CMSC 330: Organization of Programming Languages

Operational Semantics
Formal Semantics of a Prog. Lang.

- Mathematical description of the meaning of programs written in that language
  - What a program computes, and what it does

- Three main approaches to formal semantics
  - Operational ⇐ this course
    - Often on an abstract machine (mathematical model of computer)
    - Analogous to interpretation
  - Denotational
  - Axiomatic
Operational Semantics

- We will show how an operational semantics may be defined for Micro-Ocaml
  - And develop an interpreter for it, along the way

- Approach: use rules to define a judgment

\[ e \Rightarrow v \]

Says “*e evaluates to* \( v \)”

- \( e \): expression in Micro-Ocaml
- \( v \): value that results from evaluating \( e \)
Definitional Interpreter

- Rules for judgment $e \Rightarrow v$ can be easily turned into idiomatic OCaml code for an interpreter
  - The language’s expressions $e$ and values $v$ have corresponding OCaml datatype representations $\text{exp}$ and $\text{value}$
  - The semantics is represented as a function

\[
\text{eval: exp} \rightarrow \text{value}
\]

- This way of presenting the semantics is referred to as a definitional interpreter
  - The interpreter defines the language’s meaning
Abstract Syntax Tree spec. via “Grammar”

- We use a grammar for \( e \) to **directly** describe an expression’s abstract syntax tree (AST), i.e., \( e \)'s structure.

\[
e ::= x | n | e + e | \text{let } x = e \text{ in } e
\]

corresponds to (in definitional interpreter)

```plaintext
type id = string
type num = int
type exp =
  | Ident of id       (* x *)
  | Num of num       (* n *)
  | Plus of exp * exp (* e+e *)
  | Let of id * exp * exp
                   (* let x=e in e *)
```

We are *not* concerned about the process of **parsing**, i.e., from text to an AST. We can thus ignore issues of ambiguity, etc. and focus on the **structure** of the AST given by the grammar.
Micro-OCaml Expression Grammar

e ::= x | n | e + e | let x = e in e

- e, x, n are meta-variables that stand for categories of syntax (like non-terminals in a CFG)
  - x is any identifier (like z, y, foo)
  - n is any numeral (like 1, 0, 10, -25)
  - e is any expression (here defined, recursively!)

- Concrete syntax of actual expressions in black
  - Such as let, +, z, foo, in, ... (like terminals in a CFG)

- ::= and | are meta-syntax used to define the syntax of a language
  (part of “Backus-Naur form,” or BNF)
Micro-OCaml Expression Grammar

\[ e ::= x \mid n \mid e + e \mid \text{let } x = e \text{ in } e \]

Examples

- 1 is a numeral \( n \) which is an expression \( e \)
- 1+z is an expression \( e \) because
  - 1 is an expression \( e \),
  - \( z \) is an identifier \( x \), which is an expression \( e \), and
  - \( e + e \) is an expression \( e \)

- let \( z = 1 \) in 1+z is an expression \( e \) because
  - \( z \) is an identifier \( x \),
  - 1 is an expression \( e \),
  - 1+z is an expression \( e \), and
  - let \( x = e \) in \( e \) is an expression \( e \)
Values

- A value $v$ is an expression’s final result
  \[ v ::= n \]

- Just numerals for now
  - In terms of an interpreter’s representation:
    \[ \text{type value} = \text{int} \]
  - In a full language, values $v$ will also include booleans (true, false), strings, functions, …
Defining the Semantics

- Use rules to define judgment $e \Rightarrow v$

- Judgments are just statements. We use rules to prove that the statement is true.
  - $1+3 \Rightarrow 4$
    - $1+3$ is an expression $e$, and 4 is a value $v$
    - This judgment claims that $1+3$ evaluates to 4
    - We use rules to prove it to be true
  - $\text{let foo}=1+2 \text{ in foo}+5 \Rightarrow 8$
  - $\text{let } f=1+2 \text{ in let } z=1 \text{ in } f+z \Rightarrow 4$
Suppose $e$ is a numeral $n$

