Rational Number Arithmetic

George E. Collins

September 23, 1998

A rational number in SACLIB is represented by a numerator and a denominator, which are relatively prime. To make the representation unique, the denominator is required to be positive. The rational number 0, however, is an exception. It is represented by the integer 0. This treatment of 0 is standard throughout SACLIB; the zero element of every algebraic domain is represented by the integer 0. The numerator and denominator are the first and second elements, respectively, of a list of length two.

The SACLIB algorithms for rational number addition and multiplication are significant improvements of the obvious algorithms that were originated by Henrici in 1956, [1]. Henrici's purpose was to avoid having numerators and denominators that would not fit into one computer word. But when working with infinite precision integers, the important advantage is speedup.

Let us begin with multiplication. Let $w = (u/u')(v/v')$. Let $d_1 =$gcd(u, v'), $d_2 =$gcd(v, u'). Let $u_1 = u/d_1$, $v'_1 = v'/d_1$, $v_2 = v/d_2$ and $u'_2 = u'/d_2$. Then $w = u_1 v_2 / u'_2 v'_1$ in lowest terms because each of the two factors in thenumerator is relatively prime to each of the two factors in the denominator. This Henrici's method, and it is implemented in the SACLIB program RNPROD. This method is much faster than the more direct method of computing the gcd of uv and $u'v'$ and then dividing each product by their gcd.

Now let $w = (u/u') + (v/v')$. Let $d_1 =$gcd$(u', v'), u'_1 = u'/d_1, v'_1 = v'/d_1$. Then $w = (uv'_1 + vu'_1)/u'_1 v'$. The reduction of this fraction to lowest terms can also be optimized as follows. Let $t = uv'_1 + vu'_1$ and observe that $u'_1 v' = d_1 u'_1 v'_1$. Let p be any prime that divides both t and u'_1. Then p certainly divides vu'_1 so p must also divide uv'_1. But $u \perp u'$ so $u \perp u'_1$ and hence $p|v'_1$. But $u'_1 \perp v'_1$, a contradiction. We have proved that $t \perp u'_1$. Similarly $t \perp v`_1$. Therefore gcd$(t, d_1 u`_1 v'_1) =$gcd(t, d_1). This is Henrici's addition algorithm, and it is implemented in RNSUM. The method applies in the same way to subtraction; see RNDIF.

The multiplicative inverse of a nonzero rational number u/u' is obviously u'/u if $u > 0$, and is $-u'/-u$ if $u < 0$. See RNINV. Division is performed by inverting the divisor and then multiplying; see RNQ.

References

[1] P. Henrici. A Subroutine for Computations with Rational Numbers. JACM, **3** (1956), 6-9.