi_y(C_i)) = 0 \text{ or } v(\phi_y(C_i)) < v(Q_{max}(\mathcal{C})).$$

Hence, for all $i \in L(\mathcal{C})$ and for all $j \in \{1, \ldots, n+i-1\}$ we can guess the value of $\phi_{y_j}(C_i)$ since there is only a finite number of possibilities. It remains to show that the algorithm we propose to decide whether there exists a substitution that is both a solution to

- the unification problem $\mathcal{U} = \{C_i[t_1, \ldots, t_{n+i-1}] = u_i \mid i \in L(\mathcal{C})\}$ (modulo E), and
- the set of deducibility constraint $\{t_1, \ldots, t_{n+i-1} \Vdash u_i \mid i \notin L(\mathcal{C})\}$ (in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$)

is complete.

By hypothesis, σ is a solution to the problem described above. Hence the unification problem $\mathcal{U}$ has a solution. Let Θ be the set of solutions of $\mathcal{U}$. Now, we are going to show that:

Fact 74 *for all* $\theta_1, \theta_2 \in \Theta$*, we have:*

(1) $\mathcal{C}\theta_1 = \mathcal{C}\theta_2$*, and*
(2) $\mathcal{C}\theta_1$ *is a system of ground constraints.*

Hence, thanks to this fact, we obtain that $\mathcal{C}\theta = \mathcal{C}\sigma$. Moreover $\mathcal{C}\theta$ is a set of ground constraints satisfiable in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$. Note that satisfiability of ground constraints in $(\mathcal{I}_{\mathsf{M}_{\mathsf{E}}}, \mathcal{R}_{\mathsf{E}})$ is decidable since we can solve by hypothesis inhomogeneous equation systems over $\mathcal{S}_{\mathsf{E}}$ (see Example 21).

We are going to prove Fact 74 by induction on the number i of constraints in the constraint system $\mathcal{C}$. The base case $i = 1$ is obvious. Indeed, we have

either $1 \notin L(\mathcal{C})$ and all the terms of the constraint are ground, or otherwise $1 \in L(\mathcal{C})$. In this case, the fact that $\theta_1, \theta_2 \in \Theta$ allows us to deduce that $u_1\theta_1 = u_1\theta_2$. Since $t_1, \ldots, t_n$ are ground we have that $u_1\theta_1$ is ground.

Now, we consider a system of $i+1$ constraints. We know by induction hypothesis that for all $\theta_1, \theta_2 \in \Theta$, we have:

- for $1 \leq j \leq n+i-1$, we have $t_j\theta_1 = t_j\theta_2$ and $t_j\theta_1$ is ground,
- for $1 \leq j \leq i$, we have $u_j\theta_1 = u_j\theta_2$ and $u_j\theta_1$ is ground.

We distinguish two cases:

Case $i+1 \in L(\mathcal{C})$**:** We have $u_{i+1}\theta_1 = u_{i+1}\theta_2 = C_i[t_1\theta_1, \ldots, t_{n+i}\theta_1]$. By induction hypothesis, we know that $t_1\theta_1, \ldots, t_{n+i-1}\theta_1$ are ground. Moreover, we can show that $t_{n+i}\theta_1$ is also ground thanks to the well-definedness of the constraint system $\mathcal{C}$. Hence, we deduce that $u_{i+1}\theta_1$ is ground. This allows us to conclude.

Case $i+1 \notin L(\mathcal{C})$**:** We conclude thanks to the well-definedness of $\mathcal{C}$. □