Normalization and Subterm Property

Vaishnavi Sundararajan

Definition 1 (Term syntax)**.** A message is modelled as a term. The set of terms $\mathscr{T}$ is generated using the following grammar.

$$t := m \mid (t_1, t_2) \mid \mathbf{aenc}(t, \mathbf{pk}(k))$$

where $m, k, t, t_1, t_2 \in \mathscr{T}$, and m and k are "atomic" terms, i.e. terms without pairing or encryption.

Definition 2 (Proof system)**.** The proof system for this term algebra is shown in Table 1. If there is a proof of $X \vdash t$ using these rules, we denote it by $X \vdash_{pe} t$. The rules in the left column are *destructors*, while those in the right column are *constructor* rules.

For any $X \cup t \subseteq \mathscr{T}$, $X \vdash t$ is a *sequent*, and to be read as "X derives t". In a sequent, we will often refer to X and t as the LHS and RHS respectively. In any proof rule, every sequent that appears above the line is called a *premise*, and the sequent that appears below the line is called the *conclusion* of said rule. In this system, a proof rule can have up to two premises. The leftmost premise is often called the *major premise*.

$\dfrac{}{X \vdash m}\ \mathbf{ax}(m \in X)$	$\dfrac{}{X \vdash \mathbf{pk}(k)}\ \mathbf{pk}$
$\dfrac{X \vdash (t_1, t_2)}{X \vdash t_i}\ \mathbf{split}$	$\dfrac{X \vdash t \quad X \vdash u}{X \vdash (t, u)}\ \mathbf{pair}$
$\dfrac{X \vdash \mathbf{aenc}(t, \mathbf{pk}(k)) \quad X \vdash k}{X \vdash t}\ \mathbf{adec}$	$\dfrac{X \vdash t \quad X \vdash \mathbf{pk}(k)}{X \vdash \mathbf{aenc}(t, \mathbf{pk}(k))}\ \mathbf{aenc}$

Table 1: Proof system for a term algebra with pairing and asymmetric encryption

Definition 3 (Normal proof)**.** A *normal proof* is one where the major premise of a destructor rule is not obtained by the application of a constructor rule.

Theorem 4. Any proof in the above system can be converted into a normal proof.

Proof. Consider a proof π of minimal size witnessing $X \vdash t$. Suppose this proof is not normal – i.e. there is a subproof ξ of $X \vdash u$ such that ξ ends in a destructor rule, and the major premise of ξ is yielded by some constructor rule. We will show how to replace ξ by a smaller proof of $X \vdash u$, thus contradicting the minimality of π.

There are two possible cases, one for each of the destructor rules. One can see that the constructor yielding the major premise for a destructor rule must be the one that "corresponds" to the destructor; one cannot, for example, have **aenc** provide the major premise for the **split** rule.

ξ **ends in split:** There exist two terms u_0 and u_1 such that u is either u_0 or u_1, and ξ has the structure as on the left. u_i is derived using a proof π_i (it does not matter what rule π_i ends in). We can pick one of the premises of the **pair** rule, and obtain a normal proof equivalent to ξ, as shown on the right.

$$\dfrac{\dfrac{\begin{array}{c}\pi_0\\ \vdots\\ X \vdash u_0\end{array} \quad \begin{array}{c}\pi_1\\ \vdots\\ X \vdash u_1\end{array}}{X \vdash (u_0, u_1)}\,\textbf{pair}}{X \vdash u_i}\,\textbf{split} \qquad\Longrightarrow\qquad \begin{array}{c}\pi_i\\ \vdots\\ X \vdash u_i\end{array}$$

ξ **ends in adec:** There exist two terms u_0 and k such that an **aenc** produces the asymmetric encryption of u_0 with $\mathbf{pk}(k)$, which is then decrypted using **adec** to produce ξ, as shown on the left. We once again pick the major premise of the **aenc** rule to obtain the normal proof equivalent to ξ, as shown on the right.

