$$
\begin{array}{lrcll}
R_1 & C \wedge T \overset{?}{\vdash} u & \rightsquigarrow & C & \text{if } T \cup \{x \mid (T' \overset{?}{\vdash} x) \in C, T' \subsetneq T\} \vdash u \\
R_2 & C \wedge T \overset{?}{\vdash} u & \rightsquigarrow & C\sigma \wedge T\sigma \overset{?}{\vdash} u\sigma \wedge t = u & \text{if } t \in \mathsf{St}(T), \sigma = \mathsf{mgu}(t,u) \\
 & & & & \quad t \neq u,\ t,u \text{ not variables} \\
R_3 & C \wedge T \overset{?}{\vdash} u & \rightsquigarrow & C\sigma \wedge T\sigma \overset{?}{\vdash} u\sigma \wedge t_1 = t_2 & \text{if } t_1, t_2 \in \mathsf{St}(T), \sigma = \mathsf{mgu}(t_1,t_2) \\
 & & & & \qquad t_1 \neq t_2,\ t_1,t_2 \text{ not variables} \\
R'_3 & C \wedge T \overset{?}{\vdash} u & \rightsquigarrow & C\sigma \wedge T\sigma \overset{?}{\vdash} u\sigma \wedge t_2 = \mathsf{pk}(t_3) & \text{if } \{t_1\}^p_{t_2}, \mathsf{sk}(t_3) \in \mathsf{St}(T), \\
 & & & & \qquad \sigma = \mathsf{mgu}(t_2, \mathsf{pk}(t_3)), t_2 \neq \mathsf{pk}(t_3), \\
 & & & & \qquad t_2 \text{ or } t_3 \text{ (or both) is a variable} \\
R_4 & C \wedge T \overset{?}{\vdash} u & \rightsquigarrow & \bot & \text{if } \mathcal{V}(T,u) = \emptyset \text{ and } T \not\vdash u \\
R_f & C \wedge T \overset{?}{\vdash} f(u,v) & \rightsquigarrow & C \wedge T \overset{?}{\vdash} u \wedge T \overset{?}{\vdash} v & \text{for } f \neq \mathsf{sk}(\_)
\end{array}
$$

Figure 2: Simplification rules.

3.2 Constraint Simplification

We describe here a non-deterministic simplification procedure. It can be simplified in many respects, but we will see that the problem of deciding whether a constraint system has at least one solution is NP-complete anyway.

Many parts of this section, including the set of rules, is borrowed from [**?**].

$\sigma = \mathsf{mgu}(t,u)$ is a most general unifier of t,u, such that $\mathcal{V}(t\sigma, u\sigma) \subseteq \mathcal{V}(t,u)$. We also use two properties of the unification algorithm, that we assume here: if $t \neq u$ and $\sigma = \mathsf{mgu}(t,u)$ then

1. $\mathcal{V}(t\sigma, u\sigma)$ is strictly included in $\mathcal{V}(t,u)$.

2. $\mathsf{St}(t\sigma) \cup \mathsf{St}(u\sigma) = \mathsf{St}(t)\sigma \cup \mathsf{St}(u)\sigma$.

The second property implies in particular (for a suitable representation of terms) that $|t\sigma, u\sigma| \leq |t,u|$: the number of distinct subterms of $t\sigma, u\sigma$ is smaller than the number of distinct subterms in t,u.

Example 11 *$t = f(x, g(x)), u = f(f(y,z), g(f(g(x'), g(y'))))$.*
$\sigma = mgu(t,u) = \{x \mapsto f(g(x'), g(y'));\ y \mapsto g(x');\ z \mapsto g(y')\}$.

$$
\begin{array}{rll}
St(t,u) & = \{ & x, y, z, x', y', g(x), f(y,z), g(x'), g(y'), f(x,g(x)), f(g(x'), g(y')), \\
 & & g(f(g(x'), g(y'))), f(f(y,z), g(f(g(x'), g(y'))))\}
\end{array}
$$

there are 13 elements.

$$
\begin{array}{rll}
St(t\sigma, u\sigma) & = \{ & x', y', g(x'), g(y'), f(g(x'), g(y')), g(f(g(x'), g(y'))), \\
 & & f(f(g(x'), g(y')), g(f(g(x'), g(y'))))\}
\end{array}
$$

there are 7 elements.

