More types

CS 152 (Spring 2022)

Harvard University

Thursday, March 3, 2022
Today, we will learn about

- typing extensions to the simply-typed lambda-calculus
Products

Syntax:

\[(e_1, e_2)\]

\[\#1 e\]

\[\#2 e\]

Context:

\[E ::= \ldots | (E, e) | (v, E) | \#1 E | \#2 E\]

Operational semantic rules:

\[\#1 (v_1, v_2) \rightarrow v_1\]

\[\#2 (v_1, v_2) \rightarrow v_2\]
Typing of Products

Product type: \( \tau_1 \times \tau_2 \)

Typing rules:

\[
\Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e_2 : \tau_2 \\
\Gamma \vdash (e_1, e_2) : \tau_1 \times \tau_2
\]

\[
\Gamma \vdash e : \tau_1 \times \tau_2 \\
\Gamma \vdash \#1 e : \tau_1
\]

\[
\Gamma \vdash e : \tau_1 \times \tau_2 \\
\Gamma \vdash \#2 e : \tau_2
\]
**Sums**

Syntax:

\[ e ::= \cdots \mid \text{inl}_{\tau_1+\tau_2} e \mid \text{inr}_{\tau_1+\tau_2} e \mid \text{case} e_1 \text{ of } e_2 \mid e_3 \]

\[ v ::= \cdots \mid \text{inl}_{\tau_1+\tau_2} v \mid \text{inr}_{\tau_1+\tau_2} v \]

Context:

\[ E ::= \cdots \mid \text{inl}_{\tau_1+\tau_2} E \mid \text{inr}_{\tau_1+\tau_2} E \mid \text{case} E \text{ of } e_2 \mid e_3 \]

Operational rules:

\[
\text{case } \text{inl}_{\tau_1+\tau_2} v \text{ of } e_2 \mid e_3 \longrightarrow e_2 \mid v
\]

\[
\text{case } \text{inr}_{\tau_1+\tau_2} v \text{ of } e_2 \mid e_3 \longrightarrow e_3 \mid v
\]
Typing of Sums

Sum type: \( \tau_1 + \tau_2 \)

Typing rules:

\[
\begin{align*}
\Gamma & \vdash e : \tau_1 \\
\Gamma & \vdash \text{inl}_{\tau_1 + \tau_2} e : \tau_1 + \tau_2
\end{align*}
\]

\[
\begin{align*}
\Gamma & \vdash e : \tau_2 \\
\Gamma & \vdash \text{inr}_{\tau_1 + \tau_2} e : \tau_1 + \tau_2
\end{align*}
\]

\[
\begin{align*}
\Gamma & \vdash e : \tau_1 + \tau_2 \quad \Gamma & \vdash e_1 : \tau_1 \rightarrow \tau \quad \Gamma & \vdash e_2 : \tau_2 \rightarrow \tau \\
\Gamma & \vdash \text{case } e \text{ of } e_1 \mid e_2 : \tau
\end{align*}
\]
Example Program

\[
\text{let } f : (\text{int } + \text{ (int } \rightarrow \text{ int})) \rightarrow \text{ int } = \\
\quad \lambda a : \text{int } + \text{ (int } \rightarrow \text{ int}). \\
\quad \text{case } a \text{ of } \lambda y. y + 1 \mid \lambda g. g \ 35 \ \text{in} \\
\text{let } h : \text{int } \rightarrow \text{ int } = \lambda x : \text{int}. x + 7 \ \text{in} \\
f \ (\text{inr}_{\text{int } + \text{ (int } \rightarrow \text{ int)}} \ h)
\]
Recursion

We saw in last lecture that we could not type recursive functions or fixed-point combinators in the simply-typed lambda calculus. So instead of trying (and failing) to define a fixed-point combinator in the simply-typed lambda calculus, we add a new primitive $\mu x : \tau. \ e$ to the language. The evaluation rules for the new primitive will mimic the behavior of fixed-point combinators.
Recursion: Syntax

\[ e ::= \cdots | \mu x : \tau. e \]

Intuitively, \( \mu x : \tau. e \) is the fixed-point of the function \( \lambda x : \tau. e \).

