# Verifying equivalence properties of security protocols

Daniel Pasailă
email: daniel.pasaila@gmail.com
Advisors: Stephanie Delaune and Steve Kremer

August 19, 2011

## 1 Introduction

Security protocols are used nowadays for securing transactions through public channels, like the Internet. Typical examples of applications include electronic commerce, electronic voting or mobile ad hoc networking. In order to obtain as much confidence as possible, several formal methods have been proposed for analyzing properties of security protocols. Depending on the goals which a security protocol has, there are several types of properties that need to be verified. First, there are reachability or trace-based properties, which express the fact that a bad state cannot be reached. Two classical reachability properties are secrecy and authentication. Secrecy expresses the fact that a secret key or nonce cannot become public and authentication is used for ensuring an agent of other's identity. However, there are some security properties, like privacy, that cannot be formulated in terms of reachability. These can be modeled using equivalence-based properties, usually used to express indistinguishably, a security property satisfied when an observer cannot distinguish between two processes. This is crucial in proving anonymity properties, where an attacker should not be able to distinguish a run involving an agent $A$ from a run involving another participant $A'$. Anonymity is also used in the context of electronic voting, where two different runs of the voting protocol should be indistinguishable for the attacker in order to ensure that no information is leaked about the vote of a participant. Another equivalence-based property is resistance to off line

Due to the fact that the author does not have a proper command of French, this report is written in English.

guessing attacks, which occur when an attacker is able to guess a secret by just trying every possible value for it.

Several reachability and equivalence-based properties have been successfully analyzed using symbolic methods. Used for detecting logical flaws in protocols, symbolic methods have been introduced by Dolev and Yao in early 80s [1]. In the symbolic model, messages are represented by an abstract term algebra and nonces by fresh names. Two different nonces are represented by different names and they are never equal. The attacker has full control over the network: it can read all the exchanged messages and can reply by constructing new messages according to his knowledge and a predefined set of rules. Moreover, the attacker may initiate an unbounded number of sessions with the honest participants. In other computational models the attacker is a probabilistic Turing machine, and messages are bitstrings that do not have any particular structure. Nonces are represented by random numbers drawn from a specific distribution, thus two nonces can be equal with small probability.

Among symbolic approaches that have been successfully used is constraint solving. Introduced by J.Millen and V.Shmatikov [2], this technique is suitable for verifying security properties for bounded number of sessions. A symbolic trace of a protocol is an interleaving of roles of the participants, and it can be represented using a constraint system. Let us consider the following Example which uses the Handshake protocol [3, 4]:

$$\begin{array}{ll} A \to B: & \{N\}_{k_{AB}} \\ B \to A: & \{f(N)\}_{k_{AB}}, \end{array}$$

where $\{x\}_{k_{AB}}$ denotes the encryption of the message $x$ with the key $k_{AB}$. The goal of this protocol is to authenticate $B$ to $A$, provided that they share the symmetric encryption key $k_{AB}$. First, $A$ challenges $B$ by creating a nonce $N$ and sending it to $B$, encrypted with the shared key $k_{AB}$. Then $B$ receives the message, decrypts it with $k_{AB}$ obtaining $N$, applies a previously given function $f$ (for instance $f(N) = N + 1$) and sends it to $A$. Finally $A$ checks the validity of the response by decrypting the received message and confruting it with $f(N)$. Suppose that we want to prove the authentication property for two sessions on our example. Consider the following symbolic

trace of the protocol, where the intruder $I$ interleaves between $A$ and $B$ :

$$\begin{array}{lll} A & \xrightarrow{\{N\}_{k_{AB}}} & I \\ & & I \qquad \xrightarrow{x_1} \qquad B \\ & & I \quad \xleftarrow{\{f(sdec(x_1,k_{AB}))\}_{k_{AB}}} \quad B \\ A & \xleftarrow{x_2} & I \end{array}$$

Here, $sdec(x, k)$ denotes the decryption of the message $x$ with the key $k$. Notice that since this is a symbolic trace, all the messages that are sent by the intruder are encoded by variables. Thus, an attack on this symbolic trace exists iff the intruder intruder can deduce messages $x_1$ and $x_2$ such that $sdec(x_2, k_{AB}) = f(N)$. This can be answered by solving the following constraint system:

$$\exists x_1, x_2, \begin{cases} X_1[\{N\}_{k_{AB}}] & =^? & x_1 \\ X_2[\{N\}_{k_{AB}}, \{f(sdec(x_1, k_{AB}))\}_{k_{AB}}] & =^? & x_2 \\ sdec(x_2, k_{AB}) & = & f(n). \end{cases}$$

Intuitively, the first line means that $x_1$ must be computable from the message sent by $A$ to the intruder, which is $\{N\}_{k_{AB}}$. The computation used for computing $x_1$ is denoted by $X_1$. Then, $B$ receives $x_1$, decrypts it, applies the function $f$ and sends the result to the intruder, encrypted with $k_{AB}$. Thus, the intruder receives the message $\{f(sdec(x_1, k_{AB}))\}_{k_{AB}}$ from $B$. Then it must compute a message $x_2$ that satisfies the test made by $A$, which is $sdec(x_2, k_{AB}) = f(N)$. It can be seen that by taking $x_1 = \{N\}_{k_{AB}}$ and $x_2 = \{f(sdec(x_1, k_{AB}))\}_{k_{AB}} = \{f(N)\}_{k_{AB}}$ we obtain a valid attack on this symbolic trace, thus the protocol is not safe for two sessions. The variables $X_1, X_2$ are called second order variables and they are used for encoding the computations used for obtaining $x_1$ and $x_2$, which are first order variables.

Two constraint systems are considered to be equivalent if they have the same second order solutions. In other words, their first order solutions can be computed by using the same set of computations. Equivalence of constraint systems is a procedure which is used more and more lately as a subroutine in algorithms deciding equivalence-based properties. This is the case for [5], where a method for deciding trace equivalence is proposed. In [6] the problem of off line guessing attacks is studied. A protocol is said to be subject to off line guessing attacks iff an attacker is able to guess a secret by trying every value for it. To decide whether a protocol is subject to off line guessing attacks, it has been shown in [6] that it suffices to construct two constraint systems for each symbolic trace and decide whether they are equivalent.

**Our contribution** Algorithms for deciding equivalence of constraint systems have been proposed in [6] for subterm convergent equational theories. While this suffices for expressing properties of digital signatures, pairing, symmetric and asymmetric encryptions, it does not provide enough means for dealing with arithmetic operations like addition, multiplication or exclusive or. While many formal analysis abstract from this low-level operators, many attacks and weaknesses rely on these properties. For example, attacks exploiting the exclusive or properties have been showed in [7], in the context of mobile communications. In this report we propose a procedure for deciding equivalence of constraint systems when using the Abelian Groups and Exclusive Or equational theories.

**Related Work** When the number of sessions is unbounded, many reachability properties have been proved to be undecidable. For example secrecy has been shown to be undecidable [8, 9] even if the size of the exchanged messages is bounded [10]. For bounded number of sessions, an algorithm for trace equivalence is proposed in [5], for theories that contain only signatures, pairing, symmetric and asymmetric encryptions. In [11] it has been shown that trace equivalence can be reduced to equivalence of finitely many pairs of constraint systems in the case of determinate processes. In [6] an algorithm for deciding equivalence of constraint systems is given for subterm convergent equational theories.

Recently procedures that combine algorithms for disjoint intruder theories have been studied. In [12] it has been shown that if satisfiability of constraint systems is decidable for two disjoint intruder theories, then it is also decidable for their reunion. Similar combination results have been shown for deductibility and an indistinguishably property called static equivalence in [13].

