Note Title 11/12/2006

Algorithmic Problem Solving

FOP Away Day

17th January 2007

Edsger W. Dijkstra (1930-2002)

"Mathematics = The Art of Effective Reasoning"

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

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

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

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

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 $0 = n$) .

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 :

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

$x,y := m,n$

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

$\quad\text{Bound}:\ x+y\ \}$

$\textbf{do}\ \ x<y \rightarrow y := y-x$

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

$\textbf{od}$

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

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. $\square$

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

$$[\ k\backslash m \wedge k\backslash n \equiv k\backslash m\nabla n\ ] \quad . \qquad \square$$

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

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

od

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

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

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

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

Verification Condition

$$[\ (x,y) = (m,n) \times C$$

$$\Rightarrow\ (x,y) \times A = (m,n) \times (C \times A)\ ]$$

$$(x,y)\times A \;=\; (m,n)\times(C\times A)$$

$=$ { matrix multiplication is associative }

$$(x,y)\times A \;=\; ((m,n)\times C)\times A$$

$\Leftarrow$ { Leibniz }

$$(x,y) \;=\; (m,n)\times C\;.$$