Call function of two parameters

ApplyUser

$$\frac{\begin{array}{c}\phi(f) = \textsf{USER}(\langle x_1, x_2\rangle, e) \\ x_1, x_2 \text{ distinct} \\ \langle e_1, \xi_0, \phi, \rho_0\rangle \Downarrow \langle v_1, \xi_1, \phi, \rho_1\rangle \\ \langle e_2, \xi_1, \phi, \rho_1\rangle \Downarrow \langle v_2, \xi_2, \phi, \rho_2\rangle \\ \langle e, \xi_2, \phi, \{x_1 \mapsto v_1, x_2 \mapsto v_2\}\rangle \Downarrow \langle v, \xi', \phi, \rho'\rangle\end{array}}{\langle \textsf{APPLY}(f, e_1, e_2), \xi_0, \phi, \rho_0\rangle \Downarrow \langle v, \xi', \phi, \rho_2\rangle}$$

Evaluating function application

The math demands these steps:

- **Find function in ϕ environment**

```
f = fetchfun(e->u.apply.name, functions);
```

- **Using caller's ρ, evaluate actuals**

```
vs = evallist(e->u.apply.actuals,globals,functions,
                                                formals);
```

  N.B. `actuals` **evaluated in current environment**

- **Make a new environment: bind formals to actuals**

```
new_formals = mkValenv(f.u.userdef.formals, vs);
```

- **Evaluate body in new environment**

```
return eval(f.u.userdef.body, globals, functions,
                                        new_formals);
```

Call function of two parameters

ApplyUser

$$\frac{\begin{array}{c}\phi(f) = \textsf{USER}(\langle x_1, x_2\rangle, e) \\ x_1, x_2 \text{ distinct} \\ \langle e_1, \xi_0, \phi, \rho_0\rangle \Downarrow \langle v_1, \xi_1, \phi, \rho_1\rangle \\ \langle e_2, \xi_1, \phi, \rho_1\rangle \Downarrow \langle v_2, \xi_2, \phi, \rho_2\rangle \\ \langle e, \xi_2, \phi, \{x_1 \mapsto v_1, x_2 \mapsto v_2\}\rangle \Downarrow \langle v, \xi', \phi, \rho'\rangle\end{array}}{\langle \textsf{APPLY}(f, e_1, e_2), \xi_0, \phi, \rho_0\rangle \Downarrow \langle v, \xi', \phi, \rho_2\rangle}$$

Judgment speaks truth when "derivable"

Special kind of proof: derivation

- It's a data structure (derivation tree)
- Made inductively, by composing rules
- Valid derivation matches rules (by substitution)
- Spacelike representation of timelike behavior (think flip-book animation)

A form of "syntactic proof"

Valid derivation

Initial state partially or fully known

Final state determined by initial state (homework)

Every node in tree is an instance of some rule

No primes!

- Substitute known subexpressions for $e_1, \ldots$
- Substitute known results for ξ', ρ'

Recursive evaluator travels inductive proof

Root of derivation at the bottom (surprise!)

Build

- Start on the left, go up
- Cross the $\Downarrow$
- Finish on the right, go down