- Then $e$ evaluates to itself, i.e., $n \Rightarrow n$

Suppose $e$ is an addition expression $e_1 + e_2$

- If $e_1$ evaluates to $n_1$, i.e., $e_1 \Rightarrow n_1$
- And if $e_2$ evaluates to $n_2$, i.e., $e_2 \Rightarrow n_2$
- Then $e$ evaluates to $n_3$, where $n_3$ is the sum of $n_1$ and $n_2$
- I.e., $e_1 + e_2 \Rightarrow n_3$

Suppose $e$ is a let expression $\text{let } x = e_1 \text{ in } e_2$

- If $e_1$ evaluates to $v$, i.e., $e_1 \Rightarrow v_1$
- And if $e_2\{v_1/x\}$ evaluates to $v_2$, i.e., $e_2\{v_1/x\} \Rightarrow v_2$
  - Here, $e_2\{v_1/x\}$ means “the expression after substituting occurrences of $x$ in $e_2$ with $v_1$”
- Then $e$ evaluates to $v_2$, i.e., $\text{let } x = e_1 \text{ in } e_2 \Rightarrow v_2$
Rules are Lego Blocks

- **P** = 8.0 mm
  - = 5/6 × **H**
  - = 2.5 × **h**

- **h** = 3.2 mm
  - = 1/3 × **H**
  - = 0.4 × **P**

- **2 × P** = 0.2 mm
  - = 15.8 mm

- **H** = 9.6 mm
  - = 3 × **h**
  - = 1.2 × **P**

- **4.8 mm**
  - **1.7 mm**

- **3.2 mm**

- **LEGO**

---

![LEGO car](image-url)
We can use a more compact notation for the rules we just presented: rules of inference

- Has the following format
  
  \[
  \begin{array}{c}
  H_1 \ldots \ H_n \\
  \hline
  C
  \end{array}
  \]

- Says: if the conditions $H_1 \ldots H_n$ ("hypotheses") are true, then the condition $C$ ("conclusion") is true
- If $n=0$ (no hypotheses) then the conclusion automatically holds; this is called an axiom

We are using inference rules where $C$ is our judgment about evaluation, i.e., that $e \Rightarrow v$
Rules of Inference: Num and Sum

- Suppose $e$ is a numeral $n$
  - Then $e$ evaluates to itself, i.e., $n \Rightarrow n$

- Suppose $e$ is an addition expression $e_1 + e_2$
  - If $e_1$ evaluates to $n_1$, i.e., $e_1 \Rightarrow n_1$
  - If $e_2$ evaluates to $n_2$, i.e., $e_2 \Rightarrow n_2$
  - Then $e$ evaluates to $n_3$, where $n_3$ is the sum of $n_1$ and $n_2$, i.e., $e_1 + e_2 \Rightarrow n_3$
Rules of Inference: Let

- Suppose $e$ is a let expression $\text{let } x = e_1 \text{ in } e_2$
  - If $e_1$ evaluates to $v$, i.e., $e_1 \Rightarrow v_1$
  - If $e_2\{v_1/x\}$ evaluates to $v_2$, i.e., $e_2\{v_1/x\} \Rightarrow v_2$
  - Then $e$ evaluates to $v_2$, i.e., $\text{let } x = e_1 \text{ in } e_2 \Rightarrow v_2$

\[
\begin{array}{c}
  e_1 \Rightarrow v_1 \quad e_2\{v_1/x\} \Rightarrow v_2 \\
\hline
  \text{let } x = e_1 \text{ in } e_2 \Rightarrow v_2
\end{array}
\]
Derivations

When we apply rules to an expression in succession, we produce a derivation
  • It’s a kind of tree, rooted at the conclusion

Produce a derivation by goal-directed search
  • Pick a rule that could prove the goal
  • Then repeatedly apply rules on the corresponding hypotheses

  Goal: Show that \( \text{let } x = 4 \text{ in } x+3 \Rightarrow 7 \)
Goal: show that
let x = 4 in x+3 ⇒ 7

4 ⇒ 4  3 ⇒ 3  7 is 4+3

4 ⇒ 4  4+3 ⇒ 7

let x = 4 in x+3 ⇒ 7
Quiz 1

What is derivation of the following judgment?

