The University of Waikato
Department of Computer Science
Dr. Robi Malik

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

COMP 340-08B

Reasoning about Programs

Assignment 6

In this assignment, you will complete the proof of the Euclidean Algorithm that was started in Assignment 5. The algorithm is given by the following Java program, and is claimed to compute the greatest common divider (GCD) for all pairs of non-negative integers x and y, unless both inputs are 0.

```
int gcd(int x, int y)
{
  if (y == 0) {
    return x;
  } else {
    return gcd(y, x % y);
  }
}
```

This assignment is to be done using the RISC ProofNavigator, which is installed in the Linux labs. Please download the theory file `comp340-ass6.pn` from the COMP 340-08B course home page in Moodle at

`http://elearn.waikato.ac.nz/course/view.php?id=2567`

and use it for the following exercises. This file contains the needed propositions from the previous assignment, plus some new conjectures to be attacked now.

Exercise 1 **(8 marks)**

As a first step, some properties of the greatest common divider (GCD) of two non-negative integers need to be established. Given the axioms

$$(\mathbf{GCD}_{\text{divides}}) \quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (\gcd(x,y) \mid x \wedge \gcd(x,y) \mid y)$$

$$(\mathbf{GCD}_{\max}) \quad \forall d{:}\,\mathbb{N}, x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (d \mid x \wedge d \mid y \rightarrow \gcd(x,y) \geq d)$$

and using results about the "divides" relation from assignment 5, prove the following properties.

a) $(\mathbf{GCD}_{\text{nat}}) \quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ \gcd(x,y) \geq 1$
Hint. Use $(\mathbf{DIV}_1)$.

b) $(\mathbf{GCD}_0) \quad \forall x{:}\,\mathbb{N}\ (x \neq 0 \rightarrow \gcd(x,0) = x)$
Hint. Remember that, instead of proving $A = B$, it sometimes is easier to prove $A \leq B \wedge B \leq A$.

c) $(\mathbf{GCD}_{\text{self}}) \quad \forall x{:}\,\mathbb{N}\ (x \neq 0 \rightarrow \gcd(x,x) = x)$

d) $(\mathbf{GCD}_{\text{leq}}) \quad \forall v{:}\,\mathbb{N}, w{:}\,\mathbb{N}, x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (\forall d{:}\,\mathbb{N}\ (d \mid v \wedge d \mid w \leftrightarrow d \mid x \wedge d \mid y) \rightarrow \gcd(v,w) \leq gcd(x,y))$

e) $(\mathbf{GCD}_{\text{eq}}) \quad \forall v{:}\,\mathbb{N}, w{:}\,\mathbb{N}, x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (\forall d{:}\,\mathbb{N}\ (d \mid v \wedge d \mid w \leftrightarrow d \mid x \wedge d \mid y) \rightarrow \gcd(v,w) = gcd(x,y))$
Hint. Prove this using $(\mathbf{GCD}_{\text{leq}})$ and use it for the following proofs.

f) $(\mathbf{GCD}_{\text{comm}}) \quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ \gcd(x,y) = \gcd(y,x)$

g) $(\mathbf{GCD}_{\text{plus}}) \quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ \gcd(x,y) = \gcd(x+y,y)$
Hint. Use $(\mathbf{GCD}_{\text{eq}})$, $(\mathbf{DIV}_{\text{plus}})$, and $(\mathbf{DIV}_{\text{minus}})$.

h) $(\mathbf{GCD}_{\text{minus}}) \quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (x \geq y \rightarrow \gcd(x,y) = gcd(x-y,y))$

Exercise 2 **(8 marks)**

As a second step, the result about subtraction needs to be lifted to the modulo operation. This is possible after some preparation, because modulo can be calculated by repeated subtraction. Using the axiom

$$(\mathbf{MOD})\quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (y \neq 0 \to x \bmod y < y \wedge \exists q{:}\,\mathbb{N}\ x = q \cdot y + x \bmod y)$$

prove the following properties.

