MPRI 2012-13 Cours 2-7-1

Examination November 26^{th} 2012

2:30 hours.

1 Warm-up

A fellow student claims to have written terms of the following types in type theory. For each case, tell whether this is possible.

$$\begin{array}{lcll} p_1 & : & \Pi n : nat.\Sigma m : nat.m = n + n & \textit{Possible} \\ p_2 & : & \Pi n : nat.\Sigma m : nat.n = m + m & \textit{Impossible} \\ p_3 & : & \Sigma x : nat.S(x + x) = 11 & \textit{Possible} \end{array}$$

what is the normal form of $\pi_1(p_3)$? *It is 5*

2 Impredicative encoding

Given two natural numbers x and y, we say that $R(x, y)$ if and only if there exists a natural number i such that $x = 2^i \cdot y$.

We want to represent the relation R in Higher-Order Logic (HOL, aka Church's simple type theory).

a) What is a natural type for R in HOL ?
It is $R : \iota \rightarrow \iota \rightarrow o$

b) Give a possible definition for R in HOL.

$$R \equiv \lambda x^{\iota}.\lambda y^{\iota}.\forall P : \iota \rightarrow o.(P\ x) \Rightarrow (\forall z : \iota.(P\ z) \Rightarrow (P\ 2.z)) \Rightarrow (P\ x)$$

c) Give a proof of $R(12, 3)$ is your encoding.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(P\ 3); \forall z : \iota.(P\ z) \Rightarrow (P\ 2.z) \vdash (P\ 3)}}{(P\ 3); \forall z : \iota.(P\ z) \Rightarrow (P\ 2.z) \vdash (P\ 2.3)}}{(P\ 3); \forall z : \iota.(P\ z) \Rightarrow (P\ 2.z) \vdash (P\ 2.2.3)}}{(P\ 3); \forall z : \iota.(P\ z) \Rightarrow (P\ 2.z) \vdash (P\ 2.2.2.3)} \quad \dfrac{}{\cdots \vdash 2.2.2.3 = 12}}{(P\ 3); \forall z : \iota.(P\ z) \Rightarrow (P\ 2.z) \vdash (P\ 12)}}{\vdash (P\ 3) \Rightarrow (\forall z : \iota.(P\ z) \Rightarrow (P\ 2.z)) \Rightarrow (P\ 12)}}{\vdash R(12, 3)}$$

d) What is the asymptotic size of a proof of $R(a \cdot 2^i, a)$ in your encoding ?
We see that the full writing the integer as $2.2.2. \ldots 2.a$ *is of size* $O(i \cdot a)$. *Because of the* i *uses of the assumption, the proof is of size* $O(i^2 \cdot a)$.

3 Computational encoding

a) In Martin-Löf's type theory, define a function D for double, such that : $D : nat \rightarrow nat$ and $(D\ n)$ computes $2 \cdot n$.

$$D \equiv \lambda x : nat.R(x, 0, \lambda p.\lambda r.S(S\ r))$$

b) Define the relation R in Martin-Löf's type theory.
We also define the exponention function:

$$DD \equiv \lambda x : nat.R(x, 1, \lambda p.\lambda r.(D\ r)$$

then

$$R \equiv \lambda x.\lambda y.\Sigma i : nat.x = y.(DD\ i).$$

c) Give a proof-term of $R(12, 3)$ for this encoding in type theory.

$$(2, refl(12))$$

d) What is the asymptotic size of a proof of $R(a \cdot 2^i, a)$ in this setting ?

The size of the representation of a, that is a even if we are not too careful (it can be squeezed to $log(a)$ *if we need to make it small.)*

4 Simply typed λ-terms

We are considering simple types, where $\alpha, \beta, \gamma \ldots$ are distinct atomic types.

What are the closed λ-terms of type $\alpha \to \alpha$?

only $\lambda x^\alpha.x^\alpha$

What are the closed λ-terms of type $\alpha \to (\alpha \to \alpha) \to \alpha$?

The Church numerals, that is the terms of the form : $\lambda x^\alpha.\lambda f^{\alpha\to\alpha}.(f\ \ldots(f\ x)\ldots)$

Are there terms of the following type ? which ones ?

