Euclid's Algorithm

Note Title 11/12/2006

Roland Backhouse and Joao Ferreira

University of Nottingham

Definition The divides relation, denoted by $\backslash$, is a binary relation on integers defined by

$$[\ m \backslash n \ \equiv \ \langle \exists k :: k \times m = n \rangle\ ] \qquad \square$$

Properties

$\backslash$ is a partial ordering on the natural numbers. (i.e. reflexive, transitive and anti-symmetric).

$[\ 1 \backslash m\ ]$ (1 is the *least* element in the ordering)

$[\ m \backslash 0\ ]$ (0 is the *greatest* element in the ordering)

$[\ k \backslash m \wedge k \backslash n \ \equiv \ k \backslash (m-n) \wedge k \backslash n\ ] \qquad \square$

Definition The greatest common divisor of natural numbers m and n is a solution of the equation

$$x :: \langle \forall k :: k \backslash m \wedge k \backslash n \equiv k \backslash x \rangle \; . \qquad \square$$

Aside If $\preccurlyeq$ is a partial ordering, the *greatest lower bound (infimum)* of m and n is a solution of the equation

$$x :: \langle \forall k :: k \preccurlyeq m \wedge k \preccurlyeq n \equiv k \preccurlyeq x \rangle \; .$$

Eg. the minimum of numbers m and n is a solution of

$$x :: \langle \forall k :: k \leqslant m \wedge k \leqslant n \equiv k \leqslant x \rangle \; .$$

Greatest lower bounds need not exist. Eg. equality is a partial ordering, but the equation

$$x :: \langle \forall k :: k = m \wedge k = n \equiv k = x \rangle$$

has no solution when $m \neq n$. $\square$

Definition The greatest common divisor of natural numbers m and n is a solution of the equation

$$x :: \langle \forall k :: k \backslash m \wedge k \backslash n \equiv k \backslash x \rangle \; . \qquad \square$$

Observe :

$$\langle \forall k :: k \backslash m \wedge k \backslash m \equiv k \backslash m \rangle$$

$$\langle \forall k :: k \backslash m \wedge k \backslash 0 \equiv k \backslash m \rangle$$

(m solves the equation when $m = n$ or $0 = n$) .

$$\langle \forall k :: k \backslash m \wedge k \backslash n \equiv k \backslash n \wedge k \backslash m \rangle$$

(if a gcd of (m,n) exists, so too does the gcd of (n,m), and they are equal).

Euclid's Algorithm

Replacing specification by

$x,y :: \quad x = y \wedge \langle \forall k :: k \backslash m \wedge k \backslash n \equiv k \backslash x \wedge k \backslash y \rangle$

suggests invariant in Euclid's Algorithm:

$\{ 0 < m \wedge 0 < n \}$

$x,y := m,n$

; $\{$ Invariant: $\langle \forall k :: k \backslash m \wedge k \backslash n \equiv k \backslash x \wedge k \backslash y \rangle \wedge 0 < m \wedge 0 < n$
Bound: $x+y$ $\}$

do $x < y \rightarrow y := y - x$
$\square$ $y < x \rightarrow x := x - y$
od

$\{ x = y \wedge \langle \forall k :: k \backslash m \wedge k \backslash n \equiv k \backslash x \wedge k \backslash y \rangle \}$

Properties Euclid's algorithm shows, constructively, that *at least one* solution of equation

$$x :: \langle \forall k :: k \backslash m \wedge k \backslash n \equiv k \backslash x \rangle$$

exists when $0 < m$ and $0 < n$.
Earlier we observed solutions when $0 = m$ or $0 = n$.
It is easy to show — exercise — that, if a solution exists, it is unique. □

Conclusion: There is a binary function on natural numbers, which we will denote by the infix operator ∇, such that

$$[\ k \backslash m \wedge k \backslash n \equiv k \backslash\ m \nabla n\ ]\ .$$ □

Properties

$$[\ m \nabla n = n \nabla m\ ]$$

$$[\ m \nabla (n \nabla p) = (m \nabla n) \nabla p\ ]$$

(NB. not valid if $0 \nabla 0 = 0$ is disallowed by definition.)

$$[\ m \nabla n = m \equiv m \setminus n\ ]$$

□

These properties are not peculiar to gcd. They are instances of general properties of infima.

Theorem $m \nabla n$ is a linear combination of m and n.

Proof $m \nabla 0 = m = m \times 1 + 0 \times 1$.

$\{ 0 < m \wedge 0 < n \}$

$x, y := m, n \; ; \quad C := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

; { Invariant: $(x, y) = (m, n) \times C$

where $A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$ }

do $x < y \rightarrow (x, y) := (x, y) \times A \; ; \quad C := C \times A$

□ $y < x \rightarrow (x, y) := (x, y) \times B \; ; \quad C := C \times B$

od

$\{ x = y = m \nabla n \wedge (x, y) = (m, n) \times C \}$

□

Determine sufficient conditions for f to distribute thru ∇.

(a) $\quad f.0 = 0$.

(b)

$\{ 0<m \wedge 0<n \}$

$x,y := m,n$

do $\quad x<y \rightarrow y := y-x$

$\square \quad y<x \rightarrow x := x-y$

od

$\{ x = y = m \nabla n \quad \}$

$f.x \nabla f.y$ is a constant of Euclid's algorithm
if $\langle \forall x,y : 0<y<x : f.x \nabla f.y = f.(x-y) \nabla f.y \rangle$.

Equivalently,
$f.x \nabla f.y$ is a constant of Euclid's algorithm
if $\langle \forall x,y : 0<x \wedge 0<y : f.(x+y) \nabla f.y = f.x \nabla f.y \rangle$.
(Use range translation with $x := x+y$.)

Lemma (Ferreira) All functions f that satisfy

$$f.0 = 0$$

and $\langle \forall x,y :: \langle \exists a,b : a \nabla f.y = 1 : f(x+y) = a \times f.x + b \times f.y \rangle \rangle$

distribute through ∇.

Proof

Corollary The function f defined by $f.x = k^x - 1$ distributes through ∇.

Proof

$$f.0 = 0$$

and

$$\begin{aligned} & f.(x+y) \\ = & \quad \{ \text{definition} \} \\ & k^{x+y} - 1 \\ = & \quad \{ \text{arithmetic} \} \\ & 1 \times (k^x - 1) \;+\; k^x \times (k^y - 1) \end{aligned}$$

□