Lemma 3.3 *The rules of figure 2 are correct: any deducibility constraint system C is transformed in a deducibility constraint system C' such that any solution σ of C' is also a solution of C.*

Proof: Let C be a deduction constraint, $C = \bigwedge_i (T_i \overset{?}{\vdash} u_i)$ and $C \rightsquigarrow C'$. Since $T_i \subseteq T_{i+1}$ implies $T_i\sigma \subseteq T_{i+1}\sigma$, C' satisfies the first point of the definition of deduction constraints.

We show that C' also satisfies the second point of the definition of deduction constraints.

Let $(T' \overset{?}{\vdash} u') \in C'$ and $x \in \mathcal{V}(T')$. We have to prove that T'_x exists and $T'_x \subsetneq T'$. We distinguish cases, depending on which simplification rule is applied:

- If the rule R_1 is applied, eliminating the constraint $T \overset{?}{\vdash} u$. Then $C' = C \setminus \{T \overset{?}{\vdash} u\}$. If $T_x \neq T$ then $T'_x = T_x$ (and thus T'_x exists and $T'_x \subsetneq T'$). Suppose that $T_x = T$. Then there is $(T \overset{?}{\vdash} u'') \in C$ such that $x \in \mathcal{V}(u'')$. If $u \neq u''$ then again $T'_x = T_x$ (since $(T'_x \overset{?}{\vdash} u'') \in C'$). Finally, suppose that $u = u''$. By the minimality of T, it follows that $x \notin \mathcal{V}(T)$ and $x \notin \{y \mid (T'' \overset{?}{\vdash} y) \in C, T'' \subsetneq T\}$. Since $x \in \mathcal{V}(u)$, we use the following lemma:

  Lemma 3.4 *If $T \vdash u$ then $\mathcal{V}(u) \subseteq \mathcal{V}(T)$.*

  whose proof is left to the reader. We conclude $T \cup \{y \mid (T'' \overset{?}{\vdash} y) \in C, T'' \subsetneq T\} \not\vdash u$, which contradicts the applicability of rule R_1.

- If one of the rules R_2, R_3 or R'_3 is applied, then, for each constraint $(T'' \overset{?}{\vdash} u'') \in C'$, there is a constraint $(T \overset{?}{\vdash} u) \in C$ such that $T\sigma = T''$ and $u\sigma = u''$. Consider $(T \overset{?}{\vdash} u) \in C$ such that $T\sigma = T'$ and $u\sigma = u'$.

  If x is not introduced by σ, then $x \in \mathcal{V}(T)$. Then T_x exists and $T_x \subsetneq T$. Thus $T_x\sigma \subseteq T\sigma$. If $T_x\sigma = T\sigma$, then $x \in \mathcal{V}(T_x)$, which contradicts the minimality of T_x. Thus $T_x\sigma \subsetneq T\sigma$. We also have that $\{T''\sigma \mid (T'' \Vdash u'') \in C, x \in \mathcal{V}(u'')\} \subseteq \{T''\sigma \mid (T''\sigma \Vdash u''\sigma) \in C', x \in \mathcal{V}(u''\sigma)\}$, since, for any term u'', if $x \in \mathcal{V}(u'')$, then $x \in \mathcal{V}(u''\sigma)$. It follows that T'_x exists and $T'_x \subseteq T_x\sigma$. Hence $T'_x \subsetneq T'$.