$\alpha \to \beta$

No

$\alpha \to (\alpha \to \gamma) \to \gamma$

Yes : $\lambda x^\alpha.\lambda f^{\alpha\to\gamma}.(f\ x)$

$\alpha \to \beta \to (\alpha \to \gamma) \to (\beta \to \gamma) \to \gamma$

Yes : $\lambda x^\alpha.\lambda y^\beta.\lambda f^{\alpha\to\gamma}.\lambda g^{\beta\to\gamma}.(f\ x)$ *and* $\lambda x^\alpha.\lambda y^\beta.\lambda f^{\alpha\to\gamma}.\lambda g^{\beta\to\gamma}.(g\ y)$

5 Terms in system F

Are there closed normal terms of the following types in system F ? If so, which ones ?

$\forall\alpha.\alpha \to \alpha$

$\Lambda\alpha.\lambda x : \alpha.x$

$\forall\alpha.\alpha \to \alpha \to \alpha$

$\Lambda\alpha.\lambda x : \alpha.\lambda y : \alpha.x$ and $\Lambda\alpha.\lambda x : \alpha.\lambda y : \alpha.y$

$\forall\alpha.\alpha$

Nothing : this is the empty type

$\forall\alpha.(T \to \alpha) \to \alpha$ (where T is some closed type; the answer may depend upon T).

Only when T *is inhabited (by closed terms). If* $t : T$ *then we have* $\Lambda\alpha.\lambda f : T \to \alpha.(f\ t)$

6 Well-foundedness

We work in Higher-Order Logic. We have some given type T and a binary relation over it $R : T \to T \to o$.

We are given the following definition :

$$A \quad : \quad T \to o$$
$$A \quad \equiv \quad \lambda z : T.\forall P : T \to o, (\forall x : T, (\forall y : T, R\ x\ y \to P\ y) \to P\ x) \to P\ z.$$

We want to understand this definition.

a) Show that when $\forall y : T, \neg(R\ z\ y)$ holds, then $(A\ z)$ holds.

Since we have $\forall y : T, \neg(R\ z\ y)$*, we also have* $(\forall y : T, R\ z\ y \to P\ y)$*. So :*

$$(\forall x : T, (\forall y : T, R\ x\ y \to P\ y) \to P\ x)$$

implies

$$(\forall y : T, R\ z\ y \to P\ y) \to P\ z$$

which allows us to deduce $P\ z$*.*

b) Show that when $(R\ z\ z)$ holds, then $(A\ z)$ is false.

This one is a little tricky and tedious. Here is one possible way.

We have $(R\ z\ z)$ *and* $(A\ z)$ *and need to show* $\bot$*. We instantiate* $(A\ z)$ *on the property* $\lambda x.(R\ x\ x) \Rightarrow \bot$*. This gives us :*

$$(\forall x.(\forall y.R\ y\ x \Rightarrow \neg R\ y\ y) \Rightarrow \neg R\ x\ x) \Rightarrow \neg R\ z\ z$$

So we can conclude, if we prove :

$$\forall x.(\forall y.R\ y\ x \Rightarrow \neg R\ y\ y) \Rightarrow \neg R\ x\ x$$

This means we need to prove $\bot$ *given :* x*,* $R\ x\ x$ *and* $\forall y.R\ y\ x \Rightarrow \neg R\ y\ y$*.*

We do this by using the last assumption, where we take x *for* y*.*

c) We have an infinite sequence $x_1, x_2, \ldots, x_n, \ldots$ such that $(R\ x_i\ x_{i+1})$ holds. Explain why $(A\ x_1)$ should not be true. Can you describe how this argument can be formalized (without excessive detail though).

It works by taking a sequence $u : nat \to nat$*, but is a little tedious indeed. I will give a Coq encoding.*

d) A friend explains that $(A\ z)$ means there is no infinite sequence starting from z such that $z > x_1 > x_2 > \cdots > x_n \ldots$ where $x > y$ stands for $(R\ y\ x)$.

Does this seem true to you ? Can you comment or elaborate ?

Indeed, the property A *is the standard way to exoress that a relation is well-founded.* $A(x)$ *is the impredicative way to define the inductive property given by :*

$A(x)$ *holds iff any* y *"smaller" than* x *verifies* $A(y)$*.*

Which is the same as defining: "a term t is strongly normalizing iff all its reducts are strongly normalizing.