# 2 Preliminaries

## 2.1 Signatures, terms and substitutions

A signature $\Sigma$ is a set of functional symbols $\mathcal{F}$ with an associated non-negative arity function $ar$ defined over $\mathcal{F}$. Having a set of variables $\mathcal{X}$, let $\mathcal{T}(\mathcal{F}, \mathcal{X})$ be the set of terms built over the set of variables $\mathcal{X}$ using functional symbols in $\mathcal{F}$. A term is closed if it has no variables and public if it does not contain any private functional symbol. Constants are functional symbols of arity 0. The set $\mathcal{F}$ is partitioned into the set of public symbols $\mathcal{F}_{pub}$ and the set of private symbols $\mathcal{F}_{priv}$. We assume the existence of an additional set

of constants $\mathcal{W} = \{w_1, w_2, \cdots\}$ called parameters, which are separate from $\mathcal{F}$. We also assume the existence of an infinite amount of private and public constants.

We fix an infinite set of variables $\mathcal{X}$, partitioned into the set of first order variables $\mathcal{X}^1 = \{x, y, \cdots\}$ and the set of second order variables $\mathcal{X}^2 = \{X, Y, \cdots\}$, which are given with nonnegative arities $ar(X), ar(Y), \cdots$ . We distinguish the following sets of terms:

- $\mathcal{T}(\mathcal{F}, \mathcal{X}^1)$, which are called first order terms and are denoted by $t, s, \cdots$ ,
- $\mathcal{T}(\mathcal{F}_{pub} \cup \mathcal{W}, \mathcal{X}^2)$, which are called second order terms and are denoted by $M, N, \cdots$ ,
- $\mathcal{T}(\mathcal{F} \cup \mathcal{W}, \mathcal{X})$, which are general terms denoted by $T, S, \cdots$ .

Substitutions are defined as sets of pairs written $\sigma = \{x_1 \to T_1, \cdots, x_n \to T_n\}$, where $dom(\sigma) = \{x_1, \cdots, x_n\}$. We assume that $dom(\sigma) \subset \mathcal{X}$. The substitution $\sigma$ is closed iff all terms $T_1, \cdots, T_n$ are closed. The application of a substitution $\sigma$ to a term $T$ is denoted as $T\sigma$. Next, we extend the notion of arity to general terms. Having a term $T$, $ar(T)$ denotes the maximum of the indexes of parameters contained in $T$ and arities of second order variables contained in $T$. A substitution $\sigma$ is well formed iff it assigns first order terms to first order variables and second order terms to second order variables, such that for any pair $X \to M \in \sigma$ we have that $ar(M) \leq ar(X)$. Arities are used to restrict the maximum index of parameters of terms that can replace a second order variable. Thus, the arity of a term cannot increase after applying multiple well formed substitutions. For example, the term $w_5$ contains only one parameter, and is of arity 5. By applying only well formed substitutions, the resulting terms can only contain parameters $w_1, \cdots, w_5$.

## 2.2 Equational theories

**Definition 2.1** (Equational theory)**.** *Having a signature $\Sigma = \{\mathcal{F}, ar\}$, an equational theory over $\Sigma$ is a set of pairs of terms $E = \{(T, S) \mid T, S \in \mathcal{T}(\mathcal{F} \cup \mathcal{W}, \mathcal{X})\}$. We define the equality modulo $E$, denoted as $=_E$, as the smallest equivalence relation such that:*

1. *$(T, S) \in E$ implies that $T =_E S$,*
2. *$=_E$ is closed under substitutions (not necessarily well formed) of variables with terms*
3. *$=_E$ is closed under application of functional symbols*

4. $=_E$ *is closed under bijective renaming of constants that do not appear in* $E$

**Example 2.1.** *Let* $\Sigma_+ = \{+, 0\}$ *be the signature containing a constant symbol* $0$ *and a binary symbol* $+$*. Moreover, let* $E_+$ *(Exclusive Or) be the equational theory defined by the following equations:*

$$\begin{array}{lcl@{\quad}lcl} (x+y)+z & = & x+(y+z) \quad (A) & x+0 & = & x \quad (U) \\ x+y & = & y+x \quad (C) & x+x & = & 0 \quad (N) \end{array}$$

*If* $t_1, t_2$ *and* $t_3$ *are terms, we have that* $t_1 + (t_2 + t_1) =_{E_+} t_2$ *by applying rules (C), (A), (N) and (U).*

**Example 2.2.** *Let* $\Sigma_{AG} = \{+, -, 0\}$ *be the signature containing a constant symbol* $0$*, a binary symbol* $+$ *and a unary symbol* $-$*. Moreover, let* $E_{AG}$ *(Abelian Groups) be the equational theory defined by the following equations:*

$$\begin{array}{lcl@{\quad}lcl} (x+y)+z & = & x+(y+z) \quad (A) & x+0 & = & x \quad (U) \\ x+y & = & y+x \quad (C) & x+-(x) & = & 0 \quad (Inv) \end{array}$$

*If* $t_1, t_2$ *and* $t_3$ *are terms, we have that* $-(t_1 + t_2) =_{E_{AG}} -(t_1) + -(t_2)$.

## 2.3 Intruder Constraint Systems

**Definition 2.2.** *Let* $E$ *be an equational theory and* $\mathcal{Y} = \{X_1, \cdots, X_m\}$ *a set of* $m$ *distinct second order variables that satisfy* $ar(X_i) \leq ar(X_{i+1}), 1 \leq i < m$*. An intruder constraint system (or constraint system) defined over* $E$ *and* $\mathcal{Y}$ *is a system of equations* $\mathcal{C}$ *of the form*

$$\exists x_1, \cdots, x_m, \left\{ \begin{array}{rcl} X_1[t_1, \cdots, t_{ar(X_1)}] & =^? & x_1 \\ & \cdots & \\ X_m[t_1, \cdots, t_{ar(X_m)}] & =^? & x_m \\ s_1 & =^?_E & s'_1 \\ & \cdots & \\ s_n & =^?_E & s'_n \end{array} \right.$$

*such that the following hold:*

1. $var(s_1, s'_1, \cdots, s_n, s'_n) \subseteq \{x_1, \cdots, x_m\}$*, where* $s_1, s'_1, \cdots, s_n, s'_n$ *are first order terms,*

2. $\forall 1 \leq i \leq m, \forall 1 \leq j \leq ar(X_i), var(t_j) \subseteq \{x_1, \cdots, x_{i-1}\}$ *(origination), where each* $t_j$ *is a first order term.*

A solution to $\mathcal{C}$ is a substitution $\theta$ that is closed (does not contain any variables), well formed with $dom(\theta) = \{X_1, \cdots, X_m\}$ for which there exists a closed, well formed substitution $\sigma$ with $dom(\sigma) = \{x_1, \cdots, x_m\}$ such that the following conditions are satisfied:

1. $(X_i\theta)[t_1\sigma, \cdots, t_{ar(X_i)}\sigma] = x_i\sigma, 1 \leq i \leq m$,
2. $s_i\sigma = s'_i\sigma, 1 \leq i \leq n$.

The substitution $\sigma$ is called the first order extension of $\theta$. Due to the origination property, the first order extension of a substitution $\theta$ is always unique. We denote by $\theta \models \mathcal{C}$ the fact that $\theta$ is a solution to $\mathcal{C}$.

