Prelude: Formalities

Governement health warning

This is formal.

This is very formal.

This is machine checked!
(In the theorem prover Isabelle/HOL)

Basic types

- Truth values: *bool* (*True*, *False*, $\wedge$, ...)
- Natural numbers: *nat*
- Integers: *int*
- Total functions: $\Rightarrow$
- Sets over type τ: τ *set*
- Type variables: *'a*, *'b*, ...

Notation

$t :: \tau$

"term t has type τ"

Pairs

- First component: $fst\ (x, y) = x$
- Second component: $snd\ (x, y) = y$
- Tuples are pairs nested to the right:
  - (a, b, c) means $(a, (b, c))$
  - $\tau_1 \times \tau_2 \times \tau_3$ means $\tau_1 \times (\tau_2 \times \tau_3)$

Lists

- Type: τ *list*
- Empty list: $[]$
- Cons: $x \cdot xs$
- Append: $xs \mathbin{@} ys$
- Length: $|xs|$
- Nth element: $xs_{[n]}$
- *map* :: $('a \Rightarrow 'b) \Rightarrow 'a\ list \Rightarrow 'b\ list$
- *set* :: $'a\ list \Rightarrow 'a\ set$
- *distinct* :: $'a\ list \Rightarrow bool$

Datatype option

datatype $'a\ option = None \mid Some\ 'a$

An abbreviation: $\lfloor a \rfloor \equiv Some\ a$

Partial functions or maps

$$'a \rightharpoonup 'b \quad \equiv \quad 'a \Rightarrow 'b\ option$$

Unituitively: if $f :: \tau_1 \rightharpoonup \tau_2$ and $a :: \tau_1$ then

- $f\ a = None$ means undefined
- $f\ a = \lfloor b \rfloor$ means result is b

$$dom\ m \equiv \{a \mid m\ a \neq None\}$$

Map notation

- Empty map: $empty \equiv \lambda x.\ None$
- Update: $m(a \mapsto b) \equiv \lambda x.\ if\ x{=}a\ then\ \lfloor b \rfloor\ else\ m\ x$
- Updates: $m(a_1 \mapsto b_1, a_2 \mapsto b_2) \equiv m(a_1 \mapsto b_1)(a_2 \mapsto b_2)$
- Finite maps: $[a_1 \mapsto b_1, \ldots] \equiv empty(a_1 \mapsto b_1, \ldots)$
- List update: $m([a_1,\ldots,a_i]\ [\mapsto]\ [b_1,\ldots,b_j]) \equiv m(a_1 \mapsto b_1,\ldots,a_{min\ i\ j} \mapsto b_{min\ i\ j})$
- $map\text{-}of :: ('a \times 'b)list \Rightarrow 'a \rightharpoonup 'b$
  $map\text{-}of\ [(a_1,b_1),\ldots,(a_n,b_n)] = [a_n \mapsto b_n,\ldots,a_1 \mapsto b_1]$
- Overwrite:
  $m_1 +\!+ m_2 \equiv \lambda x.\ if\ x \in dom\ m_2\ then\ m_2\ x\ else\ m_1\ x$

Inference rule notations

$$[\![A_1; \ldots; A_n]\!] \Longrightarrow A$$

$$A_1 \Longrightarrow \ldots\ A_n \Longrightarrow A$$

$$\frac{A_1 \quad \ldots \quad A_n}{A}$$

Different syntax, same meaning