Formal Methods and Functional Programming - Week 1

Ralf Sasse

February 18

General information

Basics:

- one exercise session per week
- one exercise sheet per week - due Monday by 11.00
  - submit by email or drop in box in front of CNB F101

Content of exercise session:

- feedback on last exercise sheet hand-ins
- explain solutions of (parts of) that sheet
- give *preview* information about new exercise sheet

Haskell introduction

- installation
- pick text editor of choice
- workflow demonstrated shortly:
    1. write/modify haskell source in text file
    2. load in ghci
    3. test your function definitions
    4. repeat from 1
- debugging: typecheck + runtime
    - mistakes demo

Demo

DEMO

Motivation message derivations

- Assume we have a network protocol which enables Alice and Bob to talk to each other.
- They talk about sensitive things, so they protect the messages using cryptography
- Charlie owns a router somewhere in the middle of the network and he'd like to learn (at least some part of) what Alice and Bob are talking about
- Can he combine the crypto messages he sees in some clever way to get to the secret stuff?
- Alternatively: what messages can he derive from the messages he sees?
- We'd like to reason about this formally

Crypto Messages

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)

Message Derivations

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 $M_1, \ldots, M_k$.

Derivation rules:

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

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

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

Derivations

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 $\Gamma \vdash s$.

Exercises I

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

Derivation rules:

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

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

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

Knowledge proofs

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

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

We can now write formulas such as
$\langle a, b \rangle$ *known* $\rightarrow \{a\}_b$ *known*.

Proof rules

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

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

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

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

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

Proof

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

Exercises II

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

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

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

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

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

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