\[ 2 + (3 + 8) \Rightarrow 13 \]

(a) 
\[
\begin{align*}
2 & \Rightarrow 2 \\
3 + 8 & \Rightarrow 11 \\
\hline
2 + (3 + 8) & \Rightarrow 13
\end{align*}
\]

(b) 
\[
\begin{align*}
8 & \Rightarrow 8 \\
3 & \Rightarrow 3 \\
11 & \text{is } 3+8 \\
\hline
2 & \Rightarrow 2 \\
3 + 8 & \Rightarrow 11 \\
13 & \text{is } 2+11 \\
\hline
2 + (3 + 8) & \Rightarrow 13
\end{align*}
\]

(c) 
\[
\begin{align*}
3 & \Rightarrow 3 \\
8 & \Rightarrow 8 \\
\hline
3 + 8 & \Rightarrow 11 \\
2 & \Rightarrow 2 \\
\hline
2 + (3 + 8) & \Rightarrow 13
\end{align*}
\]
Quiz 1

What is derivation of the following judgment?

\[ 2 + (3 + 8) \Rightarrow 13 \]

(a)  
\[
\begin{align*}
2 \Rightarrow 2 & \quad 3 + 8 \Rightarrow 11 \\
\hline
2 + (3 + 8) & \Rightarrow 13
\end{align*}
\]

(b)  
\[
\begin{align*}
8 \Rightarrow 8 & \\
3 \Rightarrow 3 & \\
11 \text{ is } 3+8 & \\
\hline
2 \Rightarrow 2 & \quad 3 + 8 \Rightarrow 11 & \quad 13 \text{ is } 2+11 \\
\hline
2 + (3 + 8) & \Rightarrow 13
\end{align*}
\]

(c)  
\[
\begin{align*}
3 \Rightarrow 3 & \quad 8 \Rightarrow 8 \\
\hline
3 + 8 \Rightarrow 11 & \quad 2 \Rightarrow 2 \\
\hline
2 + (3 + 8) & \Rightarrow 13
\end{align*}
\]
Definitional Interpreter

- The style of rules lends itself directly to the implementation of an interpreter as a recursive function.

```ocaml
let rec eval (e:exp):value =  
  match e with
  | Ident x -> (* no rule *)
    failwith "no value"
  | Num n -> n
  | Plus (e1,e2) ->
    let n1 = eval e1 in
    let n2 = eval e2 in
    let n3 = n1+n2 in
    n3
  | Let (x,e1,e2) ->
    let v1 = eval e1 in
    let e2' = subst v1 x e2 in
    let v2 = eval e2' in
    v2
```

- \[ n \Rightarrow n \]
- \[ e_1 \Rightarrow n_1 \quad e_2 \Rightarrow n_2 \quad n_3 \text{ is } n_1+n_2 \]
- \[ e_1 + e_2 \Rightarrow n_3 \]
- \[ e_1 \Rightarrow v_1 \quad e_2\{v_1/x\} \Rightarrow v_2 \]
- \[ \text{let } x = e_1 \text{ in } e_2 \Rightarrow v_2 \]
Derivations = Interpreter Call Trees

Has the same shape as the recursive call tree of the interpreter:

\[
\begin{align*}
\text{let } x &= 4 \text{ in } x+3 &\Rightarrow 7 \\
4 \Rightarrow 4 &\quad 3 \Rightarrow 3 & 7 \text{ is } 4+3 \\
4+3 \Rightarrow 7 &
\end{align*}
\]
Semantics Defines Program Meaning

- \( e \Rightarrow v \) holds if and only if a proof can be built
  - Proofs are derivations: axioms at the top, then rules whose hypotheses have been proved to the bottom
  - No proof means there exists no \( v \) for which \( e \Rightarrow v \)
- Proofs can be constructed bottom-up
  - In a goal-directed fashion
- Thus, function \( \text{eval } e = \{ v \mid e \Rightarrow v \} \)
  - Determinism of semantics implies at most one element for any \( e \)
- So: Expression \( e \) means \( v \)
Environment-style Semantics

