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 \( \, \), is a binary relation on integers defined by
\[
\left[ \frac{m}{n} = \exists k :: k \times m = n \right] \tag{\Box}
\]

Properties

\( \, \) is a partial ordering (i.e. reflexive, transitive and anti-symmetric).
\[
\left[ \frac{1}{m} \right] \quad (1 \text{ is the least element in the ordering})
\]
\[
\left[ \frac{m}{0} \right] \quad (0 \text{ is the greatest element in the ordering})
\]
\[
\left[ \frac{k}{m} \land k \land n \equiv \frac{k \land (m-n)}{k \land n} \right] \quad \Box
\]
Definition  The greatest common divisor of natural
numbers \( m \) and \( n \) is a solution of the equation
\[
x :: \langle \forall k :: k\mid m \land k\mid n = k\mid x \rangle.
\]

Aside  If \( \leq \) is a partial ordering, the greatest lower
bound (infimum) of \( m \) and \( n \) is a solution of the equation
\[
x :: \langle \forall k :: k \leq m \land k \leq n = k \leq x \rangle.
\]

Eg. the minimum of numbers \( m \) and \( n \) is a solution of
\[
x :: \langle \forall k :: k \leq m \land k \leq n = k \leq x \rangle.
\]

Greatest lower bounds need not exist. Eg. equality is
a partial ordering, but the equation
\[
x :: \langle \forall k :: k = m \land k = n = k = x \rangle
\]
has no solution when \( m \neq n \).
Definition: The greatest common divisor of natural numbers \(m\) and \(n\) is a solution of the equation
\[ x = \langle \forall k :: k \mid m \land k \mid n = k \mid x \rangle. \]

Observe:
\[ \langle \forall k :: k \mid m \land k \mid m = k \mid m \rangle \]
\[ \langle \forall k :: k \mid m \land k \mid 0 = k \mid m \rangle \]

\(m\) solves the equation when \(m = n\) or \(0 = n\).
Euclid's Algorithm

Replacing specification by
\( x, y :: x = y \land \langle \forall k :: k \mid m \land k \mid n \Rightarrow k \mid x \land k \mid y \rangle \)
suggests invariant in Euclid's Algorithm:

\[
\{ 0 < m \land 0 < n \} \\
x, y := m, n \\
; \{ \text{Invariant: } \langle \forall k :: k \mid m \land k \mid n \Rightarrow k \mid x \land k \mid y \rangle \land 0 < m \land 0 < n \} \\
\quad \text{Bound: } x + y \\
\text{do } x < y \rightarrow y := y - x \\
\quad \text{if } y < x \rightarrow x := x - y \\
\text{od} \\
\{ x = y \land \langle \forall k :: k \mid m \land k \mid n \Rightarrow k \mid x \land k \mid y \rangle \} \}
Properties  Euclid’s algorithm shows, constructively, that at least one solution of equation

\[ x \sqsubseteq (\forall k \sqsubset k \mid m \land k \mid n \equiv k \mid x) \]

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. \(\Box\)

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

\[ [ k \mid m \land k \mid n \equiv k \mid m \triangledown n ] \]. \(\Box\)
Theorem \( m \triangledown n \) is a linear combination of \( m \) and \( n \).

Proof \[ m \triangledown 0 = m = m \times 1 + 0 \times 1. \]

\[
\{ 0 < m \land 0 < n \} \\
x, y := m, n \; ; \; C := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
\{ \text{Invariant:} \; (x, y) = (m, n) \times C \}
\]

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

\[
d \begin{array}{ll}
x < y \rightarrow & (x, y) := (x, y) \times A \; ; \; C := C \times A \\
y < x \rightarrow & (x, y) := (x, y) \times B \; ; \; C := C \times B \\
\end{array}
\]

\[
\{ x = y = m \triangledown n \land (x, y) = (m, n) \times C \} \]
\[
\{ \ (x, y) = (m, n) \times C \ \} \\
\\
(x, y) := (x, y) \times A ; \quad C := C \times A \\
\{ \ (x, y) = (m, n) \times C \ \} \\
\\
\textbf{Verification Condition} \\
\\
\left[ \ (x, y) = (m, n) \times C \\
\implies (x, y) \times A = (m, n) \times (C \times A) \ \right]
\[(x, y) \times A = (m, n) \times (C \times A)\]

\[
= \{ \text{matrix multiplication is associative} \}
\]

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

\[
\Leftarrow \quad \{ \text{Leibniz} \}
\]

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