  Otherwise, assume that x is introduced by σ: $\exists y \in \mathcal{V}(T)$ such that $x \in \mathcal{V}(y\sigma)$. Then T_y exists and $T_y \subsetneq T$. Let $Y = \{z \in \mathcal{V}(T) \mid x \in \mathcal{V}(z\sigma)\}$ and let $y_0 \in Y$ be such that $T_{y_0} = \min\{T_y \mid y \in Y\}$. For all $y' \in Y$, we have that

$$\begin{aligned}
A \quad & \overset{\text{def}}{=} \{T''\sigma \mid (T'' \Vdash u'') \in C', x \in \mathcal{V}(u'')\} \\
& = \{T\sigma \mid (T \Vdash u) \in C, x \in \mathcal{V}(u\sigma)\} \\
& \supseteq \{T\sigma \mid (T \Vdash u) \in C, \exists z \in \mathcal{V}(u), x \in \mathcal{V}(z\sigma)\} \\
& \supseteq \{T\sigma \mid (T \Vdash u) \in C, y' \in \mathcal{V}(u), x \in \mathcal{V}(y'\sigma)\} \\
& = \{T\sigma \mid (T \Vdash u) \in C, y' \in \mathcal{V}(u)\} \overset{\text{def}}{=} B_{y'}.
\end{aligned}$$

  Thus $T'_x = \min A \subseteq \min B_{y'} = T_{y'}\sigma$. From $T_{y_0} \subsetneq T$, we obtain that $T_{y_0}\sigma \subseteq T\sigma$. Suppose, by contradiction, that $T_{y_0}\sigma = T\sigma$. Then $x \in \mathcal{V}(T_{y_0}\sigma)$ (since $x \in \mathcal{V}(T\sigma)$).

That is, there exists $z \in \mathcal{V}(T_{y_0})$ such that $x \in \mathcal{V}(z\sigma)$. From the second condition of Definition 3.1 applied to z, it follows that $T_z \subsetneq T_{y_0}$. As z is in Y, this contradicts the choice of y_0. Thus $T'_x \subseteq T_{y_0}\sigma \subsetneq T\sigma = T'$.

- If the rule R_4 is applied then there is nothing to prove.
- If some rule R_f is applied, then the property is preserved, since, if $x \in \mathcal{V}(u'')$ for some term u'' such that $(T'' \Vdash u'') \in C'$, then there is a term v with $x \in \mathcal{V}(v)$ such that $(T'' \Vdash v) \in C$.

□

Lemma 3.5 *There is no infinite simplification sequence using the rules of figure 2.*

Proof: The number of variables occurring in the non-equational part of the constraint is non-increasing. Furthermore, it is strictly decreasing by the rules R_2, R_3, R'_3. Any other rule strictly reduces the total size of the right hand sides of the constraint (here, the "size" is the number of symbols in the term). □

3.3 Solved forms

Definition 3.6 *A deducibility constraint system is in* solved form *if it is either $\bot, \top$ or a conjunction*

$$x_1 = s_1 \wedge \ldots \wedge x_n = s_n \wedge T_1 \overset{?}{\vdash} y_1 \wedge \ldots \wedge T_m \overset{?}{\vdash} y_m$$

where $x_1, \ldots, x_n, y_1, \ldots, y_m$ are variables and every x_i does not occur in $s_i, x_{i+1}, s_{i+1}, \ldots, s_n$, $T_1, y_1, \ldots, T_m, y_m$.

It is straighforward to see that a solved deducibility constraint that is not $\bot$ has at least a solution. Furthermore, if it is not reduced to its equational part, then it has infinitely many solutions.

3.4 Completeness

First, we show that proofs, that are considered in solutions of constraints, can be narrowed to the so-called *simple proofs*.

Definition 3.7 *Given a sequence of hypotheses $T_1 \subsetneq T_2 \cdots \subsetneq T_n$ and a term t such that $T_n \vdash t$, a* simple proof of t *is a proof Π of $T_i \vdash t$, such that*

1. *Π is a local proof (see definition 2.2)*
2. *i is the minimal index j such that there is a proof of $T_j \vdash t$*
3. *all stict subproofs are simple.*

First, we must refine the lemma 2.3 showing that there are always simple proofs:

Lemma 3.8 *For any sequence $T_1 \subsetneq T_2 \cdots \subsetneq T_n$ and any term t such that $T_n \vdash t$, there exists a simple proof of t.*

Proof: Let i be a minimal index for which there is a proof of $T_i \vdash t$. Thanks to the lemma 2.3, there is a local proof π_0 of $T_i \vdash t$.

