COMP340-08B Reasoning About Programs

15. The Euclidean Algorithm

Robi Malik

THE UNIVERSITY OF WAIKATO
DEPARTMENT OF COMPUTER SCIENCE
TARI ROROHIKO

Original Version of Euclidean Algorithm

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


So far: Properties of Multiplication

$(\text{MULT}_{\text{zero}})$ $\forall x{:}\mathbb{N}\ \ x \cdot 0 = 0$

(MULT_{1a}) $\forall x{:}\mathbb{N}\ \ 1 \cdot x = x$

(MULT_{1b}) $\forall x{:}\mathbb{N}\ \ x \cdot 1 = x$

$(\text{MULT}_{\text{dist}})$ $\forall x{:}\mathbb{N}, y{:}\mathbb{N}, z{:}\mathbb{N}$
$(x + y) \cdot z = x \cdot z + y \cdot z$

$(\text{MULT}_{\text{assoc}})$ $\forall x{:}\mathbb{N}, y{:}\mathbb{N}, z{:}\mathbb{N}\ \ x \cdot (y \cdot z) = (x \cdot y) \cdot z$

$(\text{MULT}_{\text{mon2}})$ $\forall x{:}\mathbb{N}, y{:}\mathbb{N}\ \ (x \neq 0 \rightarrow x \cdot y \geq y)$

Proving Properties of the GCD

$(\text{GCD}_{\text{zero1}})$ $\forall x{:}\mathbb{N}\ \ (x \neq 0 \rightarrow \gcd(x, 0) = x)$

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

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

$(\text{GCD}_{\text{plus}})$ $\forall x{:}\mathbb{N}, y{:}\mathbb{N}\ \ \gcd(x, y) = \gcd(x, x+y)$

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

Properties of Dividers

(DIV_0) $\forall x{:}\mathbb{N}\ \ x \mid 0$

$(\text{DIV}_{\text{self}})$ $\forall x{:}\mathbb{N}\ \ x \mid x$

(DIV_1) $\forall x{:}\mathbb{N}\ \ 1 \mid x$

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

$(\text{DIV}_{\text{minus}})$ $\forall x{:}\mathbb{N}, y{:}\mathbb{N}, d{:}\mathbb{N}$
$(x \geq y \wedge d \mid x \wedge d \mid y \rightarrow d \mid (x - y))$

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

Axioms for the GCD

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

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

Example Proof

Proposition

(GCD$_{zero1}$) $\forall x{:}\mathbb{N}\ (x \neq 0 \rightarrow \gcd(x, 0) = x)$

Proof

Let $x_0 \neq 0$. It suffices to show that $\gcd(x_0, 0) \leq x_0$ and $\gcd(x_0, 0) \geq x_0$.

1. Note that $\gcd(x_0, 0) \mid x_0$ by axiom (GCD$_{divides}$), and since $x_0 \neq 0$, this implies $\gcd(x_0, 0) \leq x_0$.
2. Since $x_0 \mid x_0$ and $x_0 \mid 0$, x_0 is a common divider of x_0 and 0. According to axiom (GCD$_{max}$), this means that $\gcd(x_0, 0) \geq x_0$. □

Proving Equality of GCDs

Lemma

(GCD$_{eq}$) $\forall v{:}\mathbb{N}, w{:}\mathbb{N}, x{:}\mathbb{N}, y{:}\mathbb{N}$
$(\forall d{:}\mathbb{N}\ (d \mid v \wedge d \mid w \leftrightarrow d \mid x \wedge d \mid y) \rightarrow \gcd(v, w) = \gcd(x, y))$

Proving this lemma first makes it easier to prove

(GCD$_{minus}$) $\forall x{:}\mathbb{N}, y{:}\mathbb{N}$
$(y \geq x \rightarrow \gcd(x, y) = \gcd(y, x–y))$

and similar properties.

ProofNavigator Proof Script

```
scatter;
assume x_0<=gcd(x_0,0) AND x_0>=gcd(x_0,0);
scatter;
instantiate x_0,x_0,0 in tsu;
split 6pq;
goal amj;
scatter;
lemma DIV_self;
auto 4ay;
lemma DIV_0;
auto f2b;
instantiate 0,x_0 in o6k;
decompose;
lemma DIV_less;
instantiate gcd(x_0,0), x_0 in sod;
```

$\gcd(x_0, 0) \geq x_0$

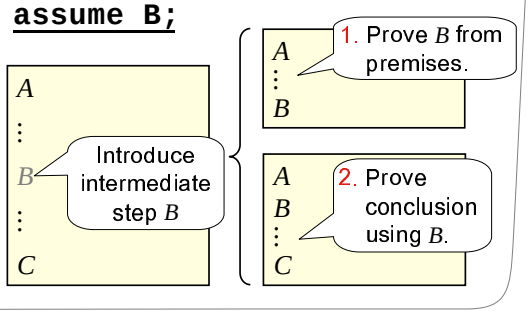
$\gcd(x_0, 0) \leq x_0$

Improved Euclidean Algorithm

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


Powerful Command

`assume B;`



Towards the Improved Algorithm

By induction from (GCD$_{minus}$) …

(GCD$_{minusn}$) $\forall x{:}\mathbb{N}, y{:}\mathbb{N}, n{:}\mathbb{N}$
$(x \geq n \cdot y \rightarrow \gcd(x, y) = \gcd(y, x - n \cdot y))$

And noting that $x \bmod y = x - n \cdot y$ for some $n \in \mathbb{N}$ …

(GCD$_{mod}$) $\forall x{:}\mathbb{N}, y{:}\mathbb{N}$
$(x \geq y \rightarrow \gcd(x, y) = \gcd(y, x \bmod y))$