# 3 Deciding equivalence of constraint systems for $E_{AG}$ and $E_+$ equational theories

We say that two constraint systems are equivalent if they have the same set of second order solutions. In this section we study the problem of equivalence when considering the Abelian Groups equational theory described in Example 2.2. We must note that this result can be easily adapted for Exclusive Or equational theory described in Example 2.1.

In the following we focus on Abelian Groups, thus we only consider the signature $\Sigma_{AG}$ and the equational theory $E_{AG}$ described in Example 2.2. Moreover, we assume that the signature contains an infinite number of constants. Having two constraint systems $\mathcal{C}^1$ and $\mathcal{C}^2$ defined over the same set of second order variables $\mathcal{Y} = \{X_1, \cdots, X_m\}$, we denote by $\mathcal{C}^1 \subseteq \mathcal{C}^2$ the fact that the set of solutions of $\mathcal{C}^1$ is included in the set of solutions of $\mathcal{C}^2$. If $\mathcal{C}^1 \subseteq \mathcal{C}^2$ we will also say that $\mathcal{C}^1$ is included in $\mathcal{C}^2$. Since for deciding equivalence between $\mathcal{C}^1$ and $\mathcal{C}^2$ it suffices to decide whether $\mathcal{C}^1 \subseteq \mathcal{C}^2$, we will focus on this problem for the rest of the section. We will show how to decide whether $\mathcal{C}^1 \subseteq \mathcal{C}^2$ in five different steps:

1. we simplify the problem of deciding whether $\mathcal{C}^1 \subseteq \mathcal{C}^2$ to deciding whether a simple constraint system is included in a general constraint system, where a simple constraint system is a constraint system for which the terms $t_1, \cdots, t_{ar(X_m)}$ are closed,
2. we show that for deciding whether $C_1 \subseteq C_2$ it suffices to decide whether the set of solutions of $\mathcal{C}^1$ that contain only constants that appear in $\mathcal{C}^1$ are also solutions of $\mathcal{C}^2$,

3. we show how to encode solutions of a constraint system $\mathcal{C}$ that contain only constants that appear in $\mathcal{C}$ in a system of equations,

4. we show that it can be decided whether the solutions of a system of linear equations are included in the set of solutions of another system of nonlinear equations,

5. we conclude by showing that it can be decided whether a simple constraint system is included in a general constraint system by using the fact that only systems of linear equations are needed for encoding simple constraint systems.

### 3.1 Simplifying the problem of inclusion

Let $\mathcal{C}$ be the constraint system defined by

$$\begin{cases} X_1[t_1, \cdots, t_{ar(X_1)}] & =^? & x_1 \\ & \cdots & \\ X_m[t_1, \cdots, t_{ar(X_m)}] & =^? & x_m \\ s_1 & =^?_{E_{AG}} & s'_1 \\ & \cdots & \\ s_n & =^?_{E_{AG}} & s'_n. \end{cases}$$

For any terms $t_1, t_2$, let $t_1 - t_2$ denote $t_1 + (-t_2)$. Let $\mathcal{T} = \{w_1 \to w_1 - M_1, \cdots, w_{ar(X_m)} \to w_{ar(X_m)} - M_m\}$ be a substitution with $dom(\mathcal{T}) = \{w_1, \cdots, w_{ar(X_m)}\}$. We say that the substitution $\mathcal{T}$ is compatible with $\mathcal{C}$ iff $M_1, \cdots, M_m$ are second order terms that do not contain parameters which, for all $1 \leq i \leq m$, satisfy $var(M_i) \subseteq \{X_1, \cdots, X_{p_i - 1}\}$, where $p_i = \min\{j \mid ar(X_j) >= i, 1 \leq j \leq m\}$. Next, we define the constraint system $\mathcal{C}_\mathcal{T}$ as

$$\begin{cases} X_1[t'_1, \cdots, t'_{ar(X_1)}] & =^? & x_1 \\ & \cdots & \\ X_m[t'_1, \cdots, t'_{ar(X_m)}] & =^? & x_m \\ s_1 & =^?_E & s'_1 \\ & \cdots & \\ s_n & =^?_E & s'_n \end{cases}$$

where, for all $1 \leq i \leq ar(X_m), t'_i = t_i + M_i[x_1/X_1, \cdots, x_{ar(X_m)}/X_{ar(X_m)}]$. Notice that, if $\mathcal{T}$ is compatible with $\mathcal{C}$, the origination property is satisfied for $\mathcal{C}_\mathcal{T}$, thus this is a well defined constraint system. Let $\theta$ be a closed, well

formed substitution with $dom(\theta) = \{X_1, \cdots, X_m\}$. We denote by $\theta_{\mathcal{T}}$ the substitution $(\theta \circ \mathcal{T})^m$. Next, we give a lemma which will be used later for symplyfing the inclusion problem.

**Lemma 3.1.** *Let $\mathcal{C}$ be a constraint system defined as above and $\mathcal{T} = \{w_1 \to w_1 - M_1, \cdots, w_{ar(X_m)} \to w_{ar(X_m)} - M_m\}$ be a substitution compatible with $\mathcal{C}$. Let $\theta = \{X_1 \to N_1, \cdots, X_m \to N_m\}$ be a closed, well formed substitution. Then, the first order extension of $\theta$ for $\mathcal{C}$ is equal to the first order extension of $\theta_{\mathcal{T}}$ for $\mathcal{C}_{\mathcal{T}}$.*

*Proof.* Let $\sigma$ be the first order extension of $\theta$ for the constraint system $\mathcal{C}$. We will prove by induction that, for all $1 \leq i \leq m$, $X_i(\theta \circ \mathcal{T})^i[t'_1\sigma, \cdots, t'_{ar(X_i)}\sigma] = X_i\theta[t_1\sigma, \cdots, t_{ar(X_i)}\sigma]$, which suffices since $X_i\theta[t_1\sigma, \cdots, t_{ar(X_i)}\sigma] = x_i\sigma$. For the rest of the proof, let $M'_i = M_i[x_1/X_1, \cdots, x_{ar(X_m)}/X_{ar(X_m)}]$ for all $1 \leq i \leq ar(X_m)$.

The base case ($i = 1$) follows from the fact that the terms $t_1, \cdots, t_{ar(X_1)}$ are closed. Moreover, due to the constraints of the substitution $\mathcal{T}$, the terms $t'_1, \cdots, t'_{ar(X_1)}$ are also closed. Thus we have the following equalities:

$$\begin{aligned} X_1\theta[t_1\sigma, \cdots, t_{ar(X_1)}\sigma] &= \\ X_1\theta[t_1, \cdots, t_{ar(X_1)}] &= \\ X_1\theta[t'_1 - M'_1, \cdots, t'_{ar(X_1)} - M'_{ar(x_1)}] &= \\ X_1(\theta \circ \mathcal{T})[t'_1, \cdots, t'_{ar(X_1)}] &= \\ X_1(\theta \circ \mathcal{T})[t'_1\sigma, \cdots, t'_{ar(X_1)}\sigma]. & \end{aligned}$$

Suppose now that $X_j(\theta \circ \mathcal{T})^j[t'_1\sigma, \cdots, t'_{ar(X_j)}\sigma] = X_j\theta[t_1\sigma, \cdots, t_{ar(X_j)}\sigma]$ holds for all $1 \leq j < i$. It remains to prove that the hypothesis also holds for $i$. We have the following equalities:

$$\begin{aligned} X_i\theta[t_1\sigma, \cdots, t_{ar(X_i)}\sigma] &= \\ X_i\theta[t'_1\sigma - M'_1\sigma, \cdots, t'_{ar(X_i)}\sigma - M'_{ar(X_i)}\sigma] &= \\ X_i\theta[t'_1\sigma - M_1, \cdots, t'_{ar(X_i)}\sigma - M_{ar(X_i)}]\theta[t_1\sigma, ..., t_{ar(X_{i-1})}\sigma] &= \\ X_i(\theta \circ \mathcal{T})[t'_1\sigma, \cdots, t'_{ar(X_i)}\sigma](\theta \circ \mathcal{T})^{i-1}[t'_1\sigma, \cdots, t'_{ar(X_{i-1})}\sigma] &= \\ X_i(\theta \circ \mathcal{T})^i[t'_1\sigma, \cdots, t'_{ar(X_i)}\sigma]. & \end{aligned}$$

The third equality follows from the fact that, for all $1 \leq j \leq ar(X_i)$, we have that $M'_j\sigma = M_j\theta[t_1\sigma, \cdots, t_{ar(X_{i-1})}\sigma]$. The forth equality follows from the induction hypothesis and the definition of $\mathcal{T}$. □

Next we give two examples which illustrate Lemma 3.1.

