TYPE SAFETY

preservation: if $e \to e'$ and

$$\vdash_{\omega} e \ \tau \text{, then}$$

$$\vdash_{\omega} e' \ \tau$$

progress: if $\vdash_{\omega} e \ \tau$, then

(a) either e VAL, or

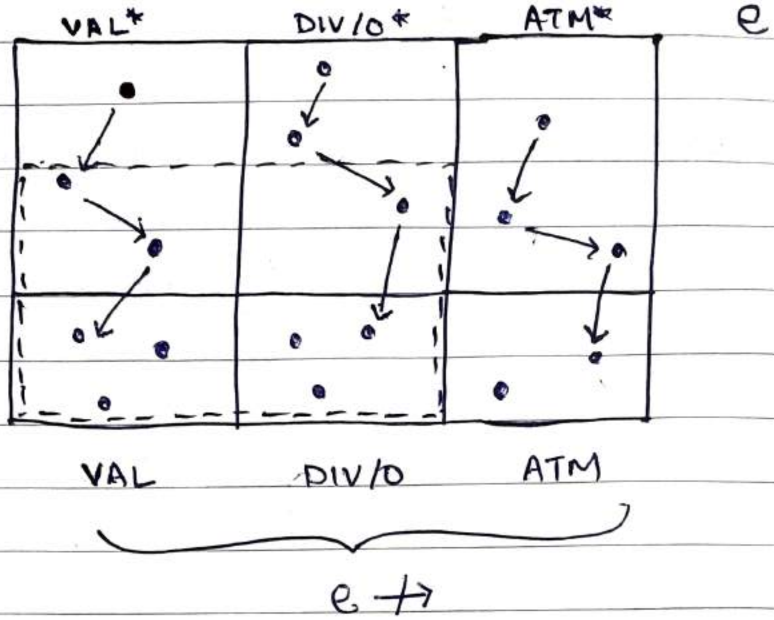
(b) e DIV/0, or

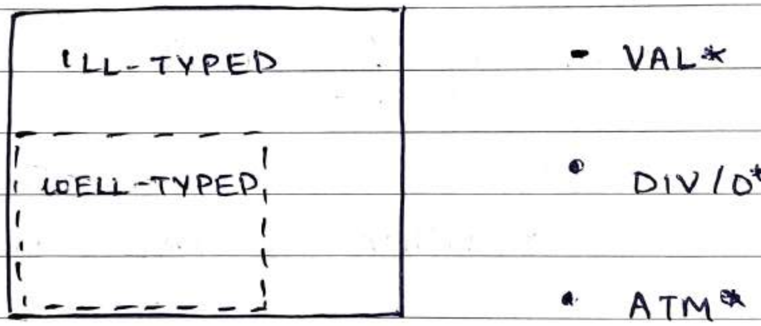
(c) $e \to$

Progress: $\forall$ e τ

either e VAL*, or

e DIV/0*

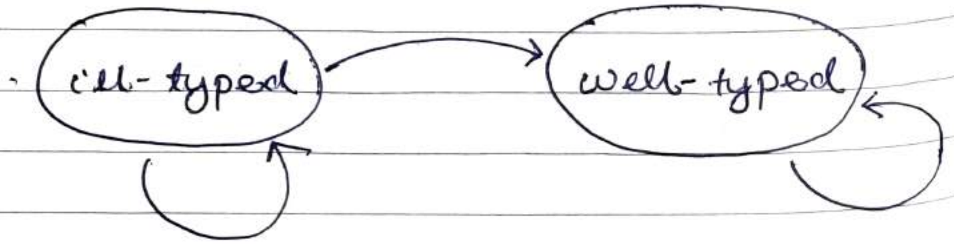




PRESERVATION

$$e\ \tau \quad \text{and} \quad e \to e' \;\Rightarrow\; e'\ \tau$$

a well-typed expression preserves its well-typedness property (as also its type) upon reduction.



