

Type Systems

Lecture 3: Consistency and Termination

Neel Krishnaswami
University of Cambridge

From Type Safety to Stronger Properties

- In the last lecture, we saw how evaluation corresponded to proof normalization
- This was an act of knowledge transfer from computation to logic
- Are there any transfers we can make in the other direction?

Logical Consistency

- An important property of any logic is consistency: there are no proofs of \perp !
- Otherwise, the \perp E rule will let us prove anything.
- What does this look like in a programming language?

Types and Values

Types $X ::= 1 \mid X \times Y \mid 0 \mid X + Y \mid X \rightarrow Y$

Values $v ::= \langle \rangle \mid \langle v, v' \rangle \mid \lambda x : A. e \mid Lv \mid Rv$

- There are no values of type 0
- I.e., no normal forms of type 0
- But what about non-normal forms?

What Type Safety Does, and Doesn't Show

- We have proved type safety:
 - Progress: If $\cdot \vdash e : X$ then e is a value or $e \rightsquigarrow e'$.
 - Type preservation If $\cdot \vdash e : X$ and $e \rightsquigarrow e'$ then $\cdot \vdash e' : X$.
- If there were a closed term of type 0, then progress means it must always step (since there are no values of type 0)
- But the term it would step to also has type 0 (by preservation)
- So any closed term of type 0 must loop – it must step forever.

A Naive Proof that Does Not Work

Theorem: If $\cdot \vdash e : X$ then there is a value v such that $e \rightsquigarrow^* v$.

“Proof”: By structural induction on $\cdot \vdash e : X$

$$\frac{\overbrace{\Gamma \vdash e : X \rightarrow Y}^{(2)} \quad \overbrace{\Gamma \vdash e' : X}^{(3)}}{\Gamma \vdash e e' : Y}$$

(1) $\Gamma \vdash e e' : Y$

Assumption

(4) $e \rightsquigarrow^* v$

Induction on (2)

(5) $e' \rightsquigarrow^* v'$

Induction on (3)

(6) $\cdot \vdash v : X \rightarrow Y$

Preservation on (2), (4)

(7) $\cdot \vdash v' : X$

Preservation on (3), (5)

(8) $\cdot \vdash v \equiv \lambda x : X. e'' : X \rightarrow Y$

Canonical forms on (6)

(9) $x : X \vdash e'' : Y$

Subderivation

(10) $\cdot \vdash \underbrace{[v'/x]e''}_{\text{Can't do induction on this!}} : Y$

Substitution

Can't do induction on this!

A Minimal Typed Lambda Calculus

Types $X ::= 1 \mid X \rightarrow Y \mid 0$

Terms $e ::= x \mid \langle \rangle \mid \lambda x : X. e \mid e e' \mid \text{abort } e$

Values $v ::= \langle \rangle \mid \lambda x : X. e$

$$\frac{X : X \in \Gamma}{\Gamma \vdash x : X} \text{HYP}$$

$$\frac{}{\Gamma \vdash \langle \rangle : 1} \text{1I}$$

$$\frac{\Gamma, X \vdash e : Y}{\Gamma \vdash \lambda x : X. e : X \rightarrow Y} \rightarrow\text{I}$$

$$\frac{\Gamma \vdash e : X \rightarrow Y \quad \Gamma \vdash e' : X}{\Gamma \vdash e e' : Y} \rightarrow\text{E}$$

$$\frac{\Gamma \vdash e : 0}{\Gamma \vdash \text{abort } e : Z} \text{OE}$$

Reductions

$$\frac{e \rightsquigarrow e'}{\text{abort } e \rightsquigarrow \text{abort } e'}$$

$$\frac{e_1 \rightsquigarrow e'_1}{e_1 e_2 \rightsquigarrow e'_1 e_2}$$

$$\frac{e_2 \rightsquigarrow e'_2}{v_1 e_2 \rightsquigarrow v_1 e'_2}$$

$$\frac{}{(\lambda x : X. e) v \rightsquigarrow [v/x]e}$$

Theorem (Determinacy): If $e \rightsquigarrow e'$ and $e \rightsquigarrow e''$ then $e' = e''$