**Example 3.1.** *Let $\mathcal{C}$ be the constraint system defined by*

$$\left\{\begin{array}{rcl} X_1[a,b] & =^? & x_1 \\ X_2[a,b,c+2x_1] & =^? & x_2 \\ x_1+x_2 & =^?_{E_{AG}} & c. \end{array}\right.$$

*Let $\mathcal{T} = \{w_1 \to w_1, w_2 \to w_2, w_3 \to w_3 - (-2X_1)\}$ be a substitution compatible with $\mathcal{C}'$. Then, the constraint system $\mathcal{C}_\mathcal{T}$ is defined by*

$$\left\{\begin{array}{rcl} X_1[a,b] & =^? & x_1 \\ X_2[a,b,c] & =^? & x_2 \\ x_1+x_2 & =^?_{E_{AG}} & c. \end{array}\right.$$

*Consider the substitution $\theta = \{X_1 \to w_1+w_2, X_2 \to -3w_1-3w_2+w_3\}$. It follows that the first order extension of $\theta$ for $\mathcal{C}$ is the substitution $\sigma = \{x_1 \to a+b, x_2 \to -a-b+c\}$. Next, we have that $(\theta \circ \mathcal{T}) = \{X_1 \to w_1+w_2, X_2 \to -3w_1-3w_2+w_3+2X_1\}$, thus $\theta_\mathcal{T} = (\theta \circ \mathcal{T})^2 = \{X_1 \to w_1+w_2, X_2 \to -w_1-w_2+w_3\}$. It follows that $\sigma$ is also the first order extension of $\theta_\mathcal{T}$ for $\mathcal{C}_\mathcal{T}$. Notice that $\theta \models \mathcal{C}$ and $\theta_\mathcal{T} \models \mathcal{C}_\mathcal{T}$.*

**Example 3.2.** *Let $\mathcal{C}'$ be the constraint system defined by*

$$\left\{\begin{array}{rcl} X_1[a,b] & =^? & x_1 \\ X_2[a,b,c+x_1] & =^? & x_2 \\ x_2+2x_1 & =^?_{E_{AG}} & c. \end{array}\right.$$

*Let $\mathcal{T} = \{w_1 \to w_1, w_2 \to w_2, w_3 \to w_3 - (-2X_1)\}$ be a substitution compatible with $\mathcal{C}$, as in Example 3.1. Then, the constraint system $\mathcal{C}'_\mathcal{T}$ is defined by*

$$\left\{\begin{array}{rcl} X_1[a,b] & =^? & x_1 \\ X_2[a,b,c-x_1] & =^? & x_2 \\ x_2+2x_1 & =^?_{E_{AG}} & c. \end{array}\right.$$

*Again, let $\theta = \{X_1 \to w_1+w_2, X_2 \to -3w_1-3w_2+w_3\}$ be defined as in Example 3.1. It follows that the first order extension of $\theta$ for $\mathcal{C}'$ is the substitution $\sigma = \{x_1 \to a+b, x_2 \to -2a-2b+c\}$. It can be shown similar as in Example 3.1 that $\theta \models \mathcal{C}'$ and $\theta_\mathcal{T} \models \mathcal{C}'_\mathcal{T}$.*

In the the rest of this section we show how to simplify the problem of deciding whether $\mathcal{C}^1 \subseteq \mathcal{C}^2$ by using the above result.

**Lemma 3.2.** *If $\mathcal{C}^1 \subseteq \mathcal{C}^2$ then, for each substitution $\mathcal{T} = \{w_1 \to w_1 - M_1, \cdots, w_{ar(X_m)} \to w_{ar(X_m)} - M_m\}$ which is compatible with $\mathcal{C}^1$ (and $\mathcal{C}^2$), we have that $\mathcal{C}^1_{\mathcal{T}} \subseteq \mathcal{C}^2_{\mathcal{T}}$.*

*Proof.* First, note that since $\mathcal{C}^1$ and $\mathcal{C}^2$ are defined over the same set of second order variables $\mathcal{Y}$, every substitution $\mathcal{T}$ compatible with $\mathcal{C}^1$ is also compatible with $\mathcal{C}^2$.

We start by defining $\mathcal{T}^- = \{w_1 \to w_1 - (-M_1), \cdots, w_{ar(X_m)} \to w_{ar(X_m)} - (-M_m)\}$. It directly follows that $\mathcal{T}^-$ is compatible with $\mathcal{C}^1_{\mathcal{T}}$ and $\mathcal{C}^2_{\mathcal{T}}$. By definition we have that $\mathcal{C}^1_{\mathcal{T}_{\mathcal{T}^-}} = \mathcal{C}_1$ and $\mathcal{C}^2_{\mathcal{T}_{\mathcal{T}^-}} = \mathcal{C}_2$.

Suppose by contradiction that $\mathcal{C}^1_{\mathcal{T}} \not\subseteq \mathcal{C}^2_{\mathcal{T}}$. Then, there exists a substitution $\theta$ such that $\theta \models \mathcal{C}^1_{\mathcal{T}}$ and $\theta \not\models \mathcal{C}^2_{\mathcal{T}}$. Using Lemma 3.1 it follows that $\theta_{\mathcal{T}^-}$ has the same first order extension for $\mathcal{C}^i$ as $\theta$ for $\mathcal{C}^i_{\mathcal{T}}$, $i \in \{1, 2\}$.This directly implies that $\theta \models \mathcal{C}^1$ and $\theta \not\models \mathcal{C}^2$, which contradicts $\mathcal{C}^1 \subseteq \mathcal{C}^2$. □

Next we give a theorem that follows directly from the above lemma.

**Theorem 3.1.** *Let $\mathcal{T} = \{w_1 \to w_1 - M_1, \cdots, w_{ar(X_m)} \to w_{ar(X_m)} - M_m\}$ be a substitution compatible with $\mathcal{C}^1$ (and $\mathcal{C}^2$). Then $\mathcal{C}^1 \subseteq \mathcal{C}^2$ iff $\mathcal{C}^1_{\mathcal{T}} \subseteq \mathcal{C}^2_{\mathcal{T}}$.*

In the following we define simple constraint systems and, using the above theorem, we will reduce the problem of inclusion between solutions of general constraint systems to the problem of inclusion between solutions of a simple constraint system and a general one.