The "Tony Hawk" algorithm

First let's see a movie

Evaluating $(10+1) \times (10-1)$

$\langle$ `(* (+ 10 1) (- 10 1))` $, \xi, \phi, \rho \rangle \Downarrow$

Evaluating $(10+1) \times (10-1)$

$$\frac{\langle \texttt{(+ 10 1)}, \xi, \phi, \rho \rangle \Downarrow}{\langle \texttt{(* (+ 10 1) (- 10 1))}, \xi, \phi, \rho \rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{}{\langle \texttt{10}, \ldots \rangle \Downarrow} \qquad \dfrac{}{\langle \texttt{(+ 10 1)}, \xi, \phi, \rho \rangle \Downarrow}}{\langle \texttt{(* (+ 10 1) (- 10 1))}, \xi, \phi, \rho \rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10}, \ldots\rangle \Downarrow \langle \texttt{10}, \ldots\rangle}}{\langle \texttt{(+ 10 1)}, \xi, \phi, \rho\rangle \Downarrow}}{\langle \texttt{(* (+ 10 1) (- 10 1))}, \xi, \phi, \rho\rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10}, \ldots\rangle \Downarrow \langle \texttt{10}, \ldots\rangle} \qquad \dfrac{}{\langle \texttt{1}, \ldots\rangle \Downarrow}}{\langle \texttt{(+ 10 1)}, \xi, \phi, \rho\rangle \Downarrow}}{\langle \texttt{(* (+ 10 1) (- 10 1))}, \xi, \phi, \rho\rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{}{\langle \texttt{10}, \ldots\rangle \Downarrow \langle \texttt{10}, \ldots\rangle} \qquad \dfrac{}{\langle \texttt{1}, \ldots\rangle \Downarrow \langle \texttt{1}, \ldots\rangle}}{\langle \texttt{(+ 10 1)}, \xi, \phi, \rho\rangle \Downarrow} \qquad \langle \texttt{(* (+ 10 1) (- 10 1))}, \xi, \phi, \rho\rangle \Downarrow$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \textbf{10},\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle \textbf{1},\ldots\rangle}}{\langle \texttt{(+ 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle \textbf{11},\xi,\phi,\rho\rangle}}{\langle \texttt{(* (+ 10 1) (- 10 1))},\xi,\phi,\rho\rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \mathbf{10},\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle \mathbf{1},\ldots\rangle}}{\langle \texttt{(+ 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle \mathbf{11},\xi,\phi,\rho\rangle} \quad \dfrac{}{\langle \texttt{(- 10 1)},\xi,\phi,\rho\rangle \Downarrow}}{\langle \texttt{(* (+ 10 1) (- 10 1))},\xi,\phi,\rho\rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \textbf{10},\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle \textbf{1},\ldots\rangle} \quad \dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow}}{\dfrac{\langle \texttt{(+ 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle \textbf{11},\xi,\phi,\rho\rangle \qquad \langle \texttt{(- 10 1)},\xi,\phi,\rho\rangle \Downarrow}{\langle \texttt{(* (+ 10 1) (- 10 1))},\xi,\phi,\rho\rangle \Downarrow}}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \textbf{10},\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle \textbf{1},\ldots\rangle}}{\langle \texttt{(+ 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle \textbf{11},\xi,\phi,\rho\rangle} \quad \dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \textbf{10},\ldots\rangle}}{\langle \texttt{(- 10 1)},\xi,\phi,\rho\rangle \Downarrow}}{\langle \texttt{(* (+ 10 1) (- 10 1))},\xi,\phi,\rho\rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \texttt{10},\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle \texttt{1},\ldots\rangle}}{\langle \texttt{(+ 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle \texttt{11},\xi,\phi,\rho\rangle} \quad \dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \texttt{10},\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow}}{\langle \texttt{(- 10 1)},\xi,\phi,\rho\rangle \Downarrow}}{\langle \texttt{(* (+ 10 1) (- 10 1))},\xi,\phi,\rho\rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle 10,\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle 1,\ldots\rangle}}{\langle \texttt{(+ 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle 11,\xi,\phi,\rho\rangle} \quad \dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle 10,\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle 1,\ldots\rangle}}{\langle \texttt{(- 10 1)},\xi,\phi,\rho\rangle \Downarrow}}{\langle \texttt{(* (+ 10 1) (- 10 1))},\xi,\phi,\rho\rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \textcolor{red}{10},\ldots\rangle}\quad\dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle \textcolor{red}{1},\ldots\rangle}}{\langle \texttt{(+ 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle \textcolor{red}{11},\xi,\phi,\rho\rangle}\quad\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle \textcolor{red}{10},\ldots\rangle}\quad\dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle \textcolor{red}{1},\ldots\rangle}}{\langle \texttt{(- 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle \textcolor{red}{9},\xi,\phi,\rho\rangle}}{\langle \texttt{(* (+ 10 1) (- 10 1))},\xi,\phi,\rho\rangle \Downarrow}$$

Evaluating $(10+1)\times(10-1)$

$$\dfrac{\dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle 10,\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle 1,\ldots\rangle}}{\langle \texttt{(+ 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle 11,\xi,\phi,\rho\rangle} \quad \dfrac{\dfrac{}{\langle \texttt{10},\ldots\rangle \Downarrow \langle 10,\ldots\rangle} \quad \dfrac{}{\langle \texttt{1},\ldots\rangle \Downarrow \langle 1,\ldots\rangle}}{\langle \texttt{(- 10 1)},\xi,\phi,\rho\rangle \Downarrow \langle 9,\xi,\phi,\rho\rangle}}{\langle \texttt{(* (+ 10 1) (- 10 1))},\xi,\phi,\rho\rangle \Downarrow \langle 99,\xi,\phi,\rho\rangle}$$

Algorithm for building derivations

Want to solve

$$\langle e, \xi, \phi, \rho \rangle \Downarrow ?$$

What rule can I use to prove it?

1. **Syntactic form of e narrows to a few choices (usually 1 or 2)**
2. **Look for form in conclusion**
3. **Now check premises**
4. **When premise is evaluation judgment, build sub-derivation recursively**

Derivation is written $\mathcal{D}$

Syntactic proofs empower meta reasoning

Proof $\mathcal{D}$ is a data structure

Got a fact about all proofs?