Proof: By structural induction on $e \rightsquigarrow e'$

Why Can't We Prove Termination

- We can't prove termination by structural induction
- Problem is that knowing a term evaluates to a function doesn't tell us that applying the function terminates
- We need to assume something stronger

A Logical Relation

1. We say that e halts if and only if there is a v such that $e \rightsquigarrow^* v$.
2. Now, we will define a type-indexed family of set of terms:
 - $\text{Halt}_0 = \emptyset$ (i.e, for all e , $e \notin \text{Halt}_0$)
 - $e \in \text{Halt}_1$ holds just when e halts.
 - $e \in \text{Halt}_{X \rightarrow Y}$ holds just when
 1. e halts
 2. For all e' , if $e' \in \text{Halt}_X$ then $(e e') \in \text{Halt}_Y$.
3. Hereditary definition:
 - Halt_1 halts
 - $\text{Halt}_{1 \rightarrow 1}$ preserves the property of halting
 - $\text{Halt}_{(1 \rightarrow 1) \rightarrow (1 \rightarrow 1)}$ preserves the property of preserving the property of halting...

Closure Lemma, 1/5

Lemma: If $e \rightsquigarrow e'$ then $e' \in \text{Halt}_X$ iff $e \in \text{Halt}_X$.

Proof: By induction on X :

• Case $X = 1, \Rightarrow$:

- (1) $e \rightsquigarrow e'$ Assumption
- (2) $e' \in \text{Halt}_1$ Assumption
- (3) $e' \rightsquigarrow^* v$ Definition of Halt_1
- (4) $e \rightsquigarrow^* v$ Def. of transitive closure, (1) and (3)
- (5) $e \in \text{Halt}_1$ Definition of Halt_1

- Case $X = 1$, \Leftarrow :
 - (1) $e \rightsquigarrow e'$ Assumption
 - (2) $e \in \text{Halt}_1$ Assumption
 - (3) $e \rightsquigarrow^* v$ Definition of Halt_1
 - (4) e is not a value: Since $e \rightsquigarrow e'$
 - (5) $e \rightsquigarrow e''$ and $e'' \rightsquigarrow^* v$ Definition of $e \rightsquigarrow^* v$
 - (6) $e'' = e'$ By determinacy on (1), (5)
 - (7) $e' \rightsquigarrow^* v$ By equality (6) on (5)
 - (8) $e' \in \text{Halt}_1$ Definition of Halt_1

Closure Lemma, 3/5

• Case $X = Y \rightarrow Z, \Rightarrow$:

- | | | |
|-----|---|--|
| (1) | $e \sim e'$ | Assumption |
| (2) | $e' \in \text{Halt}_{Y \rightarrow Z}$ | Assumption |
| (3) | $e' \sim^* v$ | Def. of $\text{Halt}_{Y \rightarrow Z}$ |
| (4) | $\forall t \in \text{Halt}_Y, e' t \in \text{Halt}_Z$ | " |
| (5) | $e \sim^* v$ | Transitive closure, (1) and (3) |
| | Assume $t \in \text{Halt}_Y$: | |
| (6) | $e t \sim e' t$ | By congruence rule on (1) |
| (7) | $e' t \in \text{Halt}_Z$ | By (4) |
| | $e t \in \text{Halt}_Z$ | By induction on (6), (7) |
| (8) | $\forall t \in \text{Halt}_Y, e t \in \text{Halt}_Z$ | |
| (9) | $e \in \text{Halt}_{Y \rightarrow Z}$ | Def of $\text{Halt}_{Y \rightarrow Z}$ on (5), (8) |