We say that a constraint system $\mathcal{C}$ is simple iff the terms $t_1, \cdots, t_{ar(X_m)}$ are closed. Moreover, let $\mathcal{T}^{\mathcal{C}}_{var} = \{w_1 \to w_1 - M_1, \cdots, w_{ar(X_m)} \to w_{ar(X_m)} - M_m\}$, where for all $1 \leq i \leq m$, $M_i$ is the inverse of the subterm of $t_i$ that contains all the variables. For example, if we have $t_i = x_{i-1} + x_{i-1} + x_{i-2} + a + (-x_{i-3})$, we have that $M_i = -(X_{i-1} + X_{i-1} + X_{i-2} + (-X_{i-3}))$. It follows that $\mathcal{C}_{\mathcal{T}^{\mathcal{C}}_{var}}$ is the constraint system obtained from $\mathcal{C}$ by removing all variables from $t_1, \cdots, t_{ar(X_m)}$. Notice that $\mathcal{C}_{\mathcal{T}^{\mathcal{C}}_{var}}$ is simple. We now give the following corollary that simplifies the inclusion problem form two constraint systems to the inclusion problem between a simple constraint system and a general one.

**Corollary 3.1.** *$\mathcal{C}^1 \subseteq \mathcal{C}^2$ iff $\mathcal{C}^1_{\mathcal{T}^{\mathcal{C}_1}_{var}} \subseteq \mathcal{C}^2_{\mathcal{T}^{\mathcal{C}_1}_{var}}$.*

Next we illustrate how the above corollary can be applied.

**Example 3.3.** *Let $\mathcal{C}$ and $\mathcal{C}'$ be the constraint systems defined in Example 3.1 and Example 3.2. Next, we have that $\mathcal{T}^{\mathcal{C}}_{var} = \mathcal{T}$, where $\mathcal{T}$ is defined in Example 3.1. Thus, using corollary 3.1, it follows that $\mathcal{C} \subseteq \mathcal{C}'$ iff $\mathcal{C}_{\mathcal{T}} \subseteq \mathcal{C}'_{\mathcal{T}}$,*

*where $\mathcal{C}_\mathcal{T}$ and $\mathcal{C}'_\mathcal{T}$ are defined in Example 3.1 and Example 3.2. Thus, the problem of equivalence between constraint systems is reduced to the problem of equivalence between a simple constraint system and a general constraint system.*

*Since $\mathcal{C}_\mathcal{T}$ and $\mathcal{C}'_\mathcal{T}$ are equivalent, using corollary 3.1, we have that $\mathcal{C}$ and $\mathcal{C}'$ are also equivalent. Intuitively, the fact that $\mathcal{C}_\mathcal{T}$ and $\mathcal{C}'_\mathcal{T}$ are equivalent follows from the fact that their solutions are substitutions that satisfy $X_1\theta + X_2\theta = w_3$.*

### 3.2 Solutions with names in $\mathcal{C}^1$ are sufficient

During this section we show that if all solutions for $\mathcal{C}^1$ that contain only constants that appear in $\mathcal{C}^1$ are also solutions of $\mathcal{C}^2$ then $\mathcal{C}^1 \subseteq \mathcal{C}^2$. Since later we will encode only these solutions into systems of equations, this section proves that this indeed suffices. We start by giving a lemma which will be used later.

**Lemma 3.3.** *Given a constraint system $\mathcal{C}$ and a substitution $\theta$ that contains constants $c_1, \cdots, c_p$ that do not appear in $\mathcal{C}$ such that $\theta \models \mathcal{C}$, then $\theta[t_1/c_1, \cdots t_p/c_p] \models \mathcal{C}$ for any closed, public first order terms $t_1, \cdots, t_p$.*

*Proof.* Let $\sigma$ be the first order extension of $\theta$ and $\sigma'$ be the first order extension of $\theta[t_1/c_1, \cdots t_p/c_p]$. Since $\theta \models \mathcal{C}$ it follows that for any $1 \leq i \leq n$, $s_i\sigma = s'_i\sigma$. Since $c_1, \cdots, c_p$ do not appear in $s_i$ and neither in $s'_i$ it follows that they are reduced in the term $(s_i - s'_i)\sigma$. Thus $(s_i - s'_i)\sigma' = (s_i - s'_i)\sigma[t_1/c_1, \cdots t_p/c_p] = (s_i - s'_i)\sigma$, which concludes. □

We now conclude the section with the final theorem.

**Theorem 3.2.** *Let $\mathcal{C}^1$ and $\mathcal{C}^2$ be two constraint systems. Then $\mathcal{C}^1 \subseteq \mathcal{C}^2$ iff all solutions to $\mathcal{C}^1$ that do not contain constants that do not appear in $\mathcal{C}^1$ are also solutions of $\mathcal{C}^2$.*

*Proof.* Since the implication is trivial, we will focus on the converse. Suppose that all solutions to $\mathcal{C}^1$ that do not contain constants that do not appear in $\mathcal{C}^1$ are also solutions of $\mathcal{C}^2$. Then, we will prove that $\mathcal{C}^1 \subseteq \mathcal{C}^2$. Suppose by contradiction that there exist a substitution $\theta$ which contains $p$ constants $c_1, \cdots, c_p$ that do not appear in $\mathcal{C}^1$ such that $\theta \models \mathcal{C}^1$ and $\theta \not\models \mathcal{C}^2$. Wlog, assume that $c_1, \cdots, c_p$ do not appear in $\mathcal{C}^2$ (otherwise take the substitution $\theta' = \theta[c'_1/c_1, \cdots, c'_p/c_p]$, where $c'_1, \cdots, c'_p$ are fresh constants that do not appear in $\mathcal{C}^1$ and neither in $\mathcal{C}^2$; indeed, according to Lemma 3.3, we have that $\theta' \models \mathcal{C}^1$; the fact that $\theta' \not\models \mathcal{C}^2$ follows by contradiction using Lemma

3.3 and the fact that $\theta'[c_1/c'_1, \cdots, c_p/c'_p] = \theta$). By using $\theta \not\models \mathcal{C}^2$, it follows that there exists an equation $s_i = s'_i \in \mathcal{C}^2$, such that $(s_i - s'_i)\sigma \neq 0$, where $\sigma$ is the first order extension of $\theta$ for $\mathcal{C}^2$. According to Lemma 3.3 it follows that $\theta[0/c_1, \cdots, 0/c_p] \models \mathcal{C}^1$, thus, using the hypothesis, we have that $\theta[0/c_1, \cdots, 0/c_p] \models \mathcal{C}^2$. It follows that $(s_i - s'_i)\sigma$ is a nonzero term that may contain only $c_1, \cdots, c_p$. Let $t_1, \cdots, t_p$ be public terms that contain only constants that appear in $\mathcal{C}^1$ such that $(s_i - s'_i)\sigma[t_1/c_1, \cdots, t_p/c_p] \neq 0$. Then, by Lemma 3.3, it follows that $\theta[t_1/c_1, \cdots, t_p/c_p] \models \mathcal{C}^1$. Using the hypothesis, we have that $\theta[t_1/c_1, \cdots, t_p/c_p] \models \mathcal{C}^2$. Thus, it follows that $(s_i - s'_i)\sigma' = 0$, where $\sigma'$ is the first order extension of $\theta[t_1/c_1, \cdots, t_p/c_p]$ for $\mathcal{C}^2$. However, this is a contradiction, since $(s_i - s'_i)\sigma' = (s_i - s'_i)\sigma[t_1/c_1, \cdots, t_p/c_p]$, which cannot be 0. □

