Distributivity and the greatest common divisor

It is known that multiplication by a natural number distributes over the greatest common divisor. It is an important property that can be used to simplify arguments where both multiplication and the greatest common divisor are involved. A nice example is Netty van Gasteren's proof (see [Dij01]) of the theorem

(0) $[\ (m\times p)\triangledown n \ = \ m\triangledown n \quad \Leftarrow \quad p\triangledown n \ = \ 1\ ]$,

where variables m, n, and p are of type integer and $\triangledown$ is a natural-valued operator that stands for the greatest common divisor. We read $m\triangledown n$ as "m nabla n" and the square brackets denote universal quantification over all free variables. Netty's proof is as follows:

$$
\begin{array}{ll}
 & m\triangledown n \\
= & \{\quad p\triangledown n = 1 \text{ and } 1 \text{ is the unit of multiplication} \quad\} \\
 & (m\times(p\triangledown n))\ \triangledown\ n \\
= & \{\quad \text{multiplication by a natural number distributes over } \triangledown \\
 & \quad\ \ \text{and } \triangledown \text{ is associative} \quad\} \\
 & (m\times p)\ \triangledown\ (m\times n)\ \triangledown\ n \\
= & \{\quad (m\times n)\triangledown n = n \quad\} \\
 & (m\times p)\triangledown n \ .
\end{array}
$$

Remark Although m is an integer, we can safely apply the distributivity property in the second step, because we can freely change the sign of the arguments of $\triangledown$ — that is, $[\ (-m)\triangledown n \ = \ m\triangledown n\ ]$. **(End of Remark)**

Similar to the multiplication by a natural number, there are other functions that distribute over $\triangledown$. The goal of this note is to determine reasonable sufficient conditions for a natural-valued function f to distribute over $\triangledown$, i.e., for the following property to hold:

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

For simplicity's sake, we restrict all variables to naturals and extend the results to integers later. This implies that the domain of f is also restricted to the natural numbers.

Due to our general line of research, we want to prove (1) by exploiting invariants of Euclid's algorithm involving the function f. Recall that Euclid's algorithm can be written (for positive arguments m and n) as:

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

$x\,,y\ :=\ m\,,n;$

$\{$ **Invariant**: $0<x \ \wedge\ 0<y \ \wedge\ m\triangledown n = x\triangledown y\ \}$

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

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

od

$\{\ 0<x \ \wedge\ 0<y \ \wedge\ x = m\triangledown n \ \wedge\ y = m\triangledown n\ \}$

To determine an appropriate loop invariant, we take the right-hand side of (1) and we observe:

$$
\begin{array}{ll}
 & f.m \ \triangledown\ f.n \\
= & \{\quad \text{initially: } x = m \wedge y = n \quad\} \\
 & f.x \ \triangledown\ f.y \\
= & \{\quad \text{suppose that } f.x \ \triangledown\ f.y \text{ is invariant;} \\
 & \quad\ \ \text{on termination: } x = m\triangledown n \ \wedge\ y = m\triangledown n \quad\} \\
 & f.(m\triangledown n) \ \triangledown\ f.(m\triangledown n) \\
= & \{\quad \triangledown \text{ is idempotent} \quad\} \\
 & f.(m\triangledown n) \quad .
\end{array}
$$

Property (1) is thus established under the assumption that $f.x\triangledown f.y$ is an invariant of the loop body.

Remark "Invariants" in the literature are always boolean-valued functions of the program variables. But we see no reason why "invariants" shouldn't be of any type: for us, an *invariant* of a loop is simply a function of the program variables whose value is unchanged by execution of the loop body. In this case, the value is a natural number. **(End of Remark)**

The next step is to determine what condition on f guarantees that $f.x\triangledown f.y$ is indeed invariant. Noting the symmetry in the loop body between x and y, the condition is easily calculated to be

$$[\ f.(x-y)\ \triangledown\ f.y\ =\ f.x\ \triangledown\ f.y\ \ \Leftarrow\ \ 0<y<x\ ]\qquad .$$

Equivalently, by the rule of range translation ($x\ :=\ x+y$), the condition can be written as

(2) $[\ f.x\ \triangledown\ f.y\ =\ f.(x+y)\ \triangledown\ f.y\ \ \Leftarrow\ \ 0<x\ \wedge\ 0<y\ ]$.