We prove the lemma by induction on the size of π_0. If $t \in T_i \backslash T_{i-1}$, then the proof reduced to the leaf node is a simple proof.

Otherwise, consider the last rule in the proof of t:

$$\pi_0 = \frac{\begin{matrix}\pi_1 \\ t_1\end{matrix} \quad \cdots \quad \begin{matrix}\pi_n \\ t_n\end{matrix}}{t}$$

For every $j = 1, ..., n$, π_j is a proof of $T_i \vdash t_i$. By induction hypothesis, there are simple proofs π'_j of $T_{i_j} \vdash t_j$ with $i_j \leq i$. If t appears as a node in some of these proofs, we simply replace π_0 with the corresponding subproof and get the desired result. Otherwise we let

$$\Pi = \frac{\begin{matrix}\pi'_1 \\ t_1\end{matrix} \quad \cdots \quad \begin{matrix}\pi'_n \\ t_n\end{matrix}}{t}$$

Π is a simple proof of t. Indeed, all properties are satisfied, except possibly the first one. But, as shown in the proof of lemma 2.3, $t_j \notin \mathsf{St}(T_i) \cup \mathsf{St}(t)$ can only occur when the last rule of Π is a decomposition and the last rule of π'_j is a composition, which would yield a loop. □

Lemma 3.9 *Let σ be a solution of $C = T_0 \overset{?}{\vdash} x_0, \ldots, t_{i-1} \overset{?}{\vdash} x_{i-1}, T_i \overset{?}{\vdash} s, \ldots,$ with $T_0 \subseteq \cdots \subseteq T_i \subseteq \cdots$ If there is a simple proof of $T_i\sigma \vdash u$ whose last inference rule is a decomposition, then there is a non-variable $t \in \mathsf{St}(()T_i)$ such that $t\sigma = u$.*

Proof:

Consider a simple proof π of $T_i\sigma \vdash u$. We may assume, without loss of generality, that i is minimal. Otherwise, we simply replace everywhere T_i with a minimal T_j such that $T_j\theta \vdash u$. Such a $T_j \subseteq T_i$ also satisfies the hypotheses of the lemma.

We reason by induction on the depth of the proof π. We make a case distinction, depending on the last rule of π:

The last rule is an axiom Then $u \in T_i\sigma$ and there is $t \in T_i$ (thus $t \in \mathsf{St}(T_i)$) such that $t\sigma = u$. By contradiction, if t was a variable then $T_t \overset{?}{\vdash} w$, with $t \in \mathcal{V}(w)$ is a constraint in C such that $T_t \subsetneq T_i$. By hypothesis of the lemma, w must be a variable. Hence $w = t$. Then $T_t\theta \vdash u$, which contradicts the minimality of i.

The last rule is a symmetric decryption

$$\pi = \frac{\begin{matrix}\pi_1 \\ \{u\}^s_w\end{matrix} \quad \begin{matrix}\pi_2 \\ T_i w\end{matrix}}{u}$$

By simplicity, the last rule of π_1 cannot be a composition: u would appear twice on the same path. Then, by induction hypothesis, there is a non variable $t \in \mathsf{St}(T_i)$ such that $t\sigma = \{u\}^s_w$. It follows that $t = \{t'\}^s_{t''}$ with $t'\sigma = u$. If t' was a variable, then $T_{t'}\sigma \vdash t'\sigma$. Hence $T_{t'}\sigma \vdash u$ would be derivable, which again contradicts the minimality of i. Hence t' is not variable, as required.