### 3.3 Encoding solutions of constraint systems into systems of equations

The purpose of this section is to show how to construct systems of equations that encode solutions of constraint systems that contain only constants that appear in the constraint system. First, we need to encode second order variables as sums of terms containing unknown variables over $\mathbf{Z}$. Wlog, we assume that the set of public constants that appear in $\mathcal{C}$ are included in the set of terms $t_1, \cdots, t_{ar(X_1)}$. Thus, for all $1 \leq i \leq m$, each second order variable $X_i$ can be seen as a sum $y^i_1 t_1 + \cdots + y^i_{ar(X_i)} t_{ar(X_i)}$, where $y^i_1, \cdots, y^i_{ar(X_i)}$ are unknowns over $\mathbf{Z}$. Therefore every constraint system $\mathcal{C}$ can be brought in the following form:

$$\begin{cases} y^1_1 t_1 + \cdots + y^1_{ar(X_1)} t_{ar(X_1)} = x_1 \\ \cdots \\ y^m_1 t_1 + \cdots + y^m_{ar(X_m)} t_{ar(X_m)} = x_m \\ s_1 = s'_1 \\ \cdots \\ s_n = s'_n, \end{cases}$$

where, for all $1 \leq i \leq m$ and $1 \leq j \leq ar(X_i)$, $y^i_j$ are unknowns over $\mathbf{Z}$, $s_1, s'_1, \cdots, s_n, s'_n$ are first order terms that contain only variables $x_1, \cdots, x_m$ and $t_1, \cdots, t_{ar(X_m)}$ are first order terms that satisfy the origination property. Our next goal is to remove variables $x_1, \cdots, x_m$ from the terms $t_1, \cdots, t_{ar(X_m)}$. By origination property, this can be done using replacements. For each variable $x_i$, we will construct inductively a closed first order term $E(x_i)$ as follows:

$$\begin{cases} E(x_1) & = & y_1^1 t_1 + \cdots + y_{ar(X_1)}^1 t_{ar(X_1)} \\ E(x_i) & = & (y_1^i t_1 + \cdots + y_{ar(X_i)}^i t_{ar(X_i)})[E(x_1)/x_1, \cdots, E(x_p)/x_p], \\ & & \text{where } i > 1 \text{ and } p = ar(X_{i-1}). \end{cases} \tag{1}$$

By origination it follows that, for all $1 \leq i \leq m$, $E(x_i)$ is a closed term. Finally, we will show how a system of equations can be obtained. Given the constraint system $\mathcal{C}$, let $\mathcal{C}_{eq}$ denote the equivalent system of equations that we construct. We have to note that the variables of $\mathcal{C}_{eq}$ are $\{y_j^i \mid 1 \leq i \leq m, 1 \leq j \leq ar(X_i)\}$, thus each solution to $\mathcal{C}_{eq}$ encodes a second order substitution which is a solution of $\mathcal{C}$.

Next, we take each equation $s_i = s_i'$ from $\mathcal{C}$ and add a set of equations into the system $C_{eq}$. We assume that the equation $s_i = s_i'$ has the form $a_1 x_1 + \cdots + a_m x_m = p_i$, where $a_i \in \mathbf{Z}$ and $p_i$ is a closed first order term. Notice that any equation can be brought to this form by bringing factors that contain variables to the left side, and the other factors to the right side. Next, we remove the variables from the left side by replacing them with the closed terms $E(x_i)$, for all $1 \leq i \leq m$. Thus, we now have the equation $a_1 E(x_1) + \cdots + a_m E(x_m) = p_i$. We obtain an equation for each constant, by taking the corresponding coefficients from the left hand side and equalizing with the coefficients from the right hand side. Finally, we add this equation to $\mathcal{C}_{eq}$. We give an example to illustrate the construction.

**Example 3.4.** *Consider the constraint system $\mathcal{C}_{\mathcal{T}}'$ defined in Example 3.2 as*

$$\begin{cases} X_1[a,b] & =^? & x_1 \\ X_2[a,b,c-x_1] & =^? & x_2 \\ x_2 + 2x_1 & =^?_{E_{AG}} & c. \end{cases}$$

*First, we rewrite this constraint system as*

$$\begin{cases} y_1^1 a + y_2^1 b & = & x_1 \\ y_1^2 a + y_2^2 b + y_3^2 (c - x_1) & = & x_2 \\ x_2 + 2x_1 & = & c. \end{cases}$$

*By definition, we have that*

$$\begin{cases} E(x_1) & = & y_1^1 a + y_2^1 b \\ E(x_2) & = & (y_1^2 a + y_2^2 b + y_3^2 (c - x_1))[E(x_1)/x_1] \\ & = & y_1^2 a + y_2^2 b + y_3^2 c - y_3^2 y_1^1 a - y_3^2 y_2^1 b. \end{cases}$$

*Now, we take the equation* $x_2 + 2x_1 =^?_{E_{AG}} c$ *and, by replacing* $x_2$ *with* $E(x_2)$ *and* $x_1$ *with* $E(x_1)$*, we obtain* $a(y_1^2 - y_3^2 y_1^1 + 2y_1^1) + b(y_2^2 - y_3^2 y_2^1 + 2y_2^1) + cy_3^2 = c$*. Thus, we obtain the following system of equations* $\mathcal{C}'_{\mathcal{T}_{eq}}$ *:*

$$\begin{cases} y_1^2 - y_3^2 y_1^1 + 2y_1^1 &= 0 \\ y_2^2 - y_3^2 y_2^1 + 2y_2^1 &= 0 \\ y_3^2 &= 1. \end{cases}$$

*It can be seen that any integer solution of the system of equations encodes a solution of the constraint system. For instance, take* $y_1^1 = 1, y_2^1 = 1, y_1^2 = -1, y_2^2 = -2, y_3^2 = 1$*. This encodes the substitution* $\theta = \{X_1 \to w_1 + w_2, X_2 \to -w_1 - w_2 + w_3\}$*, which is a solution of* $\mathcal{C}'_{\mathcal{T}}$*.*

When the constraint system $\mathcal{C}$ is simple, then $C_{eq}$ becomes a system of linear equations. This happens because, in Equation 1, substitutions are no longer needed. Example 3.5 illustrates this fact.

**Example 3.5.** *Consider the constraint system* $\mathcal{C}_{\mathcal{T}}$ *is defined in example* 3.1 *as*

$$\begin{cases} X_1[a,b] &=^? x_1 \\ X_2[a,b,c] &=^? x_2 \\ x_1 + x_2 &=^?_{E_{AG}} c. \end{cases}$$

*Then, we bring this constraint system into the following form:*

$$\begin{cases} y_1^1 a + y_2^1 b &= x_1 \\ y_1^2 a + y_2^2 b + y_3^2 c &= x_2 \\ x_1 + x_2 &= c. \end{cases}$$

*It follows that*

$$\begin{cases} E(x_1) &= y_1^1 a + y_2^1 b \\ E(x_2) &= y_1^2 a + y_2^2 b + y_3^2 c. \end{cases}$$

*Thus, taking equation* $x_1 + x_2 = c$ *and replacing* $x_1$ *with* $E(x_1)$ *and* $x_2$ *with* $E(x_2)$ *we obtain* $a(y_1^1 + y_1^2) + b(y_2^1 + y_2^2) + cy_3^2 = c$*. Therefore the obtained system of linear equations* $\mathcal{C}_{\mathcal{T}_{eq}}$ *is*

$$\begin{cases} y_1^1 + y_1^2 &= 0 \\ y_2^1 + y_2^2 &= 0 \\ y_3^2 &= 1. \end{cases}$$

### 3.4 Deciding inclusion of solutions of a system of linear equations in solutions of a system of nonlinear equations

Let $\mathcal{C}_{eq}^1$ be a system of linear equations and $\mathcal{C}_{eq}^2$ be a system of nonlinear equations. The first thing to note is that it is sufficient to check whether $\mathcal{C}_{eq}^1$ implies each equation of $\mathcal{C}_{eq}^2$. Also, each equation in $\mathcal{C}_{eq}^2$ can be seen as a polynomial with multiple variables. Thus, we have to decide whether a system of linear equations implies a polynomial which has the same variables. We give a theorem which states that this can be decided in polynomial time. Before giving the main theorem we fix some notations on polynomials.

