Proving with Computer Assistance, 2IMF15

Herman Geuvers, TUE

Exercises on Higher order logic and the Calculus of Constructions

NB All exercises can also be made with Coq. Please look at the web site for the `.v` file. You can create a new file under your proofweb login and work with it.

1. Definition in CC (for $t, q : A$):

$$t =_A q := \Pi P{:}A{\to}{*}.(Pt \to Pq)$$

   (a) (basic) Prove that this equality is reflexive by giving a term of type $\Pi x{:}A.x =_A x$.
   Answer: ....
   Without typing derivation:
   $\lambda x{:}A.\lambda P{:}A{\to}*.\lambda h{:}P\,x.h : \Pi x{:}A.x =_A x$
   End Answer ....

   (b) (basic) Prove that this equality is transitive by giving a term of type $\Pi x, y, z{:}A.x =_A y \to y =_A z \to x =_A z$.
   Answer: ....
   Without typing derivation:
   $\lambda x, y, z{:}A.\lambda f{:}x =_A y.\lambda g{:}y =_A z.\lambda P{:}A{\to}*.\lambda h{:}P\,x.g\,P(f\,P\,h) :$
   $\Pi x, y, z{:}A.x =_A y \to y =_A z \to x =_A z$
   End Answer ....

   (c) (advanced) Prove that this equality is symmetric by giving a term of the type $\Pi x, y{:}A.x =_A y \to y =_A x$.
   Answer: ....
   Without typing derivation:
   $\lambda x, y{:}A.\lambda e{:}x =_A y.\lambda P{:}A{\to}*.\lambda h{:}P\,y.e\,(\lambda z{:}A.P\,z \to P\,x)\,(\lambda u{:}P\,x.u)\,h :$
   $\Pi x, y{:}A.x =_A y \to y =_A x$
   With typing derivation. At line 5 we need a smart choice for P' so that e can help us to construct a term of type $P\,x$ from $h : P\,y$. The trick is to take $\lambda z : A.P\,z{\to}P\,x$ for P'.

1	$x, y : A$
2	$e : \Pi P' : A \to * . P'\, x \to P\, y$
3	$P : A \to *$
4	$h : P\, y$
5	$e\,(\lambda z : A.P\, z \to P\, x) : (P\, x \to P\, x) \to (P\, y \to P\, x)$
6	$u : P\, x$
7	$u : P\, x$
8	$\lambda u{:}P\, x.u : P\, x \to P\, x$
9	$e\,(\lambda z : A.P\, z \to P\, x)\,(\lambda u{:}P\, x.u) : P\, y \to P\, x$
10	$e\,(\lambda z : A.P\, z \to P\, x)\,(\lambda u{:}P\, x.u)\, h : P\, x$
11	$\lambda h{:}P\, y.e\,(\lambda z : A.P\, z \to P\, x)\,(\lambda u{:}P\, x.u)\, h : P\, y \to P\, x$
12	$\lambda P{:}A \to * .\lambda h{:}P\, y.e\,(\lambda z : A.P\, z \to P\, x)\,(\lambda u{:}P\, x.u)\, h : y =_A x$
13	$\lambda e{:}x =_A y.\lambda P{:}A \to * .\lambda h{:}P\, y.e\,(\lambda z : A.P\, z \to P\, x)\,(\lambda u{:}P\, x.u)\, h : x =_A y \to y =_A x$
14	$\lambda x, y{:}A.\lambda e{:}x =_A y.\lambda P{:}A \to * .\lambda h{:}P\, y.e\,(\lambda z : A.P\, z \to P\, x)\,(\lambda u{:}P\, x.u)\, h :$
15	$\Pi x, y : A.x =_A y \to y =_A x$

End Answer ....

2. The transitive closure of a binary relation R on A has been defined as follows.

$$\begin{array}{lll} \mathsf{trclos}\, R & := & \lambda x, y{:}A. \\ & & (\forall Q{:}A \to A \to * .(\mathsf{trans}\, Q \to (R \subseteq Q) \to (Q\, x\, y))). \end{array}$$

(a) (basic) Prove – by giving a proof-term – that the transitive closure of R contains R.

(b) (medium) Prove – by giving a proof-term – that the transitive closure is transitive.

Answer: ....

