MPRI
Foundations of proof systems 2
Gilles Dowek

Exercise 1 *The simple types are inductively defined by two rules:*

- ι *and* o *are simple types,*
- *if* A *and* B *are simple types, then* $A \to B$ *is a simple type.*

For each simple type, we consider an infinite set of variables of this type and possibly some constants. The Simply typed λ*-terms are defined by*

- *variables and constants of type* A *are terms of type* A*,*
- *if* t *is a term of type* $A \to B$ *and* u *a term of type* A*, then* $(t\ u)$ *is a term of type* B*,*
- *if* x *is a variable of type* A *and* t *a term of type* B*, then* $\lambda x : A\ t$ *is a term of type* $A \to B$*.*

1. *The* β*-reduction rule is*

$$((\lambda x : A\ t)\ u) \longrightarrow (u/x)t$$

   Define the notion of one-step β*-reduction, termination and strong termination of* β*-reduction.*

2. *Consider the following strong termination proof.*

   By induction of the structure of λ*-terms*

   - *variables and constants are irreducible, hence they strongly terminate,*
   - *if* t *strongly terminates, then so does* $\lambda x\ t$*,*
   - *if* t *and* u *strongly terminate, then so does* $(t\ u)$*.*

   Why is this proof wrong?

   We define, by induction over the type A*, a set of terms* R_A*.*

   - *If* $A = \iota$ *or* $A = o$*, then a term* t *is an element of* R_A *if and only if it strongly terminates.*
   - *If* $A = B \to C$*, then a term* t *is an element of* R_A *if and only if it strongly terminates and whenever it reduces to a term of the form* $\lambda x : B\ u$*, then for every term* v *in* R_B*,* $(v/x)u$ *is an element of* R_C*.*

3. *Prove that if* x *is a variable or a constant, then* $x \in R_A$ *for all* A*.*

4. *Prove that if* t *is an element of* R_A *and* t *reduces to* t'*, then* t' *is an element of* R_A*.*

5. *Let t be a term of the form $(u_1\ u_2)$ such that all the one-step reducts of t are in R_A. We want to prove that t is in R_A.*

   Prove that t strongly terminates.

   Prove that if $A = \iota$ or $A = o$, then t is in R_A.

   Prove that if $A = B \to C$, then t is in R_A.

6. *Let t_1 be a term in $R_{A \to B}$ and t_2 a term in R_A. We want to prove that $(t_1\ t_2)$ is in R_B.*

   Prove that the term t_1 and t_2 strongly terminates.

   Let n_1 be the maximum length of a reduction sequence issued from the term t_1 and n_2 be the maximum length of a reduction sequence issued from t_2.

   Prove by induction on $n_1 + n_2$ that $(t_1\ t_2)$ is in the set R_B.

7. *Let t be a term of type A and σ be a substitution mapping each variable of type B to an element of R_B. Prove that σt is in R_A.*

8. *Let t be a term of type A. Prove that t strongly terminates.*

Exercise 2 *Consider the model of Simple type theory defined as follows $\mathcal{M}_\iota = \{7\}$, $\mathcal{M}_o = \{0, 1\}$, $\mathcal{M}_{A \to B} = \mathcal{M}_A \to \mathcal{M}_B$, that is the set of all functions from A to B.*

- *$\hat{\varepsilon}$ is the identity function,*
- *$\hat{\alpha}_{A,B}$ is the function mapping f and a to $f(a)$,*
- *$\hat{K}_{A,B}$ is the function mapping a and b to a,*
- *$\hat{S}_{A,B,C}$ is the function mapping f, g and a to $f\ a\ (g\ a)$,*
- $\hat{\dot{\top}} = \tilde{\top} = 1$,
- $\hat{\dot{\bot}} = \tilde{\bot} = 0$,
- $\hat{\dot{\wedge}} = \tilde{\wedge}$,
- $\hat{\dot{\vee}} = \tilde{\vee}$,
- $\hat{\dot{\Rightarrow}} = \tilde{\Rightarrow}$,
- *$\hat{\dot{\forall}}_A$ is the function mapping f to the minimum of $f(a)$ for a in $\mathcal{M}_A$,*
- *$\hat{\dot{\exists}}_A$ is the function mapping f to the maximum of $f(a)$ for a in $\mathcal{M}_A$.*

1. *Prove that $\mathcal{M}$ is a model of Simple type theory.*

2. *Equality is defined by the rule*

$$x = y \longrightarrow \dot{\forall} c\,((c\,x) \dot{\Rightarrow} (c\,y))$$

prove that $[\![\varepsilon(t = u)]\!]_\rho = 1$ *if and only if* $[\![t]\!]_\rho = [\![u]\!]_\rho$.

Let E *be the extensionality axiom*

$$\forall f : (\iota \to \iota) \forall g : (\iota \to \iota)((\forall x : \iota\ (fx) = (gx)) \Rightarrow f = g)$$

Prove that E *is valid in this model*

Prove that $\neg E$ *is not provable in Simple type theory.*

3. *Build a model of Simple type theory where* E *is not valid.*

   Prove that E *is not provable in Simple type theory.*