Problem Sheet 3

Alex Kavvos

The following questions are about the dynamics of numbers and strings.

1. Draw derivations that justify the following transitions.

   (i) $\mathsf{plus}(\mathsf{num}[1]; \mathsf{num}[1]) \longmapsto \mathsf{num}[2]$

   (ii) $\mathsf{times}(\mathsf{plus}(\mathsf{num}[1]; \mathsf{num}[1]); \mathsf{num}[2]) \longmapsto \mathsf{times}(\mathsf{num}[2]; \mathsf{num}[2])$

   (iii) $\mathsf{len}(\mathsf{let}(\mathsf{str}[\text{‘a’}]; v.\, \mathsf{cat}(v; \mathsf{str}[\text{‘b’}]))) \longmapsto \mathsf{len}(\mathsf{cat}(\mathsf{str}[\text{‘a’}]; \mathsf{str}[\text{‘b’}]))$

2. Write down transition sequences that justify the following multi-step transitions.

   (i) $\mathsf{times}(\mathsf{plus}(\mathsf{num}[1]; \mathsf{num}[1]); \mathsf{num}[2]) \longmapsto^* \mathsf{num}[4]$

   (ii) $\mathsf{times}(\mathsf{len}(\mathsf{let}(\mathsf{str}[\text{‘a’}]; v.\, \mathsf{cat}(v; \mathsf{str}[\text{‘b’}]))); \mathsf{num}[2]) \longmapsto^* \mathsf{num}[4]$

3. Are the following terms well-typed? Write down transition sequences that reduce them to values.

   (i) $\mathsf{let}(\mathsf{str}[\text{‘a’}]; z.\, \mathsf{plus}(\mathsf{len}(z); \mathsf{len}(z)))$

   (ii) $\mathsf{let}(\mathsf{len}(\mathsf{str}[\text{‘a’}]); z.\, \mathsf{plus}(z; z))$

   (iii) $\mathsf{plus}(\mathsf{let}(\mathsf{len}(\mathsf{str}[\text{‘a’}]); z.\, \mathsf{plus}(z; z)); \mathsf{num}[1])$

4. The rules D-Plus-1 and D-Plus-2 of the dynamics enforce that e_1 is evaluated *before* e_2 when computing the value of $\mathsf{plus}(e_1; e_2)$. Propose alternative versions of these rules that evaluate e_2 before e_1. Would you expect your rules to affect the final value that is returned?

   Solution:

   D-Plus-1
   $$\frac{e_2 \longmapsto e_2'}{\mathsf{plus}(e_1; e_2) \longmapsto \mathsf{plus}(e_1; e_2')}$$

   D-Plus-2
   $$\frac{e_2 \ \mathsf{val} \qquad e_1 \longmapsto e_1'}{\mathsf{plus}(e_1; e_2) \longmapsto \mathsf{plus}(e_1'; e_2)}$$

   Changing these rules will not influence the final value. This is because our language is purely functional. This can be shown through a result known as **confluence** (or the **Church-Rosser property**), but we will not cover the proof in this unit.

5. Prove that if e val then either $\vdash e : \mathsf{Num}$ or $\vdash e : \mathsf{Str}$.

   Solution: By induction on e val.

   Case(Val-Num).

If the derivation is of the form

$$\frac{n \in \mathbb{N}}{\mathsf{num}[n]\ \mathsf{val}}\ \textsc{Val-Num}$$

(so that $e = \mathsf{num}[n]$) then we can produce the following derivation of the conclusion:

$$\frac{n \in \mathbb{N}}{\vdash \mathsf{num}[n] : \mathsf{Num}}\ \textsc{Num}$$

Case(Val-Str).

If the derivation is of the form

$$\frac{s \in \Sigma^*}{\mathsf{str}[s]\ \mathsf{val}}\ \textsc{Val-Str}$$

(so that $e = \mathsf{str}[s]$) then we can produce the following derivation of the conclusion:

$$\frac{s \in \Sigma^*}{\vdash \mathsf{str}[s] : \mathsf{Str}}\ \textsc{Str}$$

6. Prove that multi-step transitions are transitive, i.e. that the following rule is admissible:

$$\frac{e_1 \longmapsto^* e_2 \qquad e_2 \longmapsto^* e_3}{e_1 \longmapsto^* e_3}$$

[Hint: perform an induction on the premise $e_1 \longmapsto^* e_2$.]