Note that \( \mu x : \tau. e \) is not a value, regardless of whether \( e \) is a value or not.
Recursion: Operational Semantics

There is a new axiom, but no new evaluation contexts.

\[
\mu x : \tau. \ e \rightarrow e\left\{ (\mu x : \tau. \ e) / x \right\}
\]

Note that we can define the `letrec` \( x : \tau = e_1 \) in \( e_2 \) construct in terms of this new expression.

\[
\text{letrec } x : \tau = e_1 \text{ in } e_2 \triangleq \text{let } x : \tau = \mu x : \tau. \ e_1 \text{ in } e_2
\]
Recursion: Typing

\[\Gamma \vdash e : \tau\]

\[\Gamma \vdash \mu x : \tau. e : \tau\]
Example Program

\[ FACT \triangleq \mu f : \text{int} \rightarrow \text{int}. \]
\[ \lambda n : \text{int}. \text{if } n = 0 \text{ then } 1 \text{ else } n \times (f (n - 1)) \]

\[
\text{letrec } \text{fact} : \text{int} \rightarrow \text{int} \\
= \lambda n : \text{int}. \text{if } n = 0 \text{ then } 1 \text{ else } n \times (\text{fact} (n - 1)) \\
\text{in } \ldots
\]
Non-termination?

Recall operational semantics:

\[ \mu x : \tau. \ e \rightarrow e\{(\mu x : \tau. \ e)/x\} \]

Recall typing:

\[ \Gamma \vdash e : \tau \]

\[ \vdash \Gamma \vdash \mu x : \tau. \ e : \tau \]
We can write non-terminating computations for any type: the expression $\mu x : \tau. x$ has type $\tau$, and does not terminate.
Although the $\mu x: \tau. e$ expression is normally used to define recursive functions, it can be used to find fixed points of any type. For example, consider the following expression.

$$\mu x: (\text{int} \to \text{bool}) \times (\text{int} \to \text{bool}).$$

$$(\lambda n: \text{int}. \text{if } n = 0 \text{ then true else } ((\#2 x) (n - 1)),$$

$$\lambda n: \text{int}. \text{if } n = 0 \text{ then false else } ((\#1 x) (n - 1))$$

This expression has type $(\text{int} \to \text{bool}) \times (\text{int} \to \text{bool})$—it is a pair of mutually recursive functions; the first function returns true only if its argument is even; the second function returns true only if its argument is odd.
References: Syntax and Semantics

\[
e ::= \cdots | \text{ref } e | !e | e_1 := e_2 | \ell
\]

\[
v ::= \cdots | \ell
\]

\[
E ::= \cdots | \text{ref } E | !E | E := e | v := E
\]

\[
\text{ALLOC} \quad \frac{\langle \text{ref } v, \sigma \rangle}{\langle \ell, \sigma[\ell \mapsto v] \rangle} \quad \ell \not\in \text{dom}(\sigma)
\]

\[
\text{DEREF} \quad \frac{\langle !\ell, \sigma \rangle}{\langle v, \sigma \rangle} \quad \sigma(\ell) = v
\]

\[
\text{ASSIGN} \quad \frac{\langle \ell := v, \sigma \rangle}{\langle v, \sigma[\ell \mapsto v] \rangle}
\]
Reference Type $\tau$ ref

- We add a new type for references: type $\tau$ ref is the type of a location that contains a value of type $\tau$.

- For example the expression ref 7 has type int ref, since it evaluates to a location that contains a value of type int.

- Dereferencing a location of type $\tau$ ref results in a value of type $\tau$, so $!e$ has type $\tau$ if $e$ has type $\tau$ ref.