Closure Lemma, 4/5

- Case $X = Y \rightarrow Z$, \Leftarrow :
 - (1) $e \rightsquigarrow e'$ Assumption
 - (2) $e \in \text{Halt}_{Y \rightarrow Z}$ Assumption
 - (3) $e \rightsquigarrow^* v$ Def. of $\text{Halt}_{Y \rightarrow Z}$
 - (4) $\forall t \in \text{Halt}_Y, e t \in \text{Halt}_Z$ "
 e is not a value Since (1)
 - (5) $e \rightsquigarrow e''$ and $e'' \rightsquigarrow^* v$ Definition of $e \rightsquigarrow^* v$
 - (6) $e'' = e'$ By determinacy on (1), (5)
Assume $t \in \text{Halt}_Y$:
 - (7) $e t \rightsquigarrow e' t$ By congruence rule on (1)
 - (8) $e t \in \text{Halt}_Z$ By (4)
 $e' t \in \text{Halt}_Z$ By induction on (6), (7)
 - (9) $\forall t \in \text{Halt}_Y, e' t \in \text{Halt}_Z$
 - (10) $e' \in \text{Halt}_{Y \rightarrow Z}$ Def of $\text{Halt}_{Y \rightarrow Z}$ on (5), (8)

Closure Lemma, 5/5

- Case $X = 0, \Rightarrow$:
 - (1) $e \rightsquigarrow e'$ Assumption
 - (2) $e' \in \text{Halt}_0$ Assumption
 - (3) $e' \in \emptyset$ Definition of Halt_0
 - (4) Contradiction!

- Case $X = 0, \Leftarrow$:
 - (1) $e \rightsquigarrow e'$ Assumption
 - (2) $e \in \text{Halt}_0$ Assumption
 - (3) $e \in \emptyset$ Definition of Halt_0
 - (4) Contradiction!

The Fundamental Lemma

Lemma:

If we have that:

- $x_1 : X_1, \dots, x_n : X_n \vdash e : Z$, and
- for $i \in \{1 \dots n\}$, $\cdot \vdash v_i : X_i$ and $v_i \in \text{Halt}_{X_i}$

then $[v_1/x_1, \dots, v_n/x_n]e \in \text{Halt}_Z$

Proof:

By structural induction on $x_1 : X_1, \dots, x_n : X_n \vdash e : Z$!

The Fundamental Lemma, 1/5

- Case Hyp:

- | | | |
|-----|--|----------------------|
| | $\frac{x_j : X_j \in \overrightarrow{x_i : X_i}}{x_i : X_i \vdash x_j : X_j} \text{HYP}$ | |
| (1) | $\overrightarrow{x_i : X_i} \vdash x_j : X_j$ | Assumption |
| (2) | $\overrightarrow{[v_i/x_i]}x_j = v_j$ | Def. of substitution |
| (3) | $v_j \in \text{Halt}_{X_j}$ | Assumption |
| (4) | $\overrightarrow{[v_i/x_i]}x_j \in \text{Halt}_{X_j}$ | Equality (2) on (3) |

The Fundamental Lemma, 2/5

- Case 1l:

- (1) $\overline{x_i : X_i \vdash \langle \rangle : 1}$ ^{1l} Assumption
- (2) $\overrightarrow{[v_i/x_i]} \langle \rangle = \langle \rangle$ Def. of substitution
- (3) $\langle \rangle \rightsquigarrow^* \langle \rangle$ Def. of transitive closure
- (4) $\langle \rangle \in \text{Halt}_1$ Def. of Halt_1
- (5) $\overrightarrow{[v_i/x_i]} \langle \rangle \in \text{Halt}_1$ Equality (2) on (4)

- Case \rightarrow I:

$$\begin{array}{ll}
 (1) & \frac{\overrightarrow{x_i : X_i}, y : Y \vdash e : Z}{\overrightarrow{x_i : X_i} \vdash \lambda y : Y. e : Y \rightarrow Z} \rightarrow\text{I} & \text{Assumption} \\
 (2) & \overrightarrow{x_i : X_i}, y : Y \vdash e : Z & \text{Subderivation of (1)} \\
 (3) & \overrightarrow{[v_i/x_i]}(\lambda y : Y. e) = \lambda y : Y. \overrightarrow{[v_i/x_i]}e & \text{Def of substitution} \\
 (4) & \lambda y : Y. \overrightarrow{[v_i/x_i]}e \sim^* \lambda y : Y. \overrightarrow{[v_i/x_i]}e & \text{Def of closure}
 \end{array}$$

The Fundamental Lemma, 3b/5

Case \rightarrow l:

(5) Assume $t \in \text{Halt}_Y$:

