Exercise Class November 26, 2020

This is a slightly edited and re-formated transcript of the live notes taken in class. Solutions to the tasks are available in the folder `exercise_sheets`.

Exercise Sheet 3

Task: DY closure and derivations

prove: DY derivations and "stepwise derivations" are the same.

- stepwise derivation: every step is contained in DY closure.
- example: $L_d(\mathsf{enc}^{\mathsf{a}}_{k_A}(t))$ gives us t if we have $\hat{k}_A$, same as in DY closure
- similar for other L_c,L_d

Missing for the other direction: if we have $m \in \mathsf{DY}(S)$, then there is a stepwise derivation of m from S.

Problem: $\mathsf{DY}(S)$ defined as "closure operator", stepwise derivations single-step definition DY rule similar to stepwise derivations: compare "if $t, s \in S$, then $[t, s] \in S$" to $L_c([t, s])$

write $D(S)$ for the "derivation closure of S": smallest set T with

- $S \subseteq T$
- the result of every "applicable rule" for T is in T already (performing any L_d or L_c does not give us anything new).
- (example rule for $L_d(\mathsf{enc}^{\mathsf{a}}_{k_A}(t))$): if $t, \hat{k}_A, \mathsf{enc}^{\mathsf{a}}_{k_A}(t) \in T$, then also $t \in T$

Then $D(S)$ is exactly the set of terms that are "stepwise-derivable" from S. Proof for that fact: Assume there is some $t \in D(S)$ that you cannot get via stepwise derivation. Then, define $T = D(S) \setminus t$. Then T is also closed under application of rules (since we do not get t by one of the rules). Contradiction, because $D(S)$ is minimal.
To prove that $\mathsf{DY}(S)$ is the same as $D(S)$, it is enough to show: A set T is closed under DY-rules if and only if T is closed under "stepwise" rules. This can be done by direct "translation" of each DY/stepwise rule.