- So far, semantics used substitution to handle variables
  - As we evaluate, we replace all occurrences of a variable $x$ with values it is bound to

- An alternative semantics, closer to a real implementation, is to use an environment
  - As we evaluate, we maintain an explicit map from variables to values, and look up variables as we see them
Environments

- Mathematically, an environment is a partial function from identifiers to values
  - If $A$ is an environment, and $x$ is an identifier, then $A(x)$ can either be
    - a value $v$ (intuition: the value of the variable stored on the stack)
    - undefined (intuition: the variable has not been declared)

- An environment can visualized as a table
  - If $A$ is

<table>
<thead>
<tr>
<th>Id</th>
<th>Val</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>0</td>
</tr>
<tr>
<td>$y$</td>
<td>2</td>
</tr>
</tbody>
</table>

  - then $A(x)$ is 0, $A(y)$ is 2, and $A(z)$ is undefined
Notation, Operations on Environments

- is the empty environment

- $A, \mathbf{x} : \mathbf{v}$ is the environment that extends $A$ with a mapping from $\mathbf{x}$ to $\mathbf{v}$
  - Sometimes just write $\mathbf{x} : \mathbf{v}$ instead of $\cdot, \mathbf{x} : \mathbf{v}$ for brevity
  - NB. if $A$ maps $\mathbf{x}$ to some $\mathbf{v}'$, then that mapping is shadowed by $\cdot$ in $A, \mathbf{x} : \mathbf{v}$

- Lookup $A(\mathbf{x})$ is defined as follows
  
  $$(A, \; \mathbf{y} : \mathbf{v})(\mathbf{x}) = \begin{cases} 
  \mathbf{v} & \text{if } \mathbf{x} = \mathbf{y} \\
  A(\mathbf{x}) & \text{if } \mathbf{x} \nless \mathbf{y} \text{ and } A(\mathbf{x}) \text{ defined} \\
  \text{undefined} & \text{otherwise}
  \end{cases}$$
An environment is just a list of mappings, which are just pairs of variable to value - called an association list
Semantics with Environments

- The environment semantics changes the judgment
  \[ e \Rightarrow v \]

to be

\[ A; e \Rightarrow v \]

where \( A \) is an environment
- Idea: \( A \) is used to give values to the identifiers in \( e \)
- \( A \) can be thought of as containing declarations made up to \( e \)

- Previous rules can be modified by
  - Inserting \( A \) everywhere in the judgments
  - Adding a rule to look up variables \( x \) in \( A \)
  - Modifying the rule for \texttt{let} to add \( x \) to \( A \)
Environment-style Rules

\[
\begin{align*}
A(x) &= v \\
\Rightarrow \\
A; x &
\equiv v
\end{align*}
\]

Look up variable \(x\) in environment \(A\)

\[
\begin{align*}
A; e1 &
\equiv v1 \\
A, x &: v1; e2 &
\equiv v2
\end{align*}
\]

\[
A; \text{let } x = e1 \text{ in } e2 &
\equiv v2
\]

Extend environment \(A\) with mapping from \(x\) to \(v1\)

\[
\begin{align*}
A; e1 &
\equiv n1 \\
A; e2 &
\equiv n2 \\
n3 &
\text{is } n1 + n2
\end{align*}
\]

\[
A; e1 + e2 &
\equiv n3
\]
let rec eval env e =
  match e with
  | Ident x -> lookup env x
  | Num n -> n
  | Plus (e1,e2) ->
    let n1 = eval env e1 in
    let n2 = eval env e2 in
    let n3 = n1+n2 in
    n3
  | Let (x,e1,e2) ->
    let v1 = eval env e1 in
    let env’ = extend env x v1 in
    let v2 = eval env’ e2 in
    v2
What is a derivation of the following judgment?

•; let x=3 in x+2 ⇒ 5

(a) 

x ⇒ 3  2 ⇒ 2  5 is 3+2

----------------------

3 ⇒ 3  x+2 ⇒ 5

----------------------

let x=3 in x+2 ⇒ 5

(b) 

x:3; x ⇒ 3  x:3; 2 ⇒ 2  5 is 3+2

----------------------

•; 3 ⇒ 3  x:3; x+2 ⇒ 5

----------------------

•; let x=3 in x+2 ⇒ 5

(c) 

x:2; x⇒3  x:2; 2⇒2  5 is 3+2

----------------------

•; let x=3 in x+2 ⇒ 5
What is a derivation of the following judgment?