Formally, this means that

$$\text{“ f distributes over } \triangledown \text{”}\quad \Leftarrow\quad (2)\quad .$$

Incidentally, the converse of this property is also valid:

$$(2)\ \Leftarrow\ \text{“ f distributes over } \triangledown \text{”}\quad .$$

To prove it, we use the theorem

(3) $[\ (m\ +\ a{\times}n)\ \triangledown\ n\quad =\quad m\ \triangledown\ n\ ]$,

and we calculate:

$$\begin{array}{ll} & f.(x+y)\ \triangledown\ f.y \\ = & \{\quad f \text{ distributes over } \triangledown \quad\} \\ & f.((x+y)\ \triangledown\ y) \\ = & \{\quad (3)\quad\} \\ & f.(x\ \triangledown\ y) \\ = & \{\quad f \text{ distributes over } \triangledown \quad\} \\ & f.x\ \triangledown\ f.y\quad . \end{array}$$

From the mutual implication we conclude that

$$\text{“ f distributes over } \triangledown \text{”}\quad \equiv\quad (2)\quad .$$

We have now reached a point where we can determine if a function distributes over $\triangledown$. However, since (2) still has two occurences of $\triangledown$, we want to refine it into simpler properties. Towards that end we turn our attentions to the condition

$$f.x\ \triangledown\ f.y\ =\ f.(x+y)\ \triangledown\ f.y\quad ,$$

and we try to calculate one side of it to the other. For instance, using theorem (3), it is immediate that any function that distributes over addition distributes over $\triangledown$ (note that this is the case of multiplication by a natural number). The proof is very simple:

$$\begin{array}{ll} & f.(x+y) \ \triangledown \ f.y \\ = & \{ \quad f \text{ distributes over addition} \quad \} \\ & (f.x + f.y) \ \triangledown \ f.y \\ = & \{ \quad (3) \quad \} \\ & f.x \ \triangledown \ f.y \ \ . \end{array}$$

In view of properties (3) and (0), we formulate the following lemma, which is a more general requirement:

Lemma 4 All functions f that satisfy

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

distribute over $\triangledown$.

Proof

$$\begin{array}{ll} & f.(x+y) \ \triangledown \ f.y \\ = & \{ \quad f.(x+y) \ = \ a \times f.x \ + \ b \times f.y \quad \} \\ & (a \times f.x \ + \ b \times f.y) \ \triangledown \ f.y \\ = & \{ \quad (3) \quad \} \\ & (a \times f.x) \ \triangledown \ f.y \\ = & \{ \quad a \ \triangledown \ f.y \ = \ 1 \quad \text{and} \quad (0) \quad \} \\ & f.x \ \triangledown \ f.y \ \ . \end{array}$$

Please note that since the discussion above is based on Euclid's algorithm, it only applies to positive arguments. We now investigate the case where m or n are 0. We have, for $m = 0$:

$$\begin{array}{ll} & f.(0 \triangledown n) \ = \ f.0 \ \triangledown \ f.n \\ = & \{ \quad [\ 0 \triangledown m = m \ ] \quad \} \\ & f.n \ = \ f.0 \ \triangledown \ f.n \\ = & \{ \quad f.n \text{ is a divisor of } f.0 \quad \} \\ & f.n \setminus f.0 \\ = & \{ \quad \text{definition} \quad \} \end{array}$$

$$\langle \exists k \ : \ k \in \mathbb{Z} \ : \ f.0 \ = \ k \times f.n \rangle$$
$$\Leftarrow \quad \{ \quad \text{obvious possibilities for } f.0 \text{ or for } f.n \quad \}$$
$$f.0 = 0 \ \vee \ f.n = 1 \ \vee \ f.n = f.0 \ \ .$$

Hence, using the symmetry between m and n we have, for $m = 0$ or $n = 0$:

(5) $\quad f.(m \triangledown n) \ = \ f.m \triangledown f.n \quad \Leftarrow \quad f.0 = 0 \ \vee \ f.n = 1 \ \vee \ f.n = f.0 \quad .$

The conclusion is that we can use (5) and Lemma 4 to prove that a natural-valued function with domain $\mathbb{N}$ distributes over $\triangledown$.