The last rule is an asymmetric decryption, (resp. projection, resp. unsigning) The proof is similar to the above one: by simplicity and by induction hypothesis, there is a non-variable $t \in \mathsf{St}(T_i)$ such that $t\sigma = \{u\}^p_{\mathsf{pk}(v)}$ (resp. $t\sigma = \langle u, v\rangle$, resp. $t\sigma = \mathsf{sign}(u, v)$). Then $t = \{t\}^p_{t''}$ (resp. $t = \langle t', t''\rangle$, resp. $t = \mathsf{sign}(t, t'')$). $t' \in \mathsf{St}(T_i)$, $t'\sigma = u$ and, by minimality of i, t' is not a variable.

□

Lemma 3.10 *Let C be $T_0 \overset{?}{\vdash} x_0, \dots, T_{i-1} \overset{?}{\vdash} x_{i-1}, T_i \overset{?}{\vdash} u, \dots$ be a constraint system and σ be a solution of C such that*

1. *T_i does not contain two distinct non-variable subterms t_1, t_2 with $t_1\theta = t_2\theta$;*
2. *T_i does not contain two subterms $\{t_1\}^p_{t_2}$ and $\mathsf{sk}(t_3)$ where $t_2 \neq \mathsf{pk}(t_3)$ and $t_2\sigma = \mathsf{pk}(t_3\sigma)$.*
3. *u is a non-variable subterm of T_i;*

Then $T'_i \vdash u$, where $T'_i = T_i \cup \{x \mid (T \overset{?}{\vdash} x) \in C, T \subsetneq T_i\}$.

Proof: Let j be minimal such that $T_j\theta \vdash u\theta$. Thus $j \leq i$ and $T_j \subseteq T_i$. Consider a simple proof π of $T_j\theta \vdash u\theta$. We reason by induction on the depth of π. We analyze the different cases, depending on the last rule of π:

The last rule is an axiom Suppose, by contradiction, that $u \notin T_j$. Then there is $t \in T_j$ such that $t\sigma = u\sigma$ and $t \neq u$. By hypothesis 3, u is not a variable and, by hypothesis 1 of the lemma, t, u cannot be both non-variable subterms of T_i. It follows that t is a variable. Then $T_t\sigma \vdash t\sigma$, which implies $T_t\sigma \vdash u\sigma$, contradicting the minimality of j, since $T_t \subsetneq T_j$. Hence $u \in T_j$ and then $T'_i \vdash u$, as required.

The last rule is the symmetric decryption rule There is w such that $T_j\sigma \vdash \{u\sigma\}^s_w$, $T_j\sigma \vdash w$:

$$\frac{\overset{\pi_1}{\{u\sigma\}^s_w} \qquad \overset{\pi_2}{w}}{u\sigma}$$

By simplicity, the last rule of the proof π_1 is a decomposition. By Lemma 3.9, there is $t \in \mathsf{St}(T_j)$, t not a variable, such that $t\sigma = \{u\sigma\}^s_w$. Let $t = \{t_1\}^s_{t_2}$ and $t_1\sigma = u\sigma$, $t_2\sigma = w$. By induction hypothesis, $T'_i \vdash t$.

If t_1 was a variable, then $T_{t_1} \subsetneq T_j$ and, by hypothesis of the lemma, $T_{t_1}\sigma \vdash u\sigma$, contradicting the minimality of j.

Now, by hypothesis 3 of the lemma, u is a non-variable subterm of T_i, hence t_1, u are two non variable subterms of T_i such that $t_1\sigma = u\sigma$. By hypothesis 1 of the lemma, this implies $t_1 = u$.

On the other hand, if t_2 is a variable, $t_2 \in \mathcal{V}(T_i)$ implies $T_{t_2} \subsetneq T_i$ and, by minimality of T_i $t_2 \in T'_i$. If t_2 is not a variable, then, from $T_j\sigma \vdash t_2\sigma$ and by induction hypothesis, $T'_i \vdash t_2$. So, in any case, $T'_i \vdash t_2$.

Now, both $T'_i \vdash \{()\}_u, t_2)$ and $T'_i \vdash t_2$, from which we conclude that $T'_i \vdash u$, by symmetric decryption.