a) $(\mathbf{MOD}_0)\quad \forall x{:}\,\mathbb{N}\ (x \neq 0 \to 0 \bmod x = 0)$

b) $(\mathbf{MOD}_{\mathrm{less}})\quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (x < y \to x \bmod y = x)$

c) $(\mathbf{GCD}_{\mathrm{minusn}})\quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}, n{:}\,\mathbb{N}\ (x \geq n \cdot y \to \gcd(x,y) = \gcd(y, x - n \cdot y))$

d) $(\mathbf{GCD}_{\mathrm{mod}})\quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (y \neq 0 \to \gcd(x,y) = \gcd(y, x \bmod y))$

Exercise 3 **(6 marks)**

Finally, to prove the `gcd` algorithm correct, the function $\gcd_{\mathrm{impl}}$ is defined by

$$(\mathbf{GCDIMPL})\quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ \ \gcd_{\mathrm{impl}}(x,y) = \textbf{if } y = 0 \textbf{ then } x \textbf{ else } \gcd_{\mathrm{impl}}(y, x \bmod y) \textbf{ endif}$$

and proven to give the same result as the $\gcd$ function for all acceptable inputs. This needs to be done by *strong induction* on the smaller of the two inputs. The smaller of the two inputs is y, except maybe for the first call.

Strong induction differs from regular induction in that the inductive hypothesis does not just consider one number n, but also all numbers less or equal to n. This kind of induction is not directly supported by ProofNavigator, but can easily be emulated through normal induction. To do so, prove the conjecture $(\mathbf{GCD}_{\mathrm{implaux1}})$ using induction on y and case distinction on $n = 0$, and instantiate it to get $(\mathbf{GCD}_{\mathrm{implaux2}})$.

This proves the algorithm correct for all cases where the input satisfies $x \geq y$. This result can be generalised using case distinction on $x \geq y$, producing the final result $(\mathbf{GCD}_{\mathrm{impl}})$.

Therefore, to complete the verification of the `gcd` algorithm, prove the following:

a) $(\mathbf{GCD}_{\mathrm{implaux1}})\quad \forall n{:}\,\mathbb{N}, x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (n \leq y \wedge x \geq n \wedge x \neq 0 \to \gcd_{\mathrm{impl}}(x,n) = \gcd(x,n))$

b) $(\mathbf{GCD}_{\mathrm{implaux2}})\quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (x \geq y \wedge x \neq 0 \to \gcd_{\mathrm{impl}}(x,y) = \gcd(x,y))$

c) $(\mathbf{GCD}_{\mathrm{impl}})\quad \forall x{:}\,\mathbb{N}, y{:}\,\mathbb{N}\ (x \neq 0 \vee y \neq 0 \to \gcd_{\mathrm{impl}}(x,y) = \gcd(x,y))$

Exercise 4 **(8 marks)**

Write down proofs in textual form for two of the conjectures listed below. Clearly describe the crucial steps of these proofs, and explain why the claim follows from the premises available.

$$(\mathbf{GCD}_{\mathrm{leq}})\quad (\mathbf{GCD}_{\mathrm{minusn}})\quad (\mathbf{GCD}_{\mathrm{mod}})\quad (\mathbf{GCD}_{\mathrm{implaux1}})\quad (\mathbf{GCD}_{\mathrm{impl}})$$

Verification **(10 marks)**

Each student needs to book a verification time with the lecturer before the due date. Bookings can be made during the lab session on Friday 22 August 2008 from 9:00–10:00 in Computing Laboratory 7 (R G.19), or by e-mail.

Submission

The RISC ProofNavigator will save your proofs in a directory called `comp340-08b-ass6`. Please pack this directory into a `.tar.gz` archive using the command

```
tar czf comp340-08b-ass6.tar.gz comp340-08b-ass6
```

and submit the archive through the assignment submission system in Moodle. In addition, please put your written answers to exercise 4 into the box marked **COMP340** in front of room G 1.15, and be sure to book a verification time before the due date.

Verification is a required component of this assignment. Students that fail to book a verification time or do not show up for verification cannot be awarded any marks for this assignment.

Due date: Wednesday, 10th September 2008, 17:00