- And for assignment $e_1 := e_2$, if $e_1$ has type $\tau$ ref, then $e_2$ must have type $\tau$. 
References: Typing

\[ \tau ::= \cdots \mid \tau \text{ ref} \]

\[
\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{ref } e : \tau \text{ ref}} \quad \frac{\Gamma \vdash e : \tau \text{ ref}}{\Gamma \vdash !e : \tau}
\]

\[
\frac{\Gamma \vdash e_1 : \tau \text{ ref} \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1 := e_2 : \tau}
\]
How do we type locations?
Noticeable by its absence is a typing rule for location values. What is the type of a location value $\ell$? Clearly, it should be of type $\tau \text{ ref}$, where $\tau$ is the type of the value contained in location $\ell$. But how do we know what value is contained in location $\ell$? We could directly examine the store, but that would be inefficient. In addition, examining the store directly may not give us a conclusive answer! Consider, for example, a store $\sigma$ and location $\ell$ where $\sigma(\ell) = \ell$; what is the type of $\ell$?
Instead, we introduce *store typings* to track the types of values stored in locations. Store typings are partial functions from locations to types. We use metavariable Σ to range over store typings. Our typing relation now becomes a relation over 4 entities: typing contexts, store typings, expressions, and types. We write Γ, Σ ⊢ e : τ when expression e has type τ under typing context Γ and store typing Σ.
References: Typing

\[
\Gamma, \Sigma \vdash e : \tau \\
\Gamma, \Sigma \vdash \text{ref } e : \tau \text{ ref} \\
\Gamma, \Sigma \vdash e_1 : \tau \text{ ref} \quad \Gamma, \Sigma \vdash e_2 : \tau \\
\Gamma, \Sigma \vdash e_1 := e_2 : \tau \\
\Gamma, \Sigma \vdash \ell : \tau \text{ ref} \\
\Sigma(\ell) = \tau
\]
So, how do we state type soundness? Our type soundness theorem for simply-typed lambda calculus said that if $\Gamma \vdash e : \tau$ and $e \longrightarrow^* e'$ then $e'$ is not stuck. But our operational semantics for references now has a store, and our typing judgment now has a store typing in addition to a typing context. We need to adapt the definition of type soundness appropriately. To do so, we define what it means for a store to be well-typed with respect to a typing context.
Store $\sigma$ is well-typed with respect to typing context $\Gamma$ and store typing $\Sigma$, written $\Gamma, \Sigma \vdash \sigma$, if $\text{dom}(\sigma) = \text{dom}(\Sigma)$ and for all $\ell \in \text{dom}(\sigma)$ we have $\Gamma, \Sigma \vdash \sigma(\ell) : \tau$ where $\Sigma(\ell) = \tau$. 

References: Soundness Aux. Def.
References: Soundness Theorem

If $\emptyset, \Sigma \vdash e : \tau$ and $\emptyset, \Sigma \vdash \sigma$ and

$< e, \sigma > \rightarrow^* < e', \sigma' >$ then either $e'$ is a value, or

there exists $e''$ and $\sigma''$ such that

$< e', \sigma' > \rightarrow < e'', \sigma'' >$. 
We can prove type soundness for our language using the same strategy as for the simply-typed lambda calculus: we use preservation and progress. The progress lemma can be easily adapted for the semantics and type system for references. Adapting preservation is a little more involved, since we need to describe how the store typing changes as the store evolves. The rule `ALLOC` extends the store $\sigma$ with a fresh location $\ell$, producing store $\sigma'$. Since $\text{dom}(\Sigma) = \text{dom}(\sigma) \neq \text{dom}(\sigma')$, it means that we will not have $\sigma'$ well-typed with respect to typing store $\Sigma$. 
Since the store can increase in size during the evaluation of the program, we also need to allow the store typing to grow as well.
If $\emptyset, \Sigma \vdash e : \tau$ and $\emptyset, \Sigma \vdash \sigma$ and
$< e, \sigma > \rightarrow < e', \sigma'>$ then there exists some $\Sigma' \supseteq \Sigma$ such that $\emptyset, \Sigma' \vdash e' : \tau$ and $\emptyset, \Sigma' \vdash \sigma'$. 