The last rule is an asymmetric decryption rule There is a w such that $T_j\sigma \vdash \mathsf{sk}(w)$ and $T_j\sigma \vdash \{u\sigma\}^p_{\mathsf{pk}(w)}$. As in the previous case, there is a non-variable $t \in \mathsf{St}(T_j)$ such that $t\sigma = \{u\sigma\}^p_{\mathsf{pk}(w)}$. By induction hypothesis, $T'_i \vdash t$. Let $t = \{t_1\}^p_{t_2}$.

As in the previous case, t_1 cannot be a variable. Therefore t_1, u are two non-variable subterms of T_i such that $t_1\sigma = u\sigma$, which implies that $t_1 = u$. (We use here the hypotheses 1 and 3).

On the other hand, the last rule in the proof of $T_j\sigma \vdash \mathsf{sk}(w)$ is a decomposition (no composition rule can yield a term headed with $\mathsf{sk}(\_)$). Then, by Lemma 3.9 (T_j satisfies the hypotheses of the lemma since $T_j \subseteq T_i$), there is a non-variable subterm $w_1 \in \mathsf{St}(T_j)$ such that $w_1\sigma = \mathsf{sk}(w)$. Let $w_1 = \mathsf{sk}(w_2)$. By induction hypothesis, $T'_j \vdash \mathsf{sk}(w_2)$.

$$\frac{\begin{array}{c}\{t_1\}^p_{t_2}\sigma\\ \|\\ \{u\sigma\}^p_{\mathsf{pk}(w)}\end{array}\qquad\begin{array}{c}\mathsf{sk}(w_2)\sigma\\ \|\\ \mathsf{sk}(w)\end{array}}{u\sigma}$$

By hypothesis 2 of the lemma, we must have $t_2 = \mathsf{pk}(w_2)$. Finally, from $T'_i \vdash \{u\}^p_{\mathsf{pk}(w_2)}, T'_i \vdash \mathsf{sk}(w_2)$ we conclude $T'_i \vdash u$.

The last rule is a projection rule

$$\frac{\begin{array}{c}\pi_1\\ \langle u\sigma, v\rangle\end{array}}{u\sigma}$$

As before, by simplicity, the last rule of π_1 must be a decomposition and, by Lemma 3.9, there is a non variable term $t \in \mathsf{St}(T_j)$ such that $t\sigma = \langle u\sigma, v\rangle$. We let $t = \langle t_1, t_2\rangle$. By induction hypothesis, $T'_i \vdash t$.

Now, as in the previous cases, t_1 cannot be a variable, by minimality of T_j. Next, by hypotheses 1 and 3, we must have $t_1 = u$. Finally, from $T'_i \vdash \langle u, t_2\rangle$ we conclude $T'_i \vdash u$ by projection.

The last rule is an unsigning rule

$$\frac{\begin{array}{c}\pi_1\\ \mathsf{sign}(u\sigma, v)\end{array}}{u\sigma}$$

This case is identical to the previous one.

The last rule is a composition Assume for example that it is the symmetric encryption rule.

$$\frac{\begin{array}{c}\pi_1\\ v_1\end{array}\quad\begin{array}{c}\pi_1\\ v_2\end{array}}{\{v_1\}^s_{v_2}}$$

with $u\sigma = \{v_1\}^s_{v_2}$. Since u is not a variable, $u = \{u_1\}^s_{u_2}$, $u_1\sigma = v_1$, and $u_2\sigma = v_2$. If u_1 (resp. u_2) is a variable then u_1 (resp. u_2) belongs to $\mathcal{V}(T_i)$ since $u \in \mathsf{St}(T_i)$. Again, this implies $u_1 \in T'_i$ (resp. $u_2 \in T'_i$).

Otherwise, u_1 and u_2 are non-variables. Then, by induction hypothesis, $T_i' \vdash u_1$ and $T_i' \vdash u_2$. Hence in both cases we have $T_i' \vdash u_1$ and $T_i' \vdash u_2$. Thus $T_i' \vdash u$.