: ; let x=3 in x+2 ⇒ 5

(b)  x:3; x⇒3  x:3; 2⇒2  5 is 3+2
     -----------------------------
     •; 3⇒3  x:3; x+2 ⇒ 5
     -----------------------------
     •; let x=3 in x+2 ⇒ 5

(c)  x:2; x⇒3  x:2; 2⇒2  5 is 3+2  ----
     -----------------------------
     •; let x=3 in x+2 ⇒ 5
Adding Conditionals to Micro-OCaml

\[
e ::= x | v | e + e | \text{let } x = e \text{ in } e \\
| \text{eq0 } e | \text{if } e \text{ then } e \text{ else } e
\]

\[
v ::= n | \text{true} | \text{false}
\]

- In terms of interpreter definitions:

```ocaml
type exp =
| Val of value
| ... (* as before *)
| Eq0 of exp
| If of exp * exp * exp
```

```ocaml
type value =
| Int of int
| Bool of bool
```
Rules for Eq0 and Booleans

- Booleans evaluate to themselves
  - \( A; \text{false} \Rightarrow \text{false} \)
- \text{eq0} tests for 0
  - \( A; \text{eq0} 0 \Rightarrow \text{true} \)
  - \( A; \text{eq0} 3+4 \Rightarrow \text{false} \)

\[ \begin{align*}
A; \text{true} & \Rightarrow \text{true} \\
A; \text{false} & \Rightarrow \text{false} \\
A; e & \Rightarrow 0 \\
A; \text{eq0} e & \Rightarrow \text{true} \\
A; e & \Rightarrow v \quad v \neq 0 \\
A; \text{eq0} e & \Rightarrow \text{false}
\end{align*} \]
## Rules for Conditionals

<table>
<thead>
<tr>
<th>A; $e_1 \Rightarrow true$</th>
<th>A; $e_2 \Rightarrow v$</th>
</tr>
</thead>
<tbody>
<tr>
<td>A; if $e_1$ then $e_2$ else $e_3$ $\Rightarrow v$</td>
<td></td>
</tr>
<tr>
<td>A; $e_1 \Rightarrow false$</td>
<td>A; $e_3 \Rightarrow v$</td>
</tr>
<tr>
<td>A; if $e_1$ then $e_2$ else $e_3$ $\Rightarrow v$</td>
<td></td>
</tr>
</tbody>
</table>

- Notice that only one branch is evaluated
  - A; if eq0 0 then 3 else 4 $\Rightarrow 3$
  - A; if eq0 1 then 3 else 4 $\Rightarrow 4$
Quiz 3

What is the derivation of the following judgment?

\[ ; \text{if eq0 3-2 then 5 else 10 } \Rightarrow 10 \]

(a) 
\[ ; 3 \Rightarrow 3 \quad ; 2 \Rightarrow 2 \quad 3-2 \text{ is 1} \]

\[ ; \text{eq0 } 3-2 \Rightarrow \text{false} \quad ; 10 \Rightarrow 10 \]

\[ ; \text{if eq0 3-2 then 5 else 10 } \Rightarrow 10 \]

(b) 
\[ 3 \Rightarrow 3 \quad 2 \Rightarrow 2 \]

\[ 3-2 \text{ is 1} \]

\[ \text{eq0 } 3-2 \Rightarrow \text{false} \quad 10 \Rightarrow 10 \]

\[ ; \text{if eq0 3-2 then 5 else 10 } \Rightarrow 10 \]

(c) 
\[ ; 3 \Rightarrow 3 \]

\[ ; 2 \Rightarrow 2 \]

\[ 3-2 \text{ is 1} \]

\[ ; \text{eq0 } 3-2 \Rightarrow \text{false} \quad ; 10 \Rightarrow 10 \]

\[ ; 3-2 \Rightarrow 1 \quad 1 \neq 0 \]

\[ ; \text{eq0 } 3-2 \Rightarrow \text{false} \quad ; 10 \Rightarrow 10 \]

\[ ; \text{if eq0 3-2 then 5 else 10 } \Rightarrow 10 \]
Quiz 3

What is the derivation of the following judgment?