By $P[y_1, \cdots, y_m]$ we denote a polynomial $P$ with variables $y_1, \cdots, y_m$. By $P[y_1 = s_1, \cdots, y_m = s_m]$, where $s_1, \cdots, s_m$ are terms that contain constants and variables, we denote the polynomial obtained by replacing $y_i$ with $s_i$ in $P$, for all $1 \leq i \leq m$. Having a substitution $\theta = \{y_1 \rightarrow s_1, \cdots, y_m \rightarrow s_m\}$, we denote by $P[\theta]$ the polynomial $P[y_1 = s_1, \cdots, y_m = s_m]$. A root of a polynomial $P[y_1, \cdots, y_m]$ is a sequence of terms $s_1, \cdots, s_m$ such that $P[y_1 = s_1, \cdots, y_m = s_m] = 0$. Having a system of linear equations $\mathcal{C}_{eq}$ and a polynomial $P[y_1, \cdots, y_m]$ with the same variables, we say that $\mathcal{C}_{eq}$ implies $P[y_1, \cdots, y_m]$, denoted $\mathcal{C}_{eq} \rightarrow P[y_1, \cdots, y_m]$, iff each solution of $\mathcal{C}_{eq}$ is also a root of $P[y_1, \cdots, y_m]$.

Next, we give a lemma which will be used later in the proof of the main theorem.

**Lemma 3.4.** *Having a nonzero polynomial $P[y_1, \cdots, y_m]$ where the degree of $y_i$ is $g$ and a set of values $S$ such that $|S| > g$, there exists a value $k \in S$ such that the polynomial $P[y_1, \cdots, y_i = k, \cdots, y_m] \neq 0$.*

*Proof.* Let $s_1, \cdots, s_m \in \mathbf{Z}$ be values that satisfy $P[y_1 = s_1, \cdots, y_m = s_m] \neq 0$. It follows that $P[y_1 = s_1, \cdots, y_i, y_{i+1} = s_{i+1}, \cdots, y_m = s_m] \neq 0$. Suppose by contradiction that for all $k \in S$ we have that $P[y_1, \cdots, y_i = k, \cdots, y_m] = 0$. This directly implies that for all $k \in S$, $P[y_1 = s_1, \cdots, y_i = k, y_{i+1} = s_{i+1}, \cdots, y_m = s_m] = 0$, which is a contradiction since $P[y_1 = s_1, \cdots, y_i, y_{i+1} = s_{i+1}, \cdots, y_m = s_m]$ is a polynomial in $y_i$ that can have at most $g$ roots. □

Finally we give the main theorem.

**Theorem 3.3.** *Having a system of linear equations over $\mathbf{Z}$ $\mathcal{C}_{eq}$ with variables $x_1, \cdots, x_n, y_1, \cdots, y_m$ and a polynomial $E[x_1, \cdots, x_n, y_1, \cdots, y_m]$ it is decidable to say whether $\mathcal{C}_{eq} \rightarrow E[x_1, \cdots, x_n, y_1, \cdots, y_m]$ in polynomial time. Moreover, if a solution to $\mathcal{C}_{eq}$ that is not a root of $E$ exists, it can be found in polynomial time.*

*Proof.* We assume that $\mathcal{C}_{eq}$ is given in the solved form, i.e as a list of $n$ equations of the type $x_i = \frac{t_i}{d_i}$, where $d_i$ is from $\mathbf{Z}$ and, for all $1 \leq i \leq n$, the term $t_i$ is of the form $a_1^i y_1 + \cdots + a_m^i y_m + c_i$, with $a_j^i, c_i \in \mathbf{Z}, 1 \leq j \leq m$. Thus, an integer solution for $\mathcal{C}_{eq}$ is given by a set of integer values for $y_1, \cdots, y_m$ such that $x_1, \cdots, x_n$ are also integers. We consider that solutions to $\mathcal{C}_{eq}$ are substitutions $\theta = \{y_1 \rightarrow s_1, \cdots, y_m \rightarrow s_m\}$ such that $s_1, \cdots, s_m$ are integers and $\frac{t_1\theta}{d_1}, \cdots, \frac{t_n\theta}{d_n}$ are also integers. For the rest of the proof, let $g = lcm(d_1, \cdots, d_n)$. Since, for all $1 \leq i \leq n$, $x_i$ depends only on $y_1, \cdots, y_m$, it suffices to decide whether each solution of $\mathcal{C}_{eq}$ implies the polynomial $P[y_1, \cdots, y_m] = g \cdot E[x_1 = t_i/d_i, \cdots, x_n = t_n/d_n, y_1, \cdots, y_m]$.

Next, we prove that $\mathcal{C}_{eq} \rightarrow P[y_1, \cdots, y_m]$ iff $P[y_1, \cdots, y_m]$ is the 0 polynomial or if $\mathcal{C}_{eq}$ does not admit any integer solution. This suffices, since, as shown in [14], finding an integer solution to $C_{eq}$ can be done in polynomial time. Since the converse is trivial, we will only focus on the implication.

Suppose that $\mathcal{C}_{eq} \rightarrow P[y_1, \cdots, y_m]$. Then, we must prove that either $P[y_1, \cdots, y_m]$ is the constant polynomial 0 or $\mathcal{C}_{eq}$ does not admit any integer solution. It suffices to prove the contrapositive: assuming that $P[y_1, \cdots, y_m]$ is not the constant polynomial 0 and $\mathcal{C}_{eq}$ admits an integer solution, we will prove that $\mathcal{C}_{eq}$ does not imply $P[y_1, \cdots, y_m]$ by showing that there exists a solution for $\mathcal{C}_{eq}$ that is not a root of $P[y_1, \cdots, y_m]$. For each $1 \leq i \leq n$, we have that $x_i = \frac{t_i}{d_i}$, where $t_i = a_1^i y_1 + \cdots + a_m^i y_m + c_i$. Let $0 \leq k_1, \cdots, k_m$ be integers. Let $t_i' = a_1^i(y_1 + gk_1) + \cdots + a_m^i(y_m + gk_m) + c_i$. Since $g$ is divided by $d_i$, it follows that for any integer values for $y_1, \cdots, y_m$, we have that $t_i \equiv_{d_i} t_i'$. Using the hypothesis, it follows that there exists a substitution $\theta = \{y_1 \rightarrow s_1, \cdots, y_m \rightarrow s_m\}$ which is an integer solution to $\mathcal{C}_{eq}$. From the above observation, it follows that the substitution $\theta_{k_1,\cdots,k_m} = \{y_1 \rightarrow s_1 + gk_1, \cdots, y_m \rightarrow s_m + gk_m\}$ is also an integer solution to $\mathcal{C}_{eq}$, for any integers $k_1, \cdots, k_m$. Thus, it suffices to show that there exist $k_1, \cdots, k_m$ such that $P[\theta_{k_1,\cdots,k_m}] \neq 0$. For the rest of the proof let $\theta_{k_1,\cdots,k_t} = \{y_1 \rightarrow s_1 + gk_1, \cdots, y_t \rightarrow s_t + gk_t, y_{t+1} \rightarrow s_{t+1}, \cdots, y_m \rightarrow s_m\}$, for any integers $k_1, \cdots, k_t$ with $t \leq m$.