PROOF OF PRESERVATION

given,

$$e \to e' \quad , \quad e\ \tau$$

show $e'\ \tau$

by induction on $\to$

(1) $\underbrace{\bar{n}_1 \oplus \bar{n}_2}_{e} \longrightarrow \underbrace{\overline{n_1 + n_2}}_{e'}$

(a) $e = \bar{n}_1 \oplus \bar{n}_2$

$\bar{n}_1$ NUM

$$\frac{\bar{n}_1 \text{ NUM} \qquad \bar{n}_2 \text{ NUM}}{e \text{ NUM}} \text{NUM}$$

$\bar{n}_2$ NUM

$\therefore \tau = \text{NUM}$

(b) $\overline{n_1 + n_2}$ NUM

$$\frac{}{\underbrace{\overline{n_1+n_2}}_{e'} \text{ NUM}} \text{NUM}$$

$\therefore e \text{ NUM} \longrightarrow e' \text{ NUM}$

(2) $\overline{n_1} \; / \; \overline{n_2} \longrightarrow \overline{n_1 / n_2}$

provided $n_2 \neq 0$

similar to (1)

(3) $\underbrace{\text{if true } e_2 \; e_3}_{e} \longrightarrow \underbrace{e_2}_{e'}$

$e \; \tau$,

by inversion, $e_2 \; \tau$
$e_3 \; \tau$, done

(4) $$\frac{e_1 \rightarrow e_1'}{\underbrace{e_1 + e_2}_{e} \rightarrow \underbrace{e_1' + e_2}_{e'}} \text{ PLUS-LEFT}$$

$e : \tau$ by inversion & pattern matching

$$\frac{e_1' \text{ NUM} \qquad e_2 \text{ NUM}}{e_1' + e_2 \text{ NUM}} \text{ PLUS}$$

$\tau = NUM$ $\quad$ e_1 NUM

e_2 NUM

by IH,

e_1' NUM

(5). $$\frac{e_1 \rightarrow e_1'}{e_1 \oslash e_2 \rightarrow e_1' \oslash e_2} \text{ DIV-LEFT}$$

similar to (4).

(6) $$\frac{e_1 \text{ VAL} \quad e_2 \rightarrow e_2'}{\underbrace{e_1 \oplus e_2}_{e} \rightarrow \underbrace{e_1 \oplus e_2'}_{e'}} \text{ PLUS-RIGHT}$$

by inversion & pattern matching,

$\tau = NUM$, $\quad$ e_1 NUM

e_2 NUM

by IH,

e_2' NUM

$$\therefore \frac{e_1\ NUM \qquad e_2'\ NUM}{\underbrace{e_1 \oplus e_2'}_{e'}\ \ NUM}$$

(7) $$\frac{e_1\ VAL \quad e_2 \rightarrow e_2'}{e_1 \oslash e_2 \rightarrow e_1 \oslash e_2'}\ \text{DIV-RIGHT}$$

Similar to (6)

(8) $$\frac{e_1 \rightarrow e_1'}{\underbrace{\text{if}\ e_1\ e_2\ e_3}_{e} \rightarrow \underbrace{\text{if}\ e_1'\ e_2\ e_3}_{e'}}\ \text{IF}$$

$e\ \tau$

by inversion & pattern matching

e_1 BOOL

$e_2\ \tau$

$e_3\ \tau$

$$\therefore \frac{e_1'\ BOOL \quad e_2\ \tau \quad e_3\ \tau}{\text{if}\ e_1'\ e_2\ e_3\ \ \tau}$$

by IH,

e_1' BOOL

QED

thus we have proved PRESERVATION

$e\ \tau$ and $e \to e'$

$\Rightarrow e'\ \tau$

PROGRESS

if $e\ \tau$ then,

e VAL, or

e DIV/0, or

$e \to$

PROOF BY INDUCTION ON $e\ \tau$

(1) $\dfrac{}{\underbrace{\bar{n}}_{e}\ \text{NUM}}\ \text{NUM}$ clearly e VAL

(2) $\dfrac{}{\underbrace{\bar{b}}_{e}\ \text{BOOL}}\ \text{BOOL}$ similar to (1).