Solution: By induction on $e_1 \longmapsto^* e_2$.

Case(D-Multi-Refl). If the derivation is of the form

$$\frac{}{e_1 \longmapsto^* e_1}\ \textsc{D-Multi-Refl}$$

i.e. e_1 and e_2 are syntactically identical ($e_1 \equiv e_2$). In that case, the second premise is a derivation of $e_1 \longmapsto^* e_3$, which is exactly the conclusion we were trying to show.

Case(D-Multi-Step). Suppose the derivation is of the form

$$\frac{\dfrac{\vdots}{e_1 \longmapsto e'} \qquad \dfrac{\vdots}{e' \longmapsto^* e_2}}{e_1 \longmapsto^* e_2}\ \textsc{D-Multi-Step}$$

for some e'. Then by the IH applied to the 'smaller' derivation $e' \longmapsto^* e_2$ and $e_2 \longmapsto^* e_3$

we obtain a derivation of $e' \longmapsto^* e_3$. We can then obtain a derivation of the conclusion:

$$\dfrac{\dfrac{\vdots}{e_1 \longmapsto e'} \qquad \dfrac{\vdots}{e' \longmapsto^* e_3}}{e_1 \longmapsto^* e_3} \text{ D-MULTI-STEP}$$

7. $(*)$ Complete the proof of preservation.

Solution: The claim is: if $\vdash e : \tau$ and $e \longmapsto e'$ then $\vdash e' : \tau$.

The proof is by induction on the derivation of $e \longmapsto e'$.

Case(D-PLUS).

Suppose that the reduction $e \longmapsto e'$ is of the form

$$\dfrac{n_1 + n_2 = n}{\mathsf{plus}(\mathsf{num}[n_1]; \mathsf{num}[n_2]) \longmapsto \mathsf{num}[n]} \text{ D-PLUS}$$

(so $e = \mathsf{plus}(\mathsf{num}[n_1]; \mathsf{num}[n_2])$ and $e' = \mathsf{num}[n]$). Then we have

$$\dfrac{n \in \mathbb{N}}{\vdash \mathsf{num}[n] : \mathsf{Num}} \text{ NUM}$$

Case(D-PLUS-1).

Suppose that the reduction is of the form

$$\dfrac{\dfrac{\vdots}{e_1 \longmapsto e_1'}}{\mathsf{plus}(e_1; e_2) \longmapsto \mathsf{plus}(e_1'; e_2)} \text{ D-PLUS-1}$$

It is given that $\vdash \mathsf{plus}(e_1; e_2) : \tau$. By **inversion** it must be that $\tau = \mathsf{Num}$, $\vdash e_1 : \mathsf{Num}$, and $\vdash e_2 : \mathsf{Num}$.

By the IH applied to the 'smaller' derivation of $e_1 \longmapsto e_1'$ and the judgement $\vdash e_1 : \mathsf{Num}$ we conclude that $\vdash e_1' : \mathsf{Num}$. We can then combine that into a derivation

$$\dfrac{\dfrac{\vdots}{\vdash e_1' : \mathsf{Num}} \qquad \dfrac{\vdots}{\vdash e_2 : \mathsf{Num}}}{\vdash \mathsf{plus}(e_1'; e_2) : \mathsf{Num}} \text{ PLUS}$$

Case(D-PLUS-2). Similar to D-PLUS-1.

Case(D-CAT). Similar to D-PLUS.

Case(D-CAT-1). Similar to D-PLUS-1.

Case(D-CAT-2). Similar to D-PLUS-2.

Case(D-LEN). Similar to D-PLUS.

Case(D-LEN-1). Similar to D-PLUS-2 (but with fewer premises).

Case(D-LET). Suppose that the reduction is of the form

$$\frac{}{\mathsf{let}(e_1; x.\, e_2) \longmapsto e_2[e_1/x]}\ \textsc{D-Let}$$

We know that $\vdash \mathsf{let}(e_1; x.\, e_2) : \tau$. By **inversion** there must exist σ such that $\vdash e_1 : \sigma$ and $x : \sigma \vdash e_2 : \tau$. By the **substitution lemma** (Lecture 4) we obtain $\vdash e_2[e_1/x] : \tau$, which is what we wanted to prove.

8. Complete the proof of progress.

Solution: The claim is that if $\vdash e : \tau$ then either e val or $e \longmapsto e'$ for some e'.

