~min sheet ~

# Preservation

If $\vdash e : \tau$ and $e \longmapsto e'$ then $\vdash e' : \tau$

Proof by induction $e \longmapsto e'$.

[Case : D-LET]

GOAL = If $\vdash let(e_1; x.e_2) : \tau$
and $let(e_1; x.e_2) \longmapsto e_2[e_1/x]$
then $e_2[e_1/x] : \tau$

P1 = $\vdash let(e_1; x.e_2) : \tau$
P2 = $let(e_1; x.e_2) \longmapsto e_2[e_1/x]$

GOAL' = $e_2[e_1/x] : \tau$

By inversion on P1, we know that there must exist a type $\sigma$ such that

- $\vdash e_1 : \sigma$ (INV 1)
- $x : \sigma \vdash e_2 : \tau$ (INV 2)

(Subst) If $\Gamma \vdash e : \tau$ and $\Gamma, x : \tau \vdash u : \sigma$
then $\Gamma \vdash u[e/x] : \sigma$

Subst specialised :

If $\vdash e_1 : \sigma$ and $x : \sigma \vdash e_2 : \tau$
then $\vdash e_2[e_1/x] : \tau$

We can conclude our goal by applying the subst lemma to INV1 and INV2

$\square_{D\text{-LET}}$

# Canonical Forms

(Canonical Forms) Suppose $e$ val

1. If $\vdash e : \mathsf{Nom}$ then $e = \mathsf{num}[n]$ for some $n \in \mathbb{N}$
2. If $\vdash e : \mathsf{Str}$ then $e = \mathsf{str}[s]$ for some $s \in \Sigma^*$

Proof by inspection

# Progress

(Progress) If $\vdash e : \tau$ then either $e$ val or $e \mapsto e'$ for some $e'$

Proof by induction $\vdash e : \tau$

[Case: PLUS]

GOAL = If $plus(e_1; e_2) : \tau$ then either $e$ val or $plus(e_1; e_2) \mapsto e'$ for some $e'$

P1 = $plus(e_1; e_2) : \tau$

GOAL' = either $e$ val or $plus(e_1; e_2) \mapsto e'$ for some $e'$

We will show the latter (since PLUS is not a value)

IH1 = if $\vdash e_1 : \tau_1$ then either $e_1$ val or $e_1 \mapsto e_1'$ for some $e_1'$

IH2 = if $\vdash e_2 : \tau_2$ then either $e_2$ val or $e_2 \mapsto e_2'$ for some $e_2'$

By inversion on P1 we can conclude

- $\tau = Num$ (INV1)
- $\vdash e_1 : Num$ (INV2)
- $\vdash e_2 : Num$ (INV3)

By applying IH1 to INV2 we can conclude:

UIH1 = either $e_1$ val or $e_1 \mapsto e_1'$ for some $e_1'$

By applying IH2 to INV3 we can conclude:

UIH2 = either $e_2$ val or $e_2 \mapsto e_2'$ for some $e_2'$

We proceed by case analysis on UIH1 and UIH2

[subcase: $e_1$ val]

[subsubcase: $e_2$ val]

By canonical forms, we have

$e_1 = num[n_1]$ for some $n_1 \in \mathbb{N}$
$e_2 = num[n_2]$ for some $n_2 \in \mathbb{N}$

We can apply the D-PLUS rule to get $e' = num[n']$ where $n' = n_1 + n_2$

$$\text{D-PLUS}\ \frac{n_1 + n_2 = n'}{plus(n_1; n_2) \mapsto num[n]}$$

$\square$ D-PLUS $e_1$ val $e_2$ val

[subsubcase: $e_2 \mapsto e_2'$ for some $e_2'$]

By canonical forms, we have $e_1 = num[n_1]$

$$\text{D-PLUS-2}\ \frac{e_1\ \text{val} \quad e_2 \mapsto e_2'}{plus(e_1; e_2) \mapsto plus(e_1; e_2')}$$

Thus $e' = plus(e_1; e_2')$

$\square$ D-PLUS, $e_1$ val, $e_2 \mapsto e_2'$

[subcase: $e_1 \mapsto e_1'$ for some $e_1'$]

Regardless of what $e_2$ is, we can produce $e'$ using D-PLUS-1

$$\text{D-PLUS-1}\ \frac{e_1 \mapsto e_1'}{plus(e_1; e_2) \mapsto plus(e_1'; e_2)}$$

Thus we have achieved our goal $e' = plus(e_1'; e_2)$.

$\square$ D-PLUS, $e_1 \mapsto e_1'$

We have exhaustively covered all the cases (UIH1, UIH2).

Thus we are for D-PLUS

$\square$ D-PLUS