CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL
Institut für Informatik · AG Software Engineering
Priv.-Doz. Henning Schnoor

Engineering Secure Software Systems Winter 2020/21
Exercise Sheet 8

issued: January 5, 2021 **due:** January 14, 2021

Exercise 8.1, Needham-Schroeder as Horn clauses (10 Points)

Model the Needham-Schroeder protocol as Horn clauses and use this formalism to show that the protocol is insecure. To do this, first list the facts, Dolev-Yao deductions, protocol deductions and the target clause. Then, use logical inference to show that the protocol is in fact insecure. Do you see any limits or imprecisions in this approach?

Solution See presentation in the exercise class.

Exercise 8.2, Missing Proof (10 Points)

Prove the following lemma that was stated in the lecture without proof:

If E is a convergent equational theory, then:

1. For every term t, there is a unique term $[t]$ with
   - $[t]$ is in E-normal-form,
   - $t \equiv_E [t]$.
2. For terms t and t', we have that $t \equiv_E t'$ if and only if $[t] = [t']$.

Solution Let E be a convergent equational theory, let t, and t' be terms (over the term signature corresponding to E).

1. We first prove that a normal form exists. For this, let $t_0 = t$, and inductively define t_{i+1} as an arbitrary term with $t_i \twoheadrightarrow_E t_{i+1}$, where we choose $t_{i+1} \neq t_i$ if possible. Since E is terminating, we know that there is some i such that $t_i = t_j$ for all $j \geq i$. By choice of t_{i+1}, we have that t_i is in E-normal form, and by construction, $t \equiv t_i$.

   Now assume that t_{n_1} and t_{n_2} are both normal forms of t. Then, in particular, $t \twoheadrightarrow_E^* t_{n_1}$ and $t \twoheadrightarrow_E^* t_{n_2}$. Therefore, there exists some t_{nf} with $t_{n_1} \twoheadrightarrow_E^* t_{nf}$ and $t_{n_2} \twoheadrightarrow_E^* t_{nf}$. Since t_{n_1} and t_{n_2} are in normal form, it follows that $t_{n_1} = t_{nf}$ and $t_{n_2} = t_{nf}$. Therefore, $[t] = [t_{nf}]$.
2. First assume that $t \equiv_E t'$. Therefore, there are terms $t = t_0, \ldots, t_n = t'$ such that for each i, we have that $t_i \twoheadrightarrow_E t_{i+1}$ or $t_{i+1} \twoheadrightarrow_E t_i$. We prove the claim by induction over n.
   - *Induction Start.* If $n = 0$, then $t = t'$ and the claim holds trivially.
   - *Induction Step.* By induction, it follows that $[t_1] = [t_n]$. Hence it suffices to show that $[t_0] = [t_1]$. Without loss of generality, assume that $t_0 \twoheadrightarrow_E t_1$. Then t_1 is a possible step in the construction of the (unique) normal form of t_0 from the proof of the first part above, hence the claim follows.

   The other direction is trivial, since if $[t] = [t']$, we have that $t \equiv_E [t] = [t'] \equiv_E t'$.

Exercise 8.3, "Badly-Behaved" Equational Theories (10 Points)

Define equational theories for which the resulting rewrite relation $\twoheadrightarrow_E$ is not a convergent subterm theory, i.e., one that is not confluent, not terminating, or not a subterm theory.

Solution

- An example for a theory that is not terminating, but confluent, is the following:

  $$x = f(x)$$

  Here, an arbitrary number of f-symbols can be added to any term. The theory is confluent, it is in fact deterministic (for each term, exactly one rule can be applied).

- A theory that is terminating, but not confluent, is the following:

  $$f(x) = b$$
  $$f(x) = c$$

  where x is a variable, b and c are constants that do not appear elsewhere.

- A theory that is neither terminating not confluent is the following:

  $$f(x) = g(f(x))$$
  $$f(x) = h(f(x))$$

  The theory is not terminating, since each application of a rewrite rule produces a term with an f-fall as the innermost operator, hence a follow-up step can be performed. Further, it is not confluent, since the first step performed on e.g., $f(N_A)$ determines the outmost operator of all resulting transformation steps.