Without typing derivation:

$\lambda x, y{:}A.\lambda e{:}x =_A y.\lambda P{:}A \to *.\lambda h{:}P\, y.e\,(\lambda z{:}A.P\, z \to P\, x)\,(\lambda u{:}P\, x.u)\, h :$
$\Pi x, y{:}A.x =_A y \to y =_A x$

With typing derivation. At line 5 we need a smart choice for P' so that e can help us to construct a term of type $P\, x$ from $h : P\, y$. The trick is to take $\lambda z : A.P\, z \to P\, x$ for P'.

$$
\begin{array}{rl}
1 & x, y, z : A \\
2 & \quad h : \mathsf{trclos}\, R\, x\, y \\
3 & \quad\quad g : \mathsf{trclos}\, R\, y\, z \\
4 & \quad\quad\quad Q : A{\to}A{\to}* \\
5 & \quad\quad\quad\quad t : \mathsf{trans}\, Q \\
6 & \quad\quad\quad\quad\quad s : R \subseteq Q \\
7 & \quad\quad\quad\quad\quad g\, Q\, t\, s : Q\, y\, z \\
8 & \quad\quad\quad\quad\quad h\, Q\, t\, s : Q\, x\, y \\
9 & \quad\quad\quad\quad\quad t\, x\, y\, z : Q\, x\, y{\to}Q\, y\, z{\to}Q\, x\, z \\
10 & \quad\quad\quad\quad\quad t\, x\, y\, z\, (h\, Q\, t\, s)\, (g\, Q\, t\, s) : Q\, x\, z \\
11 & \quad\quad\quad\quad \lambda s{:}R \subseteq Q.t\, x\, y\, z\, (h\, Q\, t\, s)\, (g\, Q\, t\, s) : R \subseteq Q{\to}Q\, x\, z \\
12 & \quad\quad\quad \lambda t{:}\mathsf{trans}\, Q.\lambda s{:}R \subseteq Q.t\, x\, y\, z\, (h\, Q\, t\, s)\, (g\, Q\, t\, s) : \mathsf{trans}\, Q{\to}R \subseteq Q{\to}Q\, x\, z \\
13 & \quad\quad \lambda Q{:}A{\to}A{\to} * .\lambda t{:}\mathsf{trans}\, Q.\lambda s{:}R \subseteq Q.t\, x\, y\, z\, (h\, Q\, t\, s)\, (g\, Q\, t\, s) : \mathsf{trclos}\, R\, x\, z \\
14 & \quad \lambda h{:}\mathsf{trclos}\, R\, x\, y.\lambda g{:}\mathsf{trclos}\, R\, y\, z.\lambda Q{:}A{\to}A{\to} * .\lambda t{:}\mathsf{trans}\, Q.\lambda s{:}R \subseteq Q.t\, x\, y\, z\, (h\, Q\, t\, s)\, (g\, Q\, t\, s) \\
15 & \quad\quad\quad\quad : \mathsf{trclos}\, R\, x\, y{\to}\mathsf{trclos}\, R\, y\, z{\to}\mathsf{trclos}\, R\, x\, z \\
16 & \lambda x, y, z{:}A.\lambda h{:}\mathsf{trclos}\, R\, x\, y.\lambda g{:}\mathsf{trclos}\, R\, y\, z.\lambda Q{:}A{\to}A{\to} * .\lambda t{:}\mathsf{trans}\, Q.\lambda s{:}R \subseteq Q. \\
17 & \quad\quad\quad t\, x\, y\, z\, (h\, Q\, t\, s)\, (g\, Q\, t\, s) : \mathsf{trans}(\mathsf{trclos}\, R)
\end{array}
$$

End Answer . . . .

(c) (basic) Prove – by giving a proof-term – that, if P is transitive and P contains R, then P contains $\mathsf{trclos}\, R$.

3. The existential quantifier has been defined by

$$\exists x{:}\sigma.\phi := \forall \alpha{:} * .(\forall x{:}\sigma.\phi \to \alpha) \to \alpha$$

(a) (medium) Given $t : \sigma$ and $q : P\, t$, give a term M such that $M : \exists x{:}\sigma.P\, x$

(b) (medium) Given $q : \exists x{:}\sigma.P\, x$ and $h : \forall y{:}\sigma.P\, y \to C$ with $y \notin \mathrm{FV}(C)$, give a term N of type C.

4. For $D : *$, $A, B : D{\to}*$, we define $A \subseteq B$ as $\forall x{:}D.A\, x{\to}B\, x$. We now define

$$
\begin{array}{lcl}
A \cap B & := & \lambda x{:}D.\forall P{:}D{\to} * .(\forall y{:}D.A\, y{\to}B\, y{\to}P\, y){\to}P\, x \\
A \cup B & := & \lambda x{:}D.\forall P{:}D{\to} * .A \subseteq P{\to}B \subseteq P{\to}P\, x
\end{array}
$$

Prove the following, by giving a (proof) term of the type. Remember that $X \vee Y$ is defined as $\forall \alpha{:} * .(X{\to}\alpha){\to}(Y{\to}\alpha){\to}\alpha$.

(a) $A \subseteq A \cup B$.

(b) (This is hard question) $\forall x{:}D.(A \cup B)\, x \to A\, x \vee B\, x$.

(c) $A \cap B \subseteq A$.

(d) $\forall x{:}D.A\, x \to B\, x \to (A \cap B)\, x$.