We conclude by proving the following statement by induction on $m$: given a non zero polynomial $P[y_1, \cdots, y_m]$, there exist $k_1, \cdots, k_m$ such that $P[\theta_{k_1,\cdots,k_m}] \neq 0$. The base case is trivial: for $m = 1$, we have that our polynomial has only one variable which is $y_1$. Let $p$ be the degree of the polynomial. It follows that $P$ may have at most $p$ roots, thus at least one value from the set $\{s_1 + 0 \cdot g, s_1 + 1 \cdot g, \cdots, s_1 + p \cdot g\}$ will not be a root of the polynomial. Thus there exist a $k_1$ from the set $\{0, 1, \cdots, p\}$ such that $P[\theta_{k_1}] \neq 0$. Suppose now that for all $i < t$, there exist $k_1, \cdots, k_i$ such

that $P[\theta_{k_1,\cdots,k_i}] \neq 0$, for any polynomial $P[y_1,\cdots,y_i]$. We will prove that the statement is also true for $t$. Let $p$ be the degree of $y_t$. Using Lemma 3.4, it follows that there exists $k_t \in \{0,1,\cdots,p\}$ such that the polynomial $P[y_1,\cdots,y_{t-1},y_t = s_t + k_t g]$ is not the null polynomial. By applying the induction hypothesis on $P[y_1,\cdots,y_{t-1},y_t = s_t + k_t g]$, it follows that there exists $k_1,\cdots,k_{t-1}$ such that $P[\theta_{k_1,\cdots,k_{t-1},k_t}] \neq 0$, which concludes. The polynomial algorithm that finds $k_1,\cdots,k_m$ follows directly from this proof. □

**Example 3.6.** *Consider the system of linear equations $\mathcal{C}_{\mathcal{T}_{eq}}$ defined in Example 3.5 as*

$$\begin{cases} y_1^1 + y_1^2 &= 0 \\ y_2^1 + y_2^2 &= 0 \\ y_3^2 &= 1. \end{cases}$$

*which can be rewritten into solved form as*

$$\begin{cases} y_1^1 &= -y_1^2 \\ y_2^1 &= -y_2^2 \\ y_3^2 &= 1. \end{cases}$$

*Consider also the system of equations $\mathcal{C}'_{\mathcal{T}_{eq}}$ defined in Example 3.4 as*

$$\begin{cases} y_1^2 - y_3^2 y_1^1 + 2y_1^1 &= 0 \\ y_2^2 - y_3^2 y_2^1 + 2y_2^1 &= 0 \\ y_3^2 &= 1. \end{cases}$$

*It can be seen that $\mathcal{C}_{\mathcal{T}_{eq}}$ implies the first two equation of $\mathcal{C}'_{\mathcal{T}_{eq}}$ because all the terms reduce when replacing $y_1^1$ with $-y_1^2$, $y_2^1$ with $-y_2^2$ and $y_3^2$ with 1, as indicated in the solved form of $\mathcal{C}_{\mathcal{T}_{eq}}$. Thus, we can finally conclude that $\mathcal{C} \subseteq \mathcal{C}'$, where $\mathcal{C}$ and $\mathcal{C}'$ are defined in Examples 3.1 and 3.2.*

## 3.5 Deciding $\mathcal{C}^1 \subseteq \mathcal{C}^2$ : putting the pieces together

Given two constraint systems $\mathcal{C}^1$ and $\mathcal{C}^2$, we use the constructions described earlier for deciding whether $\mathcal{C}^1 \subseteq \mathcal{C}^2$. As shown in Section 3.1, we can assume that $\mathcal{C}^1$ is simple. Wlog, we assume that all public constants that appear in both $\mathcal{C}^1, \mathcal{C}^2$ are included in the set of terms $t_1,\cdots,t_{ar(X_1)}$ and $t'_1,\cdots,t'_{ar(X_1)}$. Since $\mathcal{C}^1$ is simple, by Theorem 3.2 from Section 3.2 and the

encoding presented in Section 3.3 it suffices to check whether the set of solutions of the system of linear equations $\mathcal{C}^1_{eq}$ is included in the set of solutions of the system of nonlinear equations $\mathcal{C}^2_{eq}$, which is solved in Section 3.4.

# 4 Conclusion

We have showed how to decide whether two constraint systems are equivalent when using the Abelian Groups equational theory by presenting a procedure that can be easily adapted for Exclusive Or equational theory as well. Since combination algorithms for disjoint equational theories have been already developed for satisfiability of constraint systems [12] and static equivalence [13], we are confident in the possibility of developing a combination procedure for equivalence of constraint systems as well. In the event of such a result, our procedure could be combined with other existing procedures resulting in new algorithms for deciding equivalence of constraint systems in the presence of theories that contain signatures, pairing, symmetric and asymmetric encryptions, abelian groups and exclusive or, which would enable analysis of equivalence based properties in more detail and of even more real world protocols.

# References


[1] D. Dolev and A. C.-C. Yao, "On the security of public key protocols (extended abstract)," in *FOCS*, pp. 350–357, 1981.

[2] J. K. Millen and V. Shmatikov, "Constraint solving for bounded-process cryptographic protocol analysis," in *ACM Conference on Computer and Communications Security*, pp. 166–175, 2001.

[3] S. Delaune and F. Jacquemard, "A theory of dictionary attacks and its complexity," in *CSFW*, pp. 2–15, 2004.

[4] L. Gong, T. M. A. Lomas, R. M. Needham, and J. H. Saltzer, "Protecting poorly chosen secrets from guessing attacks," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 648–656, 1993.

[5] V. Cheval, H. Comon-Lundh, and S. Delaune, "Automating security analysis: Symbolic equivalence of constraint systems," in *IJCAR*, pp. 412–426, 2010.

[6] M. Baudet, "Deciding security of protocols against off-line guessing attacks," in *ACM Conference on Computer and Communications Security*, pp. 16–25, 2005.

[7] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *MOBICOM*, pp. 180–189, 2001.

[8] S. Even and O. Goldreich, "On the security of multi-party ping-pong protocols," in *FOCS*, pp. 34–39, 1983.

[9] H. Comon and V. Cortier, "Tree automata with one memory set constraints and cryptographic protocols," *Theor. Comput. Sci.*, vol. 331, no. 1, pp. 143–214, 2005.

[10] N. A. Durgin, P. Lincoln, and J. C. Mitchell, "Multiset rewriting and the complexity of bounded security protocols," *Journal of Computer Security*, vol. 12, no. 2, pp. 247–311, 2004.

[11] V. Cortier and S. Delaune, "A method for proving observational equivalence," in *Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF'09)*, (Port Jefferson, NY, USA), pp. 266–276, IEEE Computer Society Press, July 2009.

[12] Y. Chevalier and M. Rusinowitch, "Symbolic protocol analysis in the union of disjoint intruder theories: Combining decision procedures," *Theor. Comput. Sci.*, vol. 411, no. 10, pp. 1261–1282, 2010.

[13] V. Cortier and S. Delaune, "Decidability and combination results for two notions of knowledge in security protocols," *Journal of Automated Reasoning*, 2011. To appear.

[14] M. Goldmann and A. Russell, "The complexity of solving equations over finite groups," *Inf. Comput.*, vol. 178, no. 1, pp. 253–262, 2002.

[15] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Commun. ACM*, vol. 21, no. 12, pp. 993–999, 1978.

[16] M. Rusinowitch and M. Turuani, "Protocol insecurity with finite number of sessions is np-complete," in *CSFW*, pp. 174–, 2001.