Thanks

- I made all induction principles more "uniform"

$$\frac{\begin{array}{l}(\forall x\, a)\ P\,(\mathsf{Var}(a))\,x \\ (\forall x\, t_1, t_2)\ ((\forall z)\ P\,t_1\,z) \wedge ((\forall z)\ P\,t_2\,z) \\ \qquad\qquad\qquad\qquad \Rightarrow P\,(\mathsf{App}(t_1, t_2))\,x \\ (\forall x\, a\, t)\ a \# x \wedge\ ((\forall z)\ P\,t\,z) \Rightarrow P\,([a].t)\,x\end{array}}{(\forall x\, t)\ P\,t\,x}$$

Problem

Do definitions like the following make sense as functions?

- $\mathsf{Var}(y)[x := t] = \mathtt{if}\ x = y\ \mathtt{then}\ t\ \mathtt{else}\ \mathsf{Var}(y)$
- $\mathsf{App}(s_1, s_2)[x{:=}t] = \mathsf{App}(s_1[x{:=}t], s_2[x{:=}t])$
- $([a].s)[x{:=}t] = [a].(s[x{:=}t])$

  provided $a \# (x, t)$

Substitution as Relation

Let us define the four-place relation:

- $\mathsf{Var}(x)[x := t] \mapsto t$
- $\mathsf{Var}(y)[x := t] \mapsto t$ provided $x \neq y$
- $\mathsf{App}(s_1, s_2)[x{:=}t] \mapsto \mathsf{App}(s'_1, s'_2)$
  provided $s_1[x{:=}t] \mapsto s'_1$ and $s_2[x{:=}t] \mapsto s'_2$
- $([a].s)[x{:=}t] \mapsto [a].s'$
  provided $a \# (x, t)$ and $s[x{:=}t] \mapsto s'$

Substitution is "Total"

This substitution relation is, so to say, total:

$$\forall t_1\, x\, t_2.\ \exists t_3.\ t_1[x:=t_2] \mapsto t_3$$

Proof by induction on t_1 using the convenient structural induction principle.

Convenient Principle

$$\frac{\begin{array}{l}(\forall x\, a)\; P\,(\mathsf{Var}(a))\,x \\ (\forall x\, t_1, t_2)\;((\forall z)\; P\, t_1\, z) \wedge ((\forall z)\; P\, t_2\, z) \\ \qquad\qquad\qquad \Rightarrow P\,(\mathsf{App}(t_1, t_2))\,x \\ (\forall x\, a\, t)\; a \# x \wedge\; ((\forall z)\; P\, t\, z) \Rightarrow P\,([a].t)\,x\end{array}}{(\forall x\, t)\; P\, t\, x}$$

- $P = \lambda t_1 (x, t_2).\ \exists t_3.\ t_1[x := t_2] \mapsto t_3$
- $t = t_1$
- $x = (x, t_2)$

Lambda-case: $a \# (x, t_2)$ and $\forall x\, t_2.\ \exists t_3.t[x := t_2] \mapsto t_3$ implies $\exists t_3.\ ([a].t)[x := t] \mapsto t_3$. Trivial.

Substitution is "Unique"

This substitution relation is, so to say, total:

$$\forall s_1\, s_2.\;\; t_1[x := t_2] \mapsto s_1 \wedge \;\; t_1[x := t_2] \mapsto s_2 \;\; \Rightarrow \;\; s_1 = s_2$$

Proof by induction on t_1 using the convenient structural induction principle. Lambda-Case relies on the fact...

Lambda-Case

This case is a bit hairy:

$$([a].s)[x := t_2] \mapsto t \wedge a \# (x, t_2)$$
$$\Rightarrow \ \exists t'.\, t = [a].t' \ \wedge \ s[x := t_2] \mapsto t'$$

where we use equivariance of substitution:

$$t_1[x := t_2] \mapsto t_3 \Leftrightarrow$$
$$(\pi \bullet t_1)[(\pi \bullet x) := (\pi \bullet t_2)](\pi \bullet t_3)$$

and

$$t_1[x := t_2] \mapsto t_3 \Rightarrow$$
$$(\mathsf{supp}\ t_3) \subseteq ((\mathsf{supp}\ t_1) - \{x\}) \cup (\mathsf{supp}\ t_2)$$

Definite Description

After having shown that

$$\forall t_1\, x\, t_2.\ \exists! t_3.\ t_1[x := t_2] \mapsto t_3$$

we can use Isabelle's definite description operator THE to define substitution as function.

if $P\ a$ and $\forall x.\ P\ x \Rightarrow x = a$,

then $(THE\ x.\ P\ x) = a$

The user does not see anything of this construction, but...

Freshness Lemma

- A criterion when a construction that "picks a fresh atom" is independent of which fresh atom is chosen:

Given $pt_{\alpha,\iota}$, at_α and a function $h : \alpha \longrightarrow \iota$:

- if $\mathsf{finite}(\mathsf{supp}_\alpha\ h)$ and

  $\exists a.\ a \# h \wedge a \# (h\ a)$

  then

  $\exists! fr.\ \forall a.\ a \# h \;\Rightarrow\; (h\ a) = fr$

Proof (Existence)

From the assumption there exists an a_0 with

1. $a_0 \# h$ and 2. $a_0 \# (h\ a_0)$

Proof (Existence)

From the assumption there exists an a_0 with

1. $a_0 \# h$ and 2. $a_0 \# (h\ a_0)$

We take fr to be $h\ a_0$ and have

3. $a \# h$ and claim that $(h\ a) = (h\ a_0)$

Proof (Existence)

From the assumption there exists an a_0 with

1. $a_0 \# h$ and 2. $a_0 \# (h\ a_0)$

We take fr to be $h\ a_0$ and have

3. $a \# h$ and claim that $(h\ a) = (h\ a_0)$

Trivially true for $a = a_0$. For $a \neq a_0$:

4. $a \# (h\ a_0)$

since $a \# h$ (2) and $a \# a_0$ and

$$\mathsf{supp}(h\ a_0) \subseteq \mathsf{supp}(h) \cup \mathsf{supp}(a_0)$$

(also $\mathsf{finite}(\mathsf{supp}\ h)$ and $\mathsf{finite}(\mathsf{supp}\ a_0)$)

Proof (Existence)

From the assumption there exists an a_0 with

1. $a_0 \# h$ and 2. $a_0 \# (h\ a_0)$

We take fr to be $h\ a_0$ and have

3. $a \# h$ and claim that $(h\ a) = (h\ a_0)$

Trivially true for $a = a_0$. For $a \neq a_0$:

4. $a \# (h\ a_0)$

We get from (2,4) and (1,3):

5. $(a\,a_0)\bullet(h\ a_0) = (h\ a_0)$
6. $(a\,a_0)\bullet(h\ a_0) = ((a\,a_0)\bullet h)((a\,a_0)\bullet a_0) = (h\ a)$

Proof (Uniqeness)

From the assumption there exists an a_0 with $a_0 \# h$ and we have

1. $\forall a.\ a \# h \Rightarrow (h\ a) = fr_1$
2. $\forall a.\ a \# h \Rightarrow (h\ a) = fr_2$

Clearly, $fr_1 = fr_2$.