The proof is similar for other composition rules.

□

Theorem 3.11 (Completeness) *If σ is a solution of C and C is not in solved form, then there is a C' such that $C \rightsquigarrow C'$ and σ is a solution of C'.*

Proof: We assume here that the equations are eagerly simplified into solved equations systems, which may be not mentioned below, for simplicity.

If C is not in solved form, then there is an index i such that

$$C = T_1 \overset{?}{\vdash} x_1, \dots T_{i-1} \overset{?}{\vdash} x_{i-1}, T_i \overset{?}{\vdash} u_i, \dots, T_n \overset{?}{\vdash} u_n$$

where $T_1 \subseteq \dots \subseteq T_n$, $x_1, \dots, x_{i-1}$ are variables and u_i is not a variable.

Since σ is a solution, there is a simple proof π of $T_i\sigma \vdash u_i\sigma$. We distinguish cases, depending on the last rule of π.

The last rule is a composition Since u is not a variable, $u = f(u_1, \dots, u_n)$ and $T_i\sigma \vdash u_j\sigma$ for every $j = 1, ..., n$. Then we may apply the transformation rule R_f to C, yielding constraints $T_i \Vdash u_j$ in C' for every j. σ is a solution of C'.

The last rule is not a composition By Lemma 3.9, there is a non-variable term $t \in \mathsf{St}(T_i)$ such that $t\sigma = u_i\sigma$. We distinguish then again between cases, depending on t, u_i:

Case $t \neq u_i$ Then, since t, u_i are both non-variable terms, we may apply the simplification rule R_2 to C: $C \rightsquigarrow_{R_2} C' \wedge t = u_i$ where $C' = C\theta$ and $\theta = \mathsf{mgu}(t, u_i)$. Furthermore, $t\sigma = u_i\sigma$, hence (by definition of a mgu) there is a substitution τ such that $\sigma = \theta\tau$. Finally, σ is a solution of C, hence τ is a solution of C' and σ is a solution of $C' \wedge t = u_i$.

Case $t = u_i$ Then $u_i \in \mathsf{St}(T_i)$.

1. If there are two distinct non-variable terms $t_1, t_2 \in \mathsf{St}(T_i)$ such that $t_1\sigma = t_2\sigma$. Then we apply the simplification rule R_3, yielding $C' = C\theta \wedge t_1 = t_2$. As in the previous case, there is a substitution τ such that $\sigma = \theta\tau$ and τ is a solution of C', σ is a solution of $C' \wedge t_1 = t_2$.
2. If there are $\{t_1\}^p_{t_2}, \mathsf{sk}(()t_3) \in \mathsf{St}(T_i)$ such that either t_2 or t_3 is a variable, $t_2 \neq \mathsf{pk}(t_3)$ and $t_2\sigma = \mathsf{pk}(t_3)\sigma$, then we may apply the rule R_3' and conclude as in the previous case.
3. Otherwise, we match all hypotheses of Lemma 3.10 and we conclude that $T_i' \vdash u_i$. Then the rule R_1 can be applied to C, yielding a deduction constraint, of which σ is again a solution.

□

Exercise 7
Consider the following protocol (defined informally):

$$\begin{array}{ll} A \to B : & \nu k_1, k_2 : \left\langle \{k_1\}^p_{\mathsf{pk}(b)}, \{k_2\}^p_{\mathsf{pk}(b)} \right\rangle \\ B \to A : & \qquad \{k_1\}^s_{k_2} \end{array}$$

1. write formally the processes corresponding to an instance of the role A by two honest agents a, b and an instance of the role b with the same two honest agents
2. Give a deduction constraint system corresponding to the only relevant symbolic trace for the processes of the previous question.
3. Apply the simplification rules to this constraint system and derive all possible attacks on the secrecy of k_1 (resp. k_2) for this scenario.

Exercise 8
Give an example showing that R_3 is necessary for the completeness.

Exercise 9
Give an example showing that R_3' is necessary for the completeness.