Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

A. Lochbihler and P. Müller

Formal Methods and Functional Programming

Tutorial 1: Haskell, Derivations and Proofs

Submission deadline: no submission required

Haskell Introduction

- installation following the instructions at:
  - http://www.haskell.org/platform/
  - for additional detail see exercise sheet 1
- pick text editor of choice, some examples:
  - emacs
  - vim
  - notepad++
- workflow:
  1. write/modify haskell source in text file
  2. load in ghci
  3. test your function definitions
  4. repeat from 1
- debugging: typecheck + runtime
  - see mistakes.hs and mistakes-fixed.hs on course webpage

Message Derivations:

Let a set $\mathbf{A}$ of atomic messages be given. $\mathcal{L}_\mathrm{M}$, the language of messages, is the smallest set where:

- $M \in \mathcal{L}_\mathrm{M}$ if $M \in \mathbf{A}$
- $\langle A, B\rangle \in \mathcal{L}_\mathrm{M}$ if $A, B \in \mathcal{L}_\mathrm{M}$ (pairing)
- $\{M\}_K \in \mathcal{L}_\mathrm{M}$ if $M, K \in \mathcal{L}_\mathrm{M}$ (encryption)

For a sequence of messages $M_1, \ldots, M_k$, we call $M_1, \ldots, M_k \vdash M$ a *sequent*. Informally, this corresponds to the assertion: M can be derived from the messages $M_1, \ldots, M_k$.

We now define the set of rules that define which sequents can be derived.

$$\frac{}{\Gamma, M \vdash M}\ \textsc{Ax}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash \langle A, B\rangle}\ \textsc{Pair-I} \qquad \frac{\Gamma \vdash \langle A, B\rangle}{\Gamma \vdash A}\ \textsc{Pair-EL} \qquad \frac{\Gamma \vdash \langle A, B\rangle}{\Gamma \vdash B}\ \textsc{Pair-ER}$$

$$\frac{\Gamma \vdash M \qquad \Gamma \vdash K}{\Gamma \vdash \{M\}_K}\ \textsc{Enc-I} \qquad \frac{\Gamma \vdash \{M\}_K \qquad \Gamma \vdash K}{\Gamma \vdash M}\ \textsc{Enc-E}$$

A *derivation* is a tree. Consider the sequence of messages $\Gamma = \langle k_1, k_2\rangle, \{\{s\}_{k_1}\}_{k_2}$, then the following tree is a derivation of the sequent $\Gamma \vdash s$.

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \{\{s\}_{k_1}\}_{k_2}}\ \textsc{Ax} \qquad \dfrac{\dfrac{}{\Gamma \vdash \langle k_1, k_2\rangle}\ \textsc{Ax}}{\Gamma \vdash k_2}\ \textsc{Pair-ER}}{\Gamma \vdash \{s\}_{k_1}}\ \textsc{Enc-E} \qquad \dfrac{\dfrac{}{\Gamma \vdash \langle k_1, k_2\rangle}\ \textsc{Ax}}{\Gamma \vdash k_1}\ \textsc{Pair-EL}}{\Gamma \vdash s}\ \textsc{Enc-E}$$

Exercises:

- Derive the sequent $k_1, \{k_2\}_{k_1}, \{s\}_{k_1} \vdash \{s\}_{k_2}$.
- Derive the sequent $\langle a, \langle b, c\rangle\rangle, \{s\}_{\langle\langle a,b\rangle,c\rangle} \vdash s$.

Knowledge proofs:

We now define the language of knowledge formulas $\mathcal{L}_\mathrm{F}$ as the smallest set where:

- $M\ known \in \mathcal{L}_\mathrm{F}$ if $M \in \mathcal{L}_\mathrm{M}$ (knowledge facts)
- $A \rightarrow B \in \mathcal{L}_\mathrm{F}$ if $A, B \in \mathcal{L}_\mathrm{F}$ (implication)

We can now write formulas such as $\langle a, b\rangle\ known \rightarrow \{a\}_b\ known$. We define the following set of rules that includes the previously defined rules lifted to knowledge facts.

$$\frac{}{\Gamma, A \vdash A}\ \textsc{Ax}$$

$$\frac{\Gamma \vdash A\ known \qquad \Gamma \vdash B\ known}{\Gamma \vdash \langle A, B\rangle\ known}\ \textsc{Pair-I} \qquad \frac{\Gamma \vdash \langle A, B\rangle\ known}{\Gamma \vdash A\ known}\ \textsc{Pair-EL}$$

$$\frac{\Gamma \vdash \langle A, B\rangle\ known}{\Gamma \vdash B\ known}\ \textsc{Pair-ER}$$

$$\frac{\Gamma \vdash M\ known \qquad \Gamma \vdash K\ known}{\Gamma \vdash \{M\}_K\ known}\ \textsc{Enc-I} \qquad \frac{\Gamma \vdash \{M\}_K\ known \qquad \Gamma \vdash K\ known}{\Gamma \vdash M\ known}\ \textsc{Enc-E}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}\ \rightarrow\text{-I} \qquad \frac{\Gamma \vdash A \rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \rightarrow\text{-E}$$

A *proof* of a formula F is a derivation of the sequent $\vdash F$. For example, the following is a proof of $\langle a, b\rangle\ known \rightarrow \{a\}_b\ known$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\langle a, b\rangle\ known \vdash \langle a, b\rangle\ known}\ \textsc{Ax}}{\langle a, b\rangle\ known \vdash a\ known}\ \textsc{Pair-EL} \qquad \dfrac{\dfrac{}{\langle a, b\rangle\ known \vdash \langle a, b\rangle\ known}\ \textsc{Ax}}{\langle a, b\rangle\ known \vdash b\ known}\ \textsc{Pair-ER}}{\langle a, b\rangle\ known \vdash \{a\}_b\ known}\ \textsc{Enc-I}}{\vdash \langle a, b\rangle\ known \rightarrow \{a\}_b\ known}\ \rightarrow\text{-I}$$

Exercises:

- Prove the formula $a\ known \rightarrow \langle \{b\}_a, \{s\}_{\{a\}_b}\rangle\ known \rightarrow s\ known$.
- Prove the formula
  $d\ known \rightarrow (\{s\}_b\ known \rightarrow b\ known) \rightarrow \{\langle \{\{s\}_b\}_c, c\rangle\}_d\ known \rightarrow s\ known$.