(6) $t \rightsquigarrow^* v_y$ Def of Halt_Y

(7) $v_y \in \text{Halt}_Y$ Closure on (6)

(8) $(\lambda y : Y. \overrightarrow{[v_i/x_i]e}) v_y \rightsquigarrow \overrightarrow{[v_i/x_i, v_y/y]e}$ Rule

(9) $\overrightarrow{[v_i/x_i, v_y/y]e} \in \text{Halt}_Z$ Induction

(10) $(\lambda y : Y. \overrightarrow{[v_i/x_i]e}) t \rightsquigarrow (\lambda y : Y. \overrightarrow{[v_i/x_i]e}) v_y$ Congruence

(11) $(\lambda y : Y. \overrightarrow{[v_i/x_i]e}) t \in \text{Halt}_Z$ Closure

(12) $\forall t \in \text{Halt}_Y, (\lambda y : Y. \overrightarrow{[v_i/x_i]e}) t \in \text{Halt}_Z$

Case \rightarrow l:

$$(4) \quad \lambda y : Y. \overrightarrow{[v_i/x_i]}e \rightsquigarrow^* \lambda y : Y. \overrightarrow{[v_i/x_i]}e \quad \text{Def of closure}$$

$$(12) \quad \forall t \in \text{Halt}_Y, (\lambda y : Y. \overrightarrow{[v_i/x_i]}e) t \in \text{Halt}_Z$$

$$(13) \quad (\lambda y : Y. \overrightarrow{[v_i/x_i]}e) \in \text{Halt}_{Y \rightarrow Z} \quad \text{Def. of Halt}_{Y \rightarrow Z}$$

The Fundamental Lemma, 4/5

- Case \rightarrow E:

	$\frac{\overrightarrow{x_i : X_i} \vdash e : Y \rightarrow Z \quad \overrightarrow{x_i : X_i} \vdash e' : Y}{\overrightarrow{x_i : X_i} \vdash e e' : Z} \rightarrow E$	
(1)		Assumption
(2)	$\overrightarrow{x_i : X_i} \vdash e : Y \rightarrow Z$	Subderivation
(3)	$\overrightarrow{x_i : X_i} \vdash e' : Y$	Subderivation
(4)	$[v_i/x_i]e \in \text{Halt}_{Y \rightarrow Z}$	Induction
(5)	$\forall t \in \text{Halt}_Y, [v_i/x_i]e t \in \text{Halt}_Z$	Def of $\text{Halt}_{Y \rightarrow Z}$
(6)	$[v_i/x_i]e' \in \text{Halt}_Y$	Induction
(7)	$([v_i/x_i]e) ([v_i/x_i]e') \in \text{Halt}_Z$	Instantiate (5) w/ (6)
(8)	$[v_i/x_i](e e') \in \text{Halt}_Z$	Def. of substitution

The Fundamental Lemma, 5/5

- Case 0E:

- | | | |
|-----|---|------------------------|
| (1) | $\frac{\overrightarrow{x_i : X_i} \vdash e : 0}{\overrightarrow{x_i : X_i} \vdash \text{abort } e : Z}$ | 0E
Assumption |
| (2) | $\overrightarrow{x_i : X_i} \vdash e : 0$ | Subderivation |
| (3) | $\overrightarrow{[v_i/x_i]} e \in \text{Halt}_0$ | Induction |
| (4) | $\overrightarrow{[v_i/x_i]} e \in \emptyset$ | Def of Halt_0 |
| (5) | Contradiction! | |

Theorem: There are no terms $\cdot \vdash e : 0$.

Proof:

- (1) $\cdot \vdash e : 0$ Assumption
- (2) $e \in \text{Halt}_0$ Fundamental lemma
- (3) $e \in \emptyset$ Definition of Halt_0
- (4) Contradiction!

Conclusions

- Consistency and termination are very closely linked
- We have proved that the simply-typed lambda calculus is a total programming language
- Since every closed program reduces to a value, and there are no values of empty type, there are no programs of empty type
- We seem to have circumvented the Halting Theorem?
- No: we do not accept all terminating programs!

1. Extend the logical relation to support products
2. (Harder) Extend the logical relation to support sum types