CSC 520, Spring 2020

Principles of Programming Languages

Michelle Strout

THE UNIVERSITY OF ARIZONA

Today's Plan

THE UNIVERSITY OF ARIZONA
Computer Science

- **Do an example derivation in Impcore operational semantics**
- **Metatheory enables us to prove things about ALL programs in a language**
- **Induction on derivations**
- **Last time**
  - Operational semantics for Impcore constructs
  - A valid derivation defines the execution of a single program.

For reference: AST definition for Impcore

- The abstract-syntax tree (AST)

```
exp = LITERAL (Value)
    | VAR (Name)
    | SET (Name name, Exp exp)
    | IFX (Exp cond, Exp true, Exp false)
    | WHILEX (Exp cond, Exp exp)
    | BEGIN (Explist)
    | APPLY (Name name, Explist actuals)
```

- One kind of "application" for both user-defined and primitive functions.

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 $\mathcal{D}$

Exercise: Evaluate `(digit? 7)`

$$\vdots$$

$$\overline{\langle \texttt{(and (<= 0 n) (< n 10))}, \xi, \phi, \{\texttt{n} \mapsto 7\} \rangle \Downarrow ?}$$

Proofs about all derivations: Metatheory

- **Derivations (aka syntactic proofs) enable meta-reasoning**
  - Derivation D is a data structure
  - Got a fact about all derivations?
    - It's a fact about all terminating evaluations
    - They are in 1 to 1 correspondence
  - Prove facts by structural induction over derivations
  - Example: Evaluation an expression doesn't change the set of global variables

- **Metatheorems often help implementors**
  - 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 global variables"?

Metatheorems are proved by induction

- **Induction over structure (or height) of derivation trees**
  - 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)

Evaluation does not add or remove a global variable

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

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

we can prove

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

"Evaluation doesn't change the global domain"

Assume the existence of a derivation

Could terminate in any rule!

Base case:

$$\frac{}{\langle \mathsf{LITERAL}(v), \xi, \phi, \rho \rangle \Downarrow \langle v, \xi, \phi, \rho \rangle}$$

Both sides identical!

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

Holds for formal-parameter lookup

Another base case:

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

Both sides identical!

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

Inductive case: good sub-derivation

Assignment to formal parameter

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

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

Both sides have same domain!

Inductive case: good sub-derivation

True conditional

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

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

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

Do both sides have same domain?

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

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

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

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

Practice writing operational semantics

- **Impcore can be extended with new syntactic forms for short-circuit conditionals**
  - To evaluate expression (&& e_1 e_2), first evaluate e_1.
  - If the result of evaluatione e_1 is nonzero, evaluate e_2, and the result of evaluation e_2 is the result of evaluating the entire && expression.
  - If the result of evaluation e_1 is zero, then e_2 is not evaluated, and the result of evaluating the entire && expression is zero.
- **➔ Write as many inference rules as needed to specify the behavior of short-circuit &&**
- **➔ Piazza: write inference rules for short-circuit ||**

Metatheory exercise from book

- **15. Use the operational semantics to show that there exist environments xi, phi, rho, xi', and rho' and a value v1 such that**

$\langle \text{if(var(x),var(x),literal(0))}, \xi, \phi, \rho \rangle \Downarrow \langle \text{v1}, \xi', \phi, \rho' \rangle$

if and only if there exist environments ξ, φ, ρ, ξ'', and ρ'' and a value v2 such that

$\langle \text{var(x)}, \xi, \phi, \rho \rangle \Downarrow \langle \text{v2}, \xi'', \phi, \rho'' \rangle$.

- **Give necessary and sufficient conditions on the environments xi, phi, and rho such that both expressions evaluate successfully**

Metatheory exercise from book

- **16. Prove that the value of a while expression is always zero.**
  - That is, given any xi, phi, rho, e1, and e2, prove that if there exist a xi', rho', and v such that there is a derivation of

$$\langle \mathrm{while}(e1, e2), \xi, \phi, \rho \rangle \Downarrow \langle v, \xi', \phi, \rho' \rangle,$$

  - Then v=0.
- **Use structural induction on the derivation.**