MPRI 2012-13 Cours 2-7-1

Examination November 26^{th} 2012

2:30 hours.

1 Warm-up

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

$$p_1 \quad : \quad \Pi n : nat.\Sigma m : nat.m = n + n$$
$$p_2 \quad : \quad \Pi n : nat.\Sigma m : nat.n = m + m$$
$$p_3 \quad : \quad \Sigma x : nat.S(x + x) = 11 \qquad \text{what is the normal form of } \pi_1(p_3) \text{ ?}$$

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 ?

b) Give a possible definition for R in HOL.

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

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

3 Computational encoding

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

b) Define the relation R in Martin-Löf's type theory.

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

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

4 Simply typed λ-terms

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

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

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

Are there terms of the following type ? which ones ?

$\alpha \to \beta$

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

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

5 Terms in system F

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

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

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

$\forall alpha.\alpha$

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

$$\begin{array}{rcl} A & : & T \to o \\ A & \equiv & \lambda z : T.\forall P : T \to o, (\forall x : T, (\forall y : T, R\ y\ x \to P\ y) \to P\ x) \to P\ z. \end{array}$$

We want to understand this definition.

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

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

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).

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 ?