$$\dfrac{\dfrac{\begin{array}{c}\pi_0\\ \vdots\\ X \vdash u_0\end{array} \quad \dfrac{}{X \vdash \mathbf{pk}(k)}\,\textbf{pk}}{X \vdash \mathbf{aenc}(u_0, \mathbf{pk}(k))}\,\textbf{aenc} \qquad \begin{array}{c}\pi_k\\ \vdots\\ X \vdash k\end{array}}{X \vdash u_0}\,\textbf{adec} \qquad\Longrightarrow\qquad \begin{array}{c}\pi_0\\ \vdots\\ X \vdash u_0\end{array}$$

Thus, we see that no conclusion of a constructor rule serves as the leftmost premise of a destructor rule in a minimal proof π of $X \vdash t$. Hence, π is a normal proof of $X \vdash t$.

QED

Definition 5 (Subterms of a term)**.** The subterms of a term t are defined as all the subtrees of the term tree of t.

Theorem 6. Suppose π is a normal proof of $X \vdash t$. Consider a subproof ξ witnessing $X \vdash u$. Then, $u \in \mathbf{st}(X \cup \{t\})$. In particular, if π ends in a destructor rule, $u \in \mathbf{st}(X)$.

Proof. The proof proceeds by induction on the structure of π. Suppose π ends in a rule $\mathbf{r}$. The following cases arise when $\mathbf{r}$ is a destructor.

$\mathbf{r} = \mathbf{ax}$: In this case, $t \in X$, and thus, $t \in \mathbf{st}(X)$.

$\mathbf{r} = \mathbf{split}$: In this case, π has the following structure.

$$\dfrac{\begin{matrix}\pi_0 \\ \vdots \\ X \vdash (t_0, t_1)\end{matrix}}{X \vdash t_i}\ \mathbf{split}$$

The subproof π_0 does not contain any constructor rules (since that would lead to non-normality). Hence, by induction hypothesis, $(t_0, t_1) \in \mathbf{st}(X)$, and hence $t_i \in \mathbf{st}(X)$ for $i \in \{0, 1\}$.

$\mathbf{r} = \mathbf{adec}$: In this case, π has the following structure.

$$\dfrac{\begin{matrix}\pi_0 \\ \vdots \\ X \vdash \mathbf{aenc}(t_0, \mathbf{pk}(k))\end{matrix} \qquad \begin{matrix}\pi_1 \\ \vdots \\ X \vdash k\end{matrix}}{X \vdash t_0}\ \mathbf{adec}$$

The subproof π_0 does not contain any constructor rules (since that would lead to non-normality). Hence, again by IH, $\mathbf{aenc}(t_0, \mathbf{pk}(k)) \in \mathbf{st}(X)$, and hence $t_0 \in \mathbf{st}(X)$.

Now, when $\mathbf{r}$ is a constructor, we have some more leeway.

$\mathbf{r} = \mathbf{pk}$: In this case, there is no premise. From any X, one can always derive $\mathbf{pk}(k)$ for any k. $\mathbf{pk}(k) \in \mathbf{st}(\mathbf{pk}(k)) \subseteq \mathbf{st}(X \cup \{\mathbf{pk}(k)\})$, and we are done.

$\mathbf{r} = \mathbf{pair}$: In this case, π has the following structure.

$$\dfrac{\begin{matrix}\pi_0 \\ \vdots \\ X \vdash t_0\end{matrix} \qquad \begin{matrix}\pi_1 \\ \vdots \\ X \vdash t_1\end{matrix}}{X \vdash (t_0, t_1)}\ \mathbf{pair}$$

By IH, $t_i \in \mathbf{st}(X \cup \{t_i\})$ for $i \in \{0, 1\}$. Thus, $(t_0, t_1) \in \mathbf{st}(X \cup \{t_0, t_1\})$. We can prove the claim similarly for when $\mathbf{r} = \mathbf{aenc}$.

QED