(3) $$\frac{e_1 \text{ NUM} \quad e_2 \text{ NUM}}{e_1 \oplus e_2 \text{ NUM}} \quad \text{PLUS}$$

by IH, e_1 VAL, or

e_1 DIV/0, or

$e_1 \rightarrow$

and, (9 cases)

e_2 VAL, or

e_2 DIV/0, or

$e_2 \rightarrow$

(3.1) $e_1 \rightarrow$

then let, $e_1 \rightarrow e_1'$

$$\therefore \frac{e_1 \rightarrow e_1' \quad e_2}{\underbrace{e_1 \oplus e_2}_{e} \rightarrow \underbrace{e_1' \oplus e_2}_{e'}}$$

$\therefore$ $e \rightarrow$

(3.2) e_1 DIV/0

then we have a DIV/0 deduction

$$\frac{e_1 \;\; \text{DIV/0}}{e_1 \oplus e_2 \;\; \text{DIV/0}} \; \text{DIV/0 : LEFT}$$

(3.3) e_1 VAL 3 cases for e_2

(3.3.1) $e_2 \rightarrow$

then we have a deduction in $\rightarrow$

$$\frac{e_1 \;\text{VAL} \qquad e_2 \rightarrow e_2'}{\underbrace{e_1 \oplus e_2}_{e} \rightarrow \underbrace{e_1 \oplus e_2'}_{e'}} \; \text{P-LEFT}$$

$\therefore e \rightarrow$

(3.3.2) e_2 DIV/0

then we have a derivation in DIV/0

$$\frac{e_1 \;\text{VAL} \qquad e_2 \;\text{DIV/0}}{e_1 \oplus e_2 \;\; \text{DIV/0}} \; \text{DIV/0 : P-RIGHT}$$

3.3.3 e_2 VAL

4 cases

$$\left\{\begin{array}{l} e_1 = \bar{n}_1 \\ e_1 = \bar{b}_1 \end{array}\right\} \times \left\{\begin{array}{l} e_2 = \bar{n}_2 \\ e_2 = \bar{b}_2 \end{array}\right\}$$

of these 4 cases

$e_1 = \bar{b}$ is not possible $\because$ e_1 NUM

$e_2 = \bar{b}$ for the same reason

$\therefore$ this leaves only one case

$e_1 = \bar{n}_1$ $\qquad \therefore e_1 \oplus e_2 = \underbrace{\bar{n}_1 \oplus \bar{n}_2}_{e}$

$e_2 = \bar{n}_2$

$$\downarrow$$

$$\overline{n_1 + n_2}$$

$\therefore e \rightarrow$

done.

(4) $$\frac{e_1 \ NUM \qquad e_2 \ NUM}{e_1 \ (/) \ e_2 \ NUM} \ DIV$$

exercise

(5). $$\frac{e_1 \ BOOL \qquad e_2 \ \tau \qquad e_3 \ \tau}{\underbrace{(if) \ e_1 \ e_2 \ e_3}_{e} \quad \tau} \ IF$$

by inversion & pattern Matching

e_1 BOOL $\quad e_2 \ \tau \quad e_3 \ \tau$

by IH, there are 3 cases

e_1 VAL

e_1 DIV/0

$e_1 \rightarrow$

(5.1) $e_1 \rightarrow$

then we have a derivation

$$\frac{e_1 \rightarrow e_1'}{\underbrace{(if) \ e_1 \ e_2 \ e_3}_{e} \rightarrow (if) \ e_1' \ e_2 \ e_3} \ IF\text{-}TEST$$

$\therefore e \rightarrow \quad$ done.

5.2 e_1 DIV/0

$$\frac{e_1 \cdot \text{DIV/0}}{\underbrace{\text{if } e_1\ e_2\ e_3}_{e}\ \text{DIV/0}}\ \text{DIV/0 : IF}$$

$\therefore$ e DIV/0

5.3 e_1 VAL

sine e_1 BOOL, it follows that

5.3.1 e_1 = true, then

$$\frac{}{\underbrace{\text{if true } e_2\ e_3}_{e} \rightarrow e_2}\ \text{IF-TRUE}$$

$\therefore$ $e \rightarrow$

5.3.2 e_1 = false

similar

QED