\[ \text{•; if eq0 3-2 then 5 else 10} \Rightarrow 10 \]

(a)

\[ \text{•; 3} \Rightarrow 3 \quad \text{•; 2} \Rightarrow 2 \quad 3-2 \text{ is 1} \]

\[ \text{•; eq0 3-2} \Rightarrow \text{false} \quad \text{•; 10} \Rightarrow 10 \]

\[ \text{•; if eq0 3-2 then 5 else 10} \Rightarrow 10 \]

(b)

\[ 3 \Rightarrow 3 \quad 2 \Rightarrow 2 \]

\[ 3-2 \text{ is 1} \]

\[ \text{eq0 3-2} \Rightarrow \text{false} \quad 10 \Rightarrow 10 \]

\[ \text{if eq0 3-2 then 5 else 10} \Rightarrow 10 \]

(c)

\[ \text{•; 3} \Rightarrow 3 \]

\[ \text{•; 2} \Rightarrow 2 \]

\[ 3-2 \text{ is 1} \]

\[ \text{•; eq0 3-2} \Rightarrow \text{false} \quad \text{•; 10} \Rightarrow 10 \]

\[ \text{•; if eq0 3-2 then 5 else 10} \Rightarrow 10 \]
let rec eval env e =
  match e with
  | Ident x -> lookup env x
  | Val v -> v
  | Plus (e1,e2) ->
    let Int n1 = eval env e1 in
    let Int n2 = eval env e2 in
    let n3 = n1+n2 in
    Int n3
  | Let (x,e1,e2) ->
    let v1 = eval env e1 in
    let env' = extend env x v1 in
    let v2 = eval env' e2 in v2
  | Eq0 e1 ->
    let Int n = eval env e1 in
    if n=0 then Bool true else Bool false
  | If (e1,e2,e3) ->
    let Bool b = eval env e1 in
    if b then eval env e2
    else eval env e3

Pattern match will fail if \texttt{e1} or \texttt{e2} is not an \texttt{Int}; this is \textit{dynamic} type checking! (But not the best way to do error handling)

Basically both rules for \texttt{Eq0} in this one snippet

Both \texttt{If} rules here
Adding Closures to Micro-OCaml

\[ e ::= x | v | e + e | \text{let } x = e \text{ in } e \\
| \text{eq0 } e | \text{if } e \text{ then } e \text{ else } e \\
| e e | \text{fun } x \rightarrow e \]

\[ v ::= n | \text{true} | \text{false} | (A, \lambda x. e) \]

- In terms of interpreter definitions:

```ocaml
type exp =
  | Val of value
  | If of exp * exp * exp
  ... (* as before *)
  | Call of exp * exp
  | Fun of id * exp

type value =
  Int of int
  | Bool of bool
  | Closure of env * id * exp
```

Environment

Code (id and exp)
Rule for Closures: Lexical/Static Scoping

\[
A; \text{fun } x \rightarrow e \Rightarrow (A, \lambda x. e)
\]

\[
A; e_1 \Rightarrow (A', \lambda x. e) \quad A; e_2 \Rightarrow v_1 \quad A', x: v_1; e \Rightarrow v
\]

\[
A; e_1 \ e_2 \Rightarrow v
\]

- **Notice**
  - Creating a closure captures the current environment \( A \)
  - A call to a function
    - evaluates the body of the closure’s code \( e \) with function closure’s environment \( A' \) extended with parameter \( x \) bound to argument \( v_1 \)

- **Left to you: How will the definitional interpreter change?**
Rule for Closures: Dynamic Scoping

A; \text{fun } x \to e \Rightarrow (\cdot, \lambda x. e)

\begin{align*}
A; e1 \Rightarrow (\cdot, \lambda x. e) & \quad A; e2 \Rightarrow v1 & \quad A, x : v1; e \Rightarrow v \\
\end{align*}

A; e1 \; e2 \Rightarrow v

Notice

- Creating a closure ignores the current environment A
- A call to a function
  - evaluates the body of the closure’s code \( e \) with the current environment A extended with parameter \( x \) bound to argument \( v1 \)

Easy to see dynamic scoping was an implementation error!
Quick Look: Type Checking

- Inference rules can also be used to specify a program’s static semantics
  - i.e., the rules for type checking
- We won’t cover this in depth in this course, but here is a flavor.

