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 5

As a first step towards verification of the Euclidean Algorithm, we have to verify several properties of integer multiplication and division.

This assignment is to be done using the RISC ProofNavigator, which is installed in the Linux labs. Please download the theory file `comp340-ass5.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.

Exercise 1 (8 marks)

Given the axioms

$$(\mathbf{MULT}_{0a}) \quad \forall x\colon \mathbb{N} \quad 0 \cdot x = 0$$
$$(\mathbf{MULT}_{succ}) \quad \forall x\colon \mathbb{N}, y\colon \mathbb{N} \quad (x+1) \cdot y = x \cdot y + y$$

prove the following properties of integer multiplication.

a) $(\mathbf{MULT}_{1a}) \quad \forall x\colon \mathbb{N} \quad 1 \cdot x = x$

b) $(\mathbf{MULT}_{1b}) \quad \forall x\colon \mathbb{N} \quad x \cdot 1 = x$

Hint. This and several of the following properties are proved by induction on x.

c) $(\mathbf{MULT}_{0b}) \quad \forall x\colon \mathbb{N} \quad x \cdot 0 = x$

d) $(\mathbf{MULT}_{nat}) \quad \forall x\colon \mathbb{N}, y\colon \mathbb{N} \quad x \cdot y \geq 0$

e) $(\mathbf{MULT}_{dist}) \quad \forall x\colon \mathbb{N}, y\colon \mathbb{N}, z\colon \mathbb{N} \quad (x+y) \cdot z = x \cdot z + y \cdot z$

f) $(\mathbf{MULT}_{assoc}) \quad \forall x\colon \mathbb{N}, y\colon \mathbb{N}, z\colon \mathbb{N} \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$

g) $(\mathbf{MULT}_{mon0}) \quad \forall x\colon \mathbb{N}, y\colon \mathbb{N} \quad (x \neq 0 \rightarrow x \cdot y \geq y)$

Hint. Use $(\mathbf{MULT}_{dist})$ to establish that the result of multiplying two non-negative integers is a non-negative integer.

h) $(\mathbf{MULT}_{mon1}) \quad \forall x\colon \mathbb{N}, y\colon \mathbb{N}, z\colon \mathbb{N} \quad (z \neq 0 \wedge x \cdot z \geq y \cdot z \rightarrow x \geq y)$

Exercise 2 (7 marks)

Using the properties of multiplication from exercise 1, and given the definition of the "divides" relation for non-negative integers,

$$(\mathbf{DIV}) \quad \forall x\colon \mathbb{N}, y\colon \mathbb{N} \quad (x \mid y \leftrightarrow \exists n\colon \mathbb{N} \;\; y = n \cdot x)$$

prove the following properties.

Hint. The `divides` predicate is completely defined and can be *expanded* using the `expand` command.

a) $(\mathbf{DIV}_0) \quad \forall x\colon \mathbb{N} \quad x \mid 0$

b) $(\mathbf{DIV}_1) \quad \forall x\colon \mathbb{N} \quad 1 \mid x$

c) $(\mathbf{DIV}_{\text{self}}) \quad \forall x\colon \mathbb{N} \quad x \mid x$

d) $(\mathbf{DIV}_{\text{plus}}) \quad \forall d\colon \mathbb{N}, x\colon \mathbb{N}, y\colon \mathbb{N} \quad (d \mid x \wedge d \mid y \;\rightarrow\; d \mid (x + y))$

e) $(\mathbf{DIV}_{\text{minus}}) \quad \forall d\colon \mathbb{N}, x\colon \mathbb{N}, y\colon \mathbb{N} \quad (d \mid x \wedge d \mid y \wedge x \geq y \;\rightarrow\; d \mid (x - y))$

f) $(\mathbf{DIV}_{\text{mult}}) \quad \forall d\colon \mathbb{N}, x\colon \mathbb{N}, y\colon \mathbb{N} \quad (d \mid y \;\rightarrow\; d \mid x \cdot y)$

g) $(\mathbf{DIV}_{\text{less}}) \quad \forall d\colon \mathbb{N}, x\colon \mathbb{N} \quad (x \neq 0 \wedge d \mid x \rightarrow d \leq x)$

Verification (5 marks)

This assignment will be verified during the tutorial session on Friday 22 August 2008 from 9:00–10:00 in Computing Laboratory 7 (R G.19). You will be asked to complete one of the proofs in front of the lecturer. If you cannot attend on 22 August, please arrange an alternative verification time with the lecturer before the due date.

Submission

The RISC ProofNavigator will save your proofs in a directory called `comp340-08b-ass5`. Please pack this directory into a `.tar.gz` archive using the command

```
tar czf comp340-08b-ass5.tar.gz comp340-ass5
```

and submit the archive through the assignment submission system in Moodle at

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

Due date: Wednesday, 20th August 2007, 17:00