COMP340-08B Reasoning About Programs

12. Reasoning about Integers

Robi Malik

THE UNIVERSITY OF WAIKATO *Te Whare Wānanga o Waikato*
DEPARTMENT OF COMPUTER SCIENCE
TARI ROROHIKO

Euclidean Algorithm

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


Original Version of Euclidean Algorithm

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


A Property Greatest Common Dividers

Proposition

For any two integers x and y, it holds that

$$\mathrm{gcd}(x, y) \;=\; \mathrm{gcd}(y, x - y)$$

Proof

Let x and y be two integers. It suffices to show that every common divider of x and y also is a common divider of y and $x - y$, and vice versa.

Proving the Property continued

1. Let d be a common divider of x and y, i.e., d divides x and y. Since d divides both x and y, it holds that $x = nd$ and $y = md$ for some integers n and m. It follows that $x - y = (n - m)d$, i.e., d also divides $x - y$. Therefore, d is a common divider of y and $x - y$.
2. Let d be a common divider of y and $x - y$. Then $y = nd$ and $x - y = md$ for some integers m and n. It follows that $x = x - y + y = md + nd = (m + n)d$, i.e., d divides x. Therefore, d is a common divider of x and y. □

A Theory of the Integers

In this proof, several functions and relations regarding integers have been used (or will have to be used).

- $\cdot \;\; +$, $\mathrm{mod} \;\; \mathrm{gcd}$ — Binary function symbols
- $\mid$ ("divides"), $< \;\; \leq$ — Binary predicate symbols

Primitive Encoding of Integers

The theory of integers if based on the **primitive encoding**, represented by:

- Type predicate nat
- Constant symbol 0
- Unary function symbol s ("successor")

Axioms

- $\mathrm{nat}(0)$
- $\forall x\ (\mathrm{nat}(x) \rightarrow \mathrm{nat}(\mathrm{s}(x)))$

Axioms for the Integer Functions

Addition

$\forall x\ (\mathrm{nat}(x) \rightarrow 0 + x = x)$

$\forall x \forall y\ (\mathrm{nat}(x) \wedge \mathrm{nat}(y) \rightarrow \mathrm{s}(x) + y = \mathrm{s}(x + y))$

Multiplication

$\forall x\ (\mathrm{nat}(x) \rightarrow 0 \cdot x = 0)$

$\forall x \forall y\ (\mathrm{nat}(x) \wedge \mathrm{nat}(y) \rightarrow \mathrm{s}(x) \cdot y = x \cdot y + y)$

Modulus

$\forall x \forall y\ \ (\mathrm{nat}(x) \wedge \mathrm{nat}(y) \wedge y \neq 0 \rightarrow$
$\quad x \bmod y < y \wedge \exists n\ (\mathrm{nat}(n) \wedge x = n \cdot y + (x \bmod y)))$

Using Typed Quantification

More concise notation using typed quantification

$\forall x{:}\mathrm{N}\ \ 0 + x = x$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ \mathrm{s}(x) + y = \mathrm{s}(x + y)$

$\forall x{:}\mathrm{N}\ \ 0 \cdot x = 0$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ \mathrm{s}(x) \cdot y = x \cdot y + y$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ (y \neq 0 \rightarrow$
$\quad x \bmod y < y \wedge \exists n{:}\mathrm{N}\ x = n \cdot y + (x \bmod y))$

Axioms for Integer Comparisons

$\forall x{:}\mathrm{N}\ \ 0 < \mathrm{s}(x)$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ (x < y \rightarrow \mathrm{s}(x) < \mathrm{s}(y))$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ (x < y \rightarrow \neg(x = y \vee y < x))$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ (x \leq y \leftrightarrow x < y \vee x = y)$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ (x > y \leftrightarrow y < x)$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ (x \geq y \leftrightarrow x \leq y)$

Axiom for the "Divides" Predicate

$$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ (x \mid y \leftrightarrow \exists n{:}\mathrm{N}\ y = n \cdot x)$$

$x \mid y$ (read as "x divides y") means that y can be divided by x without remainder, or in other words that y is a multiple of x.

Axioms for the GCD

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ \mathrm{gcd}(x,y) \mid x$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}\ \ \mathrm{gcd}(x,y) \mid y$

$\forall x{:}\mathrm{N}, y{:}\mathrm{N}, d{:}\mathrm{N}\ \ (d \mid x \wedge d \mid y \rightarrow d \leq \mathrm{gcd}(x,y))$