- Types \( t ::= \text{bool} \mid \text{int} \)
- Judgment \( \vdash e : t \) says \( e \) has type \( t \)
  - We define inference rules for this judgment, just as with the operational semantics
Some Type Checking Rules

- Boolean constants have type `bool`:
  \[ \vdash \text{true} : \text{bool} \quad \vdash \text{false} : \text{bool} \]

- Equality checking has type `bool` too:
  - Assuming its target expression has type `int`:
    \[ \vdash e : \text{int} \quad \vdash \text{eq}0\ e : \text{bool} \]

- Conditionals:
  \[ \vdash e1 : \text{bool} \quad \vdash e2 : t \quad \vdash e3 : t \]
  \[ \vdash \text{if} \ e1 \ \text{then} \ e2 \ \text{else} \ e3 : t \]
Handling Binding

- What about the types of variables?
  - Taking inspiration from the environment-style operational semantics, what could you do?

- Change judgment to be $G ⊢ e : t$ which says $e$ has type $t$ under type environment $G$
  - $G$ is a map from variables $x$ to types $t$
    - Analogous to map $A$, but maps vars to types, not values

- What would be the rules for `let`, and variables?
Type Checking with Binding

- Variable lookup
  \[ G(x) = t \]
  \[ G \vdash x : t \]

- Let binding
  \[ G \vdash e1 : t1 \quad G, x : t1 \vdash e2 : t2 \]
  \[ G \vdash \text{let } x = e1 \text{ in } e2 : t2 \]

analogous to

\[ A(x) = v \]
\[ A; x \Rightarrow v \]

\[ A; e1 \Rightarrow v1 \quad A, x : v1; e2 \Rightarrow v2 \]
\[ A; \text{let } x = e1 \text{ in } e2 \Rightarrow v2 \]
Scaling up

- Operational semantics (and similarly styled typing rules) can handle full languages
  - With records, recursive variant types, objects, first-class functions, and more

- Provides a concise notation for explaining what a language does. Clearly shows:
  - Evaluation order
  - Call-by-value vs. call-by-name
  - Static scoping vs. dynamic scoping
  - ... We may look at more of these later
Scaling up: Lego City
Scaling up: Web Assembly

WebAssembly Specification

Release 1.1 (Draft, Mar 12, 2021)
Editor: Andreas Rossberg

Latest Draft: https://webassembly.github.io/spec/core/
Issue Tracker: https://github.com/webassembly/spec/issues/

- Introduction
  - Introduction
  - Overview
- Structure
  - Conventions
  - Values
  - Types
  - Instructions
  - Modules
- Validation
  - Conventions
Scaling up: Web Assembly

Formal Notation

Note:
This section gives a brief explanation of the notation for specifying execution formally. For the interested reader, a more thorough introduction can be found in respective text books. [2]

The formal execution rules use a standard approach for specifying operational semantics, rendering them into reduction rules. Every rule has the following general form:

\[
\text{configuration} \rightarrow \text{configuration}
\]

A configuration is a syntactic description of a program state. Each rule specifies one step of execution. As long as there is at most one reduction rule applicable to a given configuration, reduction – and thereby execution – is deterministic. WebAssembly has only very few exceptions to this, which are noted explicitly in this specification.

For WebAssembly, a configuration typically is a tuple \((S; F; \text{instr}^*)\) consisting of the current store \(S\), the call frame \(F\) of the current function, and the sequence of instructions that is to be executed. (A more precise definition is given later.)

To avoid unnecessary clutter, the store \(S\) and the frame \(F\) are omitted from reduction rules that do not touch them.