KRML 95 -0

The Golden Rule of Positive Integers

K. Rustan M. Leino and Lyle Ramshaw

11 October 1999

Compaq Systems Research Center
130 Lytton Ave., Palo Alto, CA 94301, U.S.A.
{rustan,ramshaw}@pa.dec.com

Consider the well-known property, stated for any positive integers a and b, that

$$a \,\mathbf{gcd}\, b \cdot a \,\mathbf{lcm}\, b \;=\; a \cdot b \tag{0}$$

where **gcd** and **lcm** denote greatest common divisor and least common multiple, respectively.

To prove this property, we think of positive integers in terms of their prime factorizations. We define a function F from positive integers to functions from the primes to the naturals: for any positive integer x, function F satisfies

$$x \;=\; (\cdot\, p \;\mathbf{|}\; p \text{ is prime} \;::\; p^{F.x.p}\,) \tag{1}$$

where we have used a left-associative infix dot to denote function application. The right-hand side of this equation denotes the product, for all primes p, of p raised to the power of $F.x.p$. In other words, $F.x.p$ gives the exponent of prime p in the prime factorization of x. Note that F is one-to-one, since $F.x$ determines x by equation (1). (The fact that F exists follows from the existence of a prime number factorization of every positive integer.)

We will use common operators like $+$ on functions by defining them as pointwise extensions of the corresponding operations on the range of the functions. That is, for integer functions v and w, $v + w$ denotes the integer function whose values are the pointwise sums of v and w:

$$(\forall\, p \;::\; (v + w).p \;=\; v.p + w.p\,)$$

We will rely on context to distinguish between operating on functions and operating on values.

Now for the proof of the well-known property (0). For any positive integers a and b,

$$
\begin{array}{ll}
 & a \,\mathbf{gcd}\, b \cdot a \,\mathbf{lcm}\, b \;=\; a \cdot b \\
= & \quad \{ \text{ by definition of } F,\ (x = y) \;=\; (F.x = F.y) \quad \} \\
 & F.(a \,\mathbf{gcd}\, b \cdot a \,\mathbf{lcm}\, b) \;=\; F.(a \cdot b) \\
= & \quad \{ \text{ distribute } F \text{ over } \cdot :\ F.(x \cdot y) = F.x + F.y \quad \} \\
 & F.(a \,\mathbf{gcd}\, b) + F.(a \,\mathbf{lcm}\, b) \;=\; F.a + F.b \\
= & \quad \{ \text{ distribute } F \text{ over } \mathbf{gcd} \text{ and } \mathbf{lcm} :\ F.(x \,\mathbf{gcd}\, y) = F.x \,\mathbf{min}\, F.y \\
 & \qquad \text{and } F.(x \,\mathbf{lcm}\, y) = F.x \,\mathbf{max}\, F.y \quad \} \\
 & F.a \,\mathbf{min}\, F.b + F.a \,\mathbf{max}\, F.b \;=\; F.a + F.b \\
= & \quad \{ \text{ property of } \mathbf{min} \text{ and } \mathbf{max} \quad \} \\
 & true
\end{array}
$$

The penultimate line,

$$F.a \,\mathbf{min}\, F.b + F.a \,\mathbf{max}\, F.b \;=\; F.a + F.b \tag{2}$$

is similar in structure to a beautiful, but less well-known, equation from predicate calculus known as the Golden Rule: for any booleans X and Y,

$$X \wedge Y \;\equiv\; X \vee Y \;\equiv\; X \;\equiv\; Y \tag{3}$$

To understand what this rule says, one needs to remember that equality on booleans is associative. Thus, one may choose to read equation (3) as

$$(X \wedge Y \;\equiv\; X \vee Y) \;\equiv\; (X \;\equiv\; Y)$$

We use the symbol $\equiv$ rather than $=$ to remind ourselves of this associativity.

So what makes the Golden Rule similar in structure to equation (2)? The operations $\wedge$ and $\vee$ are the meet and join operations, respectively, of the lattice of booleans. In the total ordering of integers, the meet and join operations are **min** and **max**, respectively.

But the Golden Rule doesn't look entirely like equation (2), because where equation (2) uses $+$, the Golden Rule uses $\equiv$. We will now show how to rewrite the Golden Rule into an equivalent form that will make it look much more like equation (2).

In predicate calculus, not only does equality, $\equiv$, associate with itself, but it also associates with discrepance, $\not\equiv$. Discrepance, which is defined for any booleans X and Y by

$$(X \;\not\equiv\; Y) \;\equiv\; (\neg X \;\equiv\; Y)$$

is perhaps better known as exclusive or, that is, xor. Because $\equiv$ and $\not\equiv$ associate, the definition of $\equiv$ can equivalently be written as

$$X \;\not\equiv\; Y \;\equiv\; \neg X \;\equiv\; Y$$

Because negation is an involution, that is, negation is its own inverse, $\equiv$ and $\not\equiv$ have another useful property: in any expression whose top-level operators are $\equiv$ and $\not\equiv$, one can change any $\equiv$ into a $\not\equiv$ and change any $\not\equiv$ into an $\equiv$, provided the number of such changes is even. For example, here are four equivalent ways of denoting the same thing:

$$
\begin{array}{l}
W \equiv X \equiv Y \equiv Z \\
W \not\equiv X \not\equiv Y \equiv Z \\
W \not\equiv X \equiv Y \not\equiv Z \\
W \equiv X \not\equiv Y \not\equiv Z
\end{array}
$$

Since xor can be construed as addition modulo 2, we are now done: the Golden Rule can be stated as

$$X \wedge Y \not\equiv X \vee Y \equiv X \not\equiv Y$$

using the same structure as equation (2). Thus, if the equation for booleans is known by a name as fancy as the Golden Rule, perhaps the well-known property that links greatest common divisors and least common multiples should be known as the Golden Rule of Positive Integers.