Foundations of Computer Software: Exercise 4

January 27, 2012

Exercise 4-1

Prove the theorem `greater` as follows.

```
Require Import Omega.
Theorem greater:
   forall x:nat, {y:nat | y>x}.
Proof.
  intro.
  exists (x+1).
  omega.
Qed.
```

If you run the following command, you will get a program code. What is it?

```
Extraction greater.
```

Check the proof of the theorem `greater` by running the following command.

```
Print greater.
```

Which part of the proof corresponds to the program code obtained by the Extraction command?

Exercise 4-2

Complete the proof of the theorem below, which means that for every natural number n, there exists m such that $2m \leq n \leq 2m + 1$. You need to load libraries by running "Require Import Arith" and "Require Import Omega" in advance.

```
Theorem div2:
  forall n:nat,
```

```
     {m:nat | 2*m <= n <= 2*m+1}.
Proof.
induction n.
exists 0.
omega.

inversion IHn.
case (eq_nat_dec (2*x) n).
(* case for 2*x=n *)
intro.
exists x.
omega.

(* case for 2*x <> n *)
... (* Fill this part *)
Qed.
```

Run the following command, and check that you get will a program for computing the quotient of m by 2.

```
Recursive Extraction div2.
```

Note: "Recursive Extraction" does not seem to work well for Coqide of version 8.3pl2. Use "Extraction" instead in that case, or update your Coq to 8.3pl3. To save the program in a file, you can instead run:

```
Extraction <filename> div2.
```

In Coqide, you probably have to specify the absolute path of the file name (otherwise the program will be saved in the default directory).

Exercise 4-3

Complete the proof of the theorem, and obtain a program code that computes the quotient and remainder of m divided by n.

```
Theorem div:
  forall m n:nat,
   n>0 ->
     { x:nat*nat | let (q, r) := x in m = q*n+r /\ 0 <= r <n}.
Proof.
intros.
induction m.
(* base case *)
```

```
exists (0, 0).
omega.

(* induction step *)
intros.
inversion IHm.
induction x. (* decompose pair x *)

(* case analysis on b (= m mod n) *)
case (eq_nat_dec (b+1) n).

(* case for b+1 = n *)
... (* fill this part *)

(* case for b+1 <> n*)
... (* fill this part *)
Qed.
```

Exercise 4-4 (optional)

Prove that for any non-zero natural numbers m and n, there exists a greatest common divisor of m and n. Extract a program that computes the greatest common divisor from the proof.