- It's a fact about all terminating evaluations
- They are 1 to 1

Prove facts by structural induction over derivations

- (Or "induction on height of derivation tree")

Example: evaluating an expression doesn't create or destroy any global variables (the set of *defined* global variables is invariant)

Metatheorems often help implementors

More example metatheorems:

- **OK to mutate environments if you use a stack**
- **Interactive browser doesn't leak space (POPL 2012)**
- **Device driver can't harm kernel (Microsoft Singularity)**

Metatheorems come in stylized form

For any e, ξ, ϕ, ρ, v, ξ', and ρ' such that

$$\langle e, \xi, \phi, \rho \rangle \Downarrow \langle v, \xi', \phi, \rho' \rangle,$$

FACT

Exercise (30 seconds): how to say "evaluation doesn't change the set of *defined* global variables"? (Values may change, but no variable is created or destroyed.)

Metatheorems are proved by induction

Induction over structure (or height) of derivation trees $\mathcal{D}$

These are "math-class proofs" (*not* derivations)

Proof

- **Has one case for each rule**
- **Has multiple cases for some syntactic forms**
- **Assumes the induction hypothesis for any proper sub-derivation (derivation of a premise)**

Let's try it!

Assume the existence of a derivation

Could terminate in any rule!

Base case:

$$\mathcal{D}= \frac{}{\langle \textsc{literal}(v), \xi, \phi, \rho \rangle \Downarrow \langle v, \xi, \phi, \rho \rangle}$$

Both sides identical!

$$\mathrm{dom}\,\xi = \mathrm{dom}\,\xi$$

Holds for formal-parameter lookup

Another base case:

$$\mathcal{D}_{=} \quad \frac{x \in \operatorname{dom} \rho}{\langle \mathsf{VAR}(x), \xi, \phi, \rho \rangle \Downarrow \langle \rho(x), \xi, \phi, \rho \rangle}$$

Both sides identical!

$$\operatorname{dom} \xi = \operatorname{dom} \xi$$

Inductive case: good sub-derivation

Assignment to formal parameter

$$\mathcal{D}_{=} \quad \frac{x \in \operatorname{dom}\rho \qquad \dfrac{\mathcal{D}_r}{\langle e, \xi, \phi, \rho\rangle \Downarrow \langle v, \xi', \phi, \rho'\rangle}}{\langle \mathsf{SET}(x, e), \xi, \phi, \rho\rangle \Downarrow \langle v, \xi', \phi, \rho'\{x \mapsto v\}\rangle}$$

By induction hypothesis on $\mathcal{D}_r$, $\operatorname{dom}\xi = \operatorname{dom}\xi'$

Both sides have same domain!

Inductive case: good sub-derivation

True conditional

$$\mathcal{D} = \dfrac{\dfrac{\mathcal{D}_1}{\langle e_1, \xi, \phi, \rho\rangle \Downarrow \langle v_1, \xi', \phi, \rho'\rangle} \quad v_1 \neq 0 \quad \dfrac{\mathcal{D}_2}{\langle e_2, \xi', \phi, \rho'\rangle \Downarrow \langle v_2, \xi'', \phi, \rho''\rangle}}{\langle \mathsf{IF}(e_1, e_2, e_3), \xi, \phi, \rho\rangle \Downarrow \langle v_2, \xi'', \phi, \rho''\rangle}$$

By induction hypothesis on $\mathcal{D}_1$, $\operatorname{dom}\xi = \operatorname{dom}\xi'$

By induction hypothesis on $\mathcal{D}_2$, $\operatorname{dom}\xi' = \operatorname{dom}\xi''$

Therefore, both sides have same domain:

$\operatorname{dom}\xi = \operatorname{dom}\xi''$

The only interesting case: assign to global

$$\frac{x \notin \mathrm{dom}\,\rho \qquad x \in \mathrm{dom}\,\xi \qquad \dfrac{\mathcal{D}_r}{\langle e, \xi, \phi, \rho\rangle \Downarrow \langle v, \xi', \phi, \rho'\rangle}}{\langle \textsf{SET}(x, e), \xi, \phi, \rho\rangle \Downarrow \langle v, \xi'\{x \mapsto v\}, \phi, \rho'\rangle}$$

Do both sides have same domain?

- **Does** $\mathrm{dom}\,\xi = \mathrm{dom}(\xi'\{x \mapsto v\})$ **?**

By induction hypothesis on $\mathcal{D}_r$**,** $\mathrm{dom}\,\xi = \mathrm{dom}\,\xi'$

And $\mathrm{dom}(\xi'\{x \mapsto v\}) = \mathrm{dom}\,\xi' \cup \{x\} = \mathrm{dom}\,\xi \cup \{x\}$

But $x \in \mathrm{dom}\,\xi$**! So** $\mathrm{dom}\,\xi \cup \{x\} = \mathrm{dom}\,\xi$