Fast multiplication of large integers

Vincent Lefèvre and Paul Zimmermann

29 May 1998

Several multiprecision libraries are available to multiply large integers. Here we focus on three implementations.

GNU MP, or **GMP** for short, is a free multi-precision C library designed by Torbjörn Granlund, and available from `http://www.matematik.su.se/~tege/gmp`. We used two versions of GMP in this review: GMP 2.0.2 is the latest public release, GMP-980312 is a prerelease kindly made available to us by Torbjörn Granlund. GMP implements Karatsuba's algorithm (it is used up from 12 limbs, except when squaring), but not (yet) FFT.

Apfloat is a C++ library available from `http://www.hut.fi/~mtommila/apfloat`, and designed by Mikko Tommila. We used here version 1.40. An originality of Apfloat is that it can use different basic types to represent the different *limbs* — in the GMP terminology — of a large integer: 32-bit integers, 64-bit integers, single- or double-precision floating point numbers. Apfloat implements FFT.

Threeway is an implementation designed by Vincent Lefèvre `vlefevre@ens-lyon.fr`. It uses the double-precision floating point numbers as limbs, storing 50 bits in each limb, and using the IEEE standard to split a limb into two parts. Threeway implements both Karatsuba's algorithm and its variant which cuts each number in three — instead of two for Karatsuba.

Here are the times needed by each library to multiply two random integers of one million bits on an Alpha, a Pentium II under Linux, and an UltraSparc:

	Alpha/OSF	PC/Linux	UltraSparc/Solaris
frequency	300Mhz	300Mhz	143Mhz
GMP 2.0.2	3.0s	3.7s	12.8s
GMP-980312	2.1s	2.7s	11.0s
Apfloat	(1)	1.4s	10.0s (2)
Threeway	(3)	2.4s	4.6s

(1) error at compilation (`try_catch_expr not supported`), both with version 1.33 and 