$e ::= \text{true} \mid \text{false} \mid \text{if } e_1 \text{ then } e_2 \text{ else } e_3 \mid 0 \mid \text{succ } e \mid \text{pred } e \mid \text{iszero } e$

Values

$v ::= \text{true} \mid \text{false} \mid 0 \mid \text{succ } v$

$$\frac{}{\text{bvalue true}} \qquad \frac{}{\text{bvalue false}} \qquad \frac{}{\text{nvalue } 0} \qquad \frac{\text{nvalue } e}{\text{nvalue (succ } e)}$$

$\text{value } e := \text{bvalue } e \vee \text{nvalue } e$

Small-step Operational Semantics

$$\frac{}{\text{if true then } e_1 \text{ else } e_2 \mapsto e_1} \qquad \frac{}{\text{if false then } e_1 \text{ else } e_2 \mapsto e_2}$$

$$\frac{e_1 \mapsto e_1'}{\text{if } e_1 \text{ then } e_2 \text{ else } e_3 \mapsto \text{if } e_1' \text{ then } e_2 \text{ else } e_3} \qquad \frac{e_1 \mapsto e_1'}{\text{succ } e_1 \mapsto \text{succ } e_1'}$$

$$\frac{}{\text{pred } 0 \mapsto 0} \qquad \frac{\text{nvalue } v_1}{\text{pred (succ } v_1) \mapsto v_1} \qquad \frac{e_1 \mapsto e_1'}{\text{pred } e_1 \mapsto \text{pred } e_1'}$$

$$\frac{}{\text{iszero } 0 \mapsto \text{true}} \qquad \frac{\text{nvalue } v_1}{\text{iszero (succ } v_1) \mapsto \text{false}} \qquad \frac{e_1 \mapsto e_1'}{\text{iszero } e_1 \mapsto \text{iszero } e_1'}$$

$\text{normalform } e := \neg \exists e'. \; e \mapsto e'$

$\text{stuck } e := \text{normalform } e \wedge \neg \text{value } e$

Theorem value_is_nf: $\forall e. \; \text{value } e \to \text{normalform } e.$

Multistep

$$\frac{}{e \mapsto^* e} \qquad \frac{e_1 \mapsto e_2 \quad e_2 \mapsto^* e_3}{e_1 \mapsto^* e_3}$$

Safety

$\text{safe } e := \forall e'. \; e \mapsto^* e' \to \neg \text{stuck } e'$

TYPES

$\tau ::= \text{Bool} \mid \text{Nat}$

TYPING RULES

$$\overline{\vdash \text{true} : \text{Bool}} \qquad \overline{\vdash \text{false} : \text{Bool}} \qquad \frac{\vdash e_1 : \text{Bool} \quad \vdash e_2 : \tau \quad \vdash e_3 : \tau}{\vdash \text{if } e_1 \text{ then } e_2 \text{ else } e_3 : \tau}$$

$$\overline{\vdash 0 : \text{Nat}} \qquad \frac{\vdash e : \text{Nat}}{\vdash \text{succ } e : \text{Nat}} \qquad \frac{\vdash e : \text{Nat}}{\vdash \text{pred } e : \text{Nat}} \qquad \frac{\vdash e : \text{Nat}}{\vdash \text{iszero } e : \text{Bool}}$$

TYPE SOUNDNESS

Theorem: $\vdash e : \tau \longrightarrow \text{Safe } e \wedge \forall v.\ e \longmapsto^* v \to \vdash v : \tau$

CANONICAL FORMS

Lemma (canonical forms)

$\vdash e : \text{Bool} \longrightarrow \text{value } e \longrightarrow \text{bvalue } e$

$\vdash e : \text{Nat} \longrightarrow \text{value } e \longrightarrow \text{nvalue } e$

PROGRESS

Lemma: $\vdash e : \tau \longrightarrow \text{value } e \vee \exists e'.\ e \longmapsto e'$

PRESERVATION

Lemma: $\vdash e : \tau \longrightarrow e \longmapsto e' \longrightarrow \vdash e' : \tau$

Corollary: type soundness