Example 0: the Fibonacci function

In [Dij90], Edsger Dijkstra proves that he Fibonacci function distributes over $\triangledown$. He does not use Lemma 4 explicitly, but he constructs the property

(6) $\quad fib.(x \ + \ y) \ = \ fib.(y \ - \ 1) \times f.x \ + \ fib.(x \ + \ 1) \times fib.y \quad ,$

and then, using the lemma

$$fib.y \triangledown fib.(y \ - \ 1) \ = \ 1 \quad ,$$

he concludes the proof. His calculation is the same as that in the proof of Lemma 4 but for particular values of a and b and with f replaced by fib . Incidentally, if we don't want to construct property (6) we can easily verify it using induction — more details are given in [GKP94].

Example 1: the Mersenne function

In this subsection we prove that, for all integers k and m such that $k^m > 0$, the function defined as

$$f.m \ = \ k^m - 1$$

distributes over $\triangledown$.

First, we observe that $f.0 = 0$. Next, we use Lemma 4. This means that we need to find integers a and b , such that

$$k^{m+n} - 1 \ = \ a \times (k^m - 1) \ + \ b \times (k^n - 1) \quad \wedge \quad a \triangledown (k^n - 1) = 1 \quad .$$

The most obvious instantiations for a are 1, k^n and $k^n - 2$. (That two consecutive numbers are coprime follows from (3).) Choosing $a = 1$, we calculate b :

$$k^{m+n} - 1 \;=\; (k^m - 1) \;+\; b{\times}(k^n - 1)$$
$=$ { arithmetic }
$$k^{m+n} - k^m \;=\; b{\times}(k^n - 1)$$
$=$ { multiplication distributes over addition }
$$k^m{\times}(k^n - 1) = b{\times}(k^n - 1)$$
$\Leftarrow$ { Leibniz }
$$k^m = b \quad .$$

We thus have

$$k^{m+n} - 1 \;=\; 1{\times}(k^m - 1) \;+\; k^m{\times}(k^n - 1) \quad \wedge \quad 1\triangledown(k^n - 1) = 1 \quad ,$$

and we use Lemma 4 to conclude that f distributes over $\triangledown$:

$$[\ (k^m - 1) \triangledown (k^n - 1) \quad = \quad k^{(m \triangledown n)} - 1\ ] \quad .$$

In result, the Mersenne function, which is defined as $2^m - 1$, distributes over $\triangledown$:

(7) $\quad [\ (2^m - 1) \triangledown (2^n - 1) \quad = \quad 2^{(m \triangledown n)} - 1\ ] \quad .$

A corollary of (7) is the property

$$[\ (2^m - 1)\triangledown(2^n - 1) \;=\; 1 \quad \equiv \quad m \triangledown n = 1\ ] \quad .$$

In words, two numbers $2^m - 1$ and $2^n - 1$ are coprime is the same as exponents m and n are coprime.

Extending the results to integers

A question that arises is whether we can extend the domain of the function f to the integer domain. To answer it, let us investigate when (1) holds for integer values. Assuming that m and n are integers, we calculate:

$$[\ f.(m \triangledown n) \;=\; f.m \;\triangledown\; f.n\ ]$$
$=$ { $[\ m \triangledown n \quad = \quad |m| \triangledown |n|\ ]$ }
$$[\ f.(|m| \triangledown |n|) \;=\; f.m \;\triangledown\; f.n\ ]$$
$=$ { f distributes over $\triangledown$ in the naturals }
$$[\ f.|m| \;\triangledown\; f.|n| \;=\; f.m \;\triangledown\; f.n\ ]$$
$\Leftarrow$ { Leibniz }
$$[\ f.|m| = f.m\ ] \quad .$$

We thus conclude that:

$$\begin{array}{ll} & \text{“ f distributes over } \triangledown \text{ in the integers”} \\ \Leftarrow & \text{“ f distributes over } \triangledown \text{ in the naturals”} \quad \wedge \quad [\ f.|m| = f.m\ ] \quad . \end{array}$$

Lemma 4 can be used to check if f distributes over $\triangledown$ in the naturals.

Acknowledgements

I thank Roland Backhouse, Alexandra Mendes, Arjan Mooij and Jeremy Weissmann for their valuable comments and help presenting parts of the note.

João Fernando Ferreira
May 8, 2007

School of Computer Science
University of Nottingham, Jubilee Campus
Wollaton Road, Nottingham
NG8 1BB
United Kingdom

joao@joaoferreira.org

References

[Dij90] Edsger W. Dijkstra. Fibonacci and the greatest common divisor. April 1990.

[Dij01] Edsger W. Dijkstra. Indirect equality enriched (and a proof by Netty). December 2001.

[GKP94] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1994.