Distributivity and the GCD

Note Title 14/01/2007

Goal: to determine sufficient conditions for a function f to distribute over the greatest common divisor, i.e.:

$$[\, f.(m \triangledown n) = f.m \triangledown f.n \,] \quad .$$

Note:

- variables m and n are naturals
- $f : \mathbb{N} \to \mathbb{N}$
- square brackets denote universal quantification over all free variables

Case $m=0 \vee n=0$

- For $m=0$, we have:

$$
\begin{aligned}
& f.(0 \triangledown n) = f.0 \triangledown f.n \\
= \quad & \{ [0 \triangledown n = n] \} \\
& f.n = f.0 \triangledown f.n \\
\Leftarrow \quad & \{ [0 \triangledown m = m] \} \\
& f.0 = 0 \quad .
\end{aligned}
$$

- Using the symmetry between m and n we have for $m=0 \vee n=0$:

$$f.(m \triangledown n) = f.m \triangledown f.n \quad \Leftarrow \quad f.0 = 0 \quad .$$

Case $m>0 \wedge n>0$

The greatest common divisor is the outcome of Euclid's Algorithm, defined for positive arguments as:

$$
\begin{array}{l}
\{0<m \ \wedge \ 0<n\} \\
x, y := m, n \\
\{\text{Invariant: } 0<x \wedge 0<y \wedge m \triangledown n = x \triangledown y\} \\
\textbf{do} \quad x>y \longrightarrow x := x-y \\
\Box \qquad y>x \longrightarrow y := y-x \\
\textbf{od} \\
\{0<x \ \wedge \ 0<y \ \wedge \ x=y=m \triangledown n\}
\end{array}
$$

Case $m>0 \wedge n>0$

Suppose we establish that $f.x \triangledown f.y$ is a constant of the loop body. Then:

- Initial value $(x,y := m,n)$:

  $$f.m \triangledown f.n$$

- On termination $(x,y := m \triangledown n \,,\, m \triangledown n)$:

  $$f.(m \triangledown n) \triangledown f.(m \triangledown n)$$

  which, by idempotency, is:

  $$f.(m \triangledown n)$$

Hence, we have $f.m \triangledown f.n = f.(m \triangledown n)$.

Case $m>0 \wedge n>0$

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

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

Lemma All functions f that satisfy $f.0 = 0$

and

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

distribute over $\triangledown$.

Proof

$$
\begin{aligned}
& f.(x+y) \triangledown f.y \\
= \quad & \{ \quad f.(x+y) = a \times f.x + b \times f.y \quad \} \\
& (a \times f.x + b \times f.y) \triangledown f.y \\
= \quad & \{ \quad [m + (a \times n) \triangledown n \;=\; m \triangledown n] \quad \} \\
& (a \times f.x) \triangledown f.y \\
= \quad & \{ \quad [(m \times p) \triangledown n = m \triangledown n \;\Leftarrow\; p \triangledown n = 1] \quad \} \\
& f.x \triangledown f.y \quad .
\end{aligned}
$$

Corollary The function f defined by $f.x = k^x - 1$ distributes over $\triangledown$.

Proof: $f.0 = 0$

and

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

Using previous Lemma $(a,b := 1, k^x)$ and the law $[1 \triangledown m = 1]$, we conclude that f distributes over $\triangledown$.

Using last corollary with $k=2$, we have that function $M.x = 2^x - 1$ (known as Mersenne Function) distributes over $\triangledown$.

$$
\begin{aligned}
& (2^m - 1) \triangledown (2^n - 1) = 1 \\
= \quad & \{ \text{distributivity} \} \\
& 2^{(m \triangledown n)} - 1 = 1 \\
= \quad & \{ \text{arithmetic} \} \\
& 2^{(m \triangledown n)} = 2 \\
= \quad & \{ \text{Leibniz and function } 2^x \text{ has inverse} \} \\
& m \triangledown n = 1 .
\end{aligned}
$$