

Lemma 3. Let \mathcal{C} be an unsolved constraint system, θ be a solution of \mathcal{C} and $T_i \Vdash u_i$ be a minimal unsolved constraint of \mathcal{C} . Let u be a term. If there is a simple proof of $T_i\theta \vdash u$ having the last rule an axiom or a decomposition then there is $t \in st(T_i) \setminus \mathcal{X}$ such that $t\theta = u$.

Proof. Consider a simple proof π of $T_i\theta \vdash u$. We can suppose without loss of generality that i is minimal since if $T_j\theta \vdash u$ with $j < i$ then π' (obtained as in the definition of a simple proof) is a simple proof having as the last rule an axiom or a decomposition.

- The last rule is an axiom. Then $u \in T_i\theta$ and hence there is $t \in T_i$ (thus $t \in st(T_i)$) such that $t\theta = u$. If t is a variable then $T_t \Vdash t$ is a constraint in \mathcal{C} with $T_t \subsetneq T_i$ (see the definition of a constraint system). Hence $T_t\theta \vdash t\theta$, that is $T_t\theta \vdash u$, which contradicts the minimality of i . Thus, as required, t is not a variable.
- The last rule is a decomposition. Suppose that it is a symmetric decryption. That is, there is w such that $T_i\theta \vdash \text{enc}(u, w)$, $T_i\theta \vdash w$. By simplicity of the proof, the last rule applied when obtaining $\text{enc}(u, w)$ was an axiom or a decomposition, otherwise the same node would appear twice. Then applying the induction hypothesis we have that there is $t \in st(T_i)$, t not a variable, such that $t\theta = \text{enc}(u, w)$. It follows that $t = \text{enc}(t', t'')$ with $t'\theta = u$. If t' is a variable then $T_{t'}\theta \vdash t'\theta$. That is $T_{t'}\theta \vdash u$, which again contradicts the minimality of i . Hence t' is not variable, as required. For the other decomposition rules the same reasoning holds. \square

Theorem 1 Let \mathcal{C} be an unsolved constraint system.

1. (Termination) There is no infinite chain $\mathcal{C} \rightsquigarrow_{\sigma_1} \mathcal{C}_1 \dots \rightsquigarrow_{\sigma_n} \mathcal{C}_n$.
2. (Correctness) If $\mathcal{C} \rightsquigarrow_{\sigma}^* \mathcal{C}'$ for some constraint system \mathcal{C}' and some substitution σ and if θ is a solution of \mathcal{C}' then $\sigma\theta$ is a solution of \mathcal{C} .
3. (Completeness) If θ is a solution of \mathcal{C} , then there exist a solved constraint system \mathcal{C}' and substitutions σ, θ' such that $\theta = \sigma\theta'$, $\mathcal{C} \rightsquigarrow_{\sigma}^* \mathcal{C}'$ and θ' is a solution of \mathcal{C}' .

Proof. (Completeness) Let \mathcal{C} be an unsolved constraint system and θ be a solution of \mathcal{C} . We show that there is a constraint system \mathcal{C}' and a solution τ of \mathcal{C}' such that $\mathcal{C} \rightsquigarrow_{\sigma} \mathcal{C}'$ and $\theta = \sigma\tau$. Together with the termination property, this allows us to conclude that there exist a solved constraint system \mathcal{C}'' and substitutions σ', θ' such that $\theta = \sigma'\theta'$, $\mathcal{C} \rightsquigarrow_{\sigma'}^* \mathcal{C}''$ and θ' is a solution of \mathcal{C}'' .

Consider a minimal unsolved constraint $T_i \Vdash u_i$ such that u_i is not a variable.

We have $T_i\theta \vdash u_i\theta$. Consider a simple proof of $T_i\theta \vdash u_i\theta$. According to the last applied rule in this proof, we can have :

1. The last rule is a composition. Suppose that it is the pairing rule. That is, there are w_1, w_2 such that $T_i\theta \vdash w_1$, $T_i\theta \vdash w_2$ and $\langle w_1, w_2 \rangle = u_i\theta$. Since u_i is not a variable there exists u', u'' such that $u_i = \langle u', u'' \rangle$. Hence we can apply the simplification rule R_5 in order to obtain \mathcal{C}' . Since $u'\theta = w_1$ and $u''\theta = w_2$, the substitution θ is also a solution to \mathcal{C}' . For the other composition rule the same reasoning holds, applying this time the corresponding R_6 rule.
2. The last rule is an axiom or a decomposition. Applying Lemma 3 we obtain that there is $t \in st(T_i)$, t not a variable, such that $t\theta = u_i\theta$. We can have the following two possibilities :

- (a) If $t \neq u_i$ then we apply the simplification rule R_2 .
- (b) Otherwise, if $t = u_i$, then $u \in st(T_i)$. We consider the cases :
 - i. There are two distinct non variable terms $t_1, t_2 \in st(T)$ such that $t_1\theta = t_2\theta$. Then we apply the simplification rule R_3 .
 - ii. Otherwise, the simplification rule R_1 can be applied. This follows from Lemma 4. \square