The proof is by induction on $\vdash e : \tau$.

Case(VAR).

It cannot be that $\vdash e : \tau$ is derived through the rule VAR, as its context is empty.

Case(NUM).

If the derivation is of the form

$$\frac{n \in \mathbb{N}}{\vdash \mathsf{num}[n] : \mathsf{Num}}\ \textsc{Num}$$

then we know that $\mathsf{num}[n]$ val by the rule VAL-NUM.

Case(STR). Similar to NUM.

Case(PLUS).

Suppose the derivation is of the form

$$\frac{\dfrac{\vdots}{\vdash e_1 : \mathsf{Num}} \qquad \dfrac{\vdots}{\vdash e_2 : \mathsf{Num}}}{\vdash \mathsf{plus}(e_1; e_2) : \mathsf{Num}}\ \textsc{Plus}$$

We apply the IH to the smaller derivation $\vdash e_1 : \mathsf{Num}$; this gives two cases.

- Suppose e_1 val. We apply the IH to smaller derivation of $\vdash e_2 : \mathsf{Num}$ to obtain two further cases.

– If e_2 val, then both e_1 and e_2 are values of numerical type. By the **canonical forms lemma** it must be that $e_1 = \mathsf{num}[n_1]$ and $e_2 = \mathsf{num}[n_2]$ for some $n_1, n_2 \in \mathbb{N}$. We then have

$$\frac{}{\mathsf{plus}(\mathsf{num}[n_1]; \mathsf{num}[n_2]) \longmapsto \mathsf{num}[n_1 + n_2]}\ \text{D-PLUS}$$

Hence there is a term to which $\mathsf{plus}(e_1; e_2) = \mathsf{plus}(\mathsf{num}[n_1]; \mathsf{num}[n_2])$ steps, namely $\mathsf{num}[n_1 + n_2]$.

– If $e_2 \longmapsto e_2'$ for some e_2' then we can construct the following derivation.

$$\frac{\dfrac{\vdots}{e_1\ \mathsf{val}} \qquad \dfrac{\vdots}{e_2 \longmapsto e_2'}}{\mathsf{plus}(e_1; e_2) \longmapsto \mathsf{plus}(e_1; e_2')}\ \text{D-PLUS-2}$$

Hence there exists a term to which $\mathsf{plus}(e_1; e_2) = \mathsf{plus}(\mathsf{num}[n_1]; \mathsf{num}[n_2])$ steps, namely $\mathsf{plus}(e_1; e_2')$.

- If there exists e_1' such that $e_1 \longmapsto e_1'$, then we can construct the derivation

$$\frac{\dfrac{\vdots}{e_1 \longmapsto e_1'}}{\mathsf{plus}(e_1; e_2) \longmapsto \mathsf{plus}(e_1'; e_2)}\ \text{D-PLUS-1}$$

Hence there is a term to which $\mathsf{plus}(e_1; e_2)$ steps, namely $\mathsf{plus}(e_1'; e_2)$.

In all cases, there exists a term to which $\mathsf{plus}(e_1; e_2)$ steps.

Case(TIMES). Similar to PLUS.

Case(CAT). Similar to PLUS, but for strings.

Case(LEN). Similar to PLUS (do it for practice).

Case(LET).

Suppose the derivation is of the form

$$\frac{\vdash e_1 : \sigma \qquad x : \sigma \vdash e_2 : \tau}{\vdash \mathsf{let}(e_1; x.\, e_2) : \tau}\ \text{LET}$$

Then we have that

$$\frac{}{\mathsf{let}(e_1; x.\, e_2) \longmapsto e_2[e_1/x]}\ \text{D-LET}$$

Hence there is a term to which $\mathsf{let}(e_1; x.\, e_2)$ steps, namely $e_2[e_1/x]$.

9. (Hard, trick, highly optional.) We proved preservation by induction on $e \longmapsto e'$, while we

proved progress by induction on $\vdash e : \sigma$. Why did we make that choice? Could we have performed an induction on $\vdash e : \sigma$ for both? Discuss.

Solution: It is sometimes theoretically possible to prove preservation by induction on the typing derivation—you are welcome to try it for this language. However, this might lead to fairly nasty inversion and case analyses on the reduction $e \longmapsto e'$ after the type and shape of e has been established, which might lead to a convoluted proof. The most straightforward proof proceeds by induction on $e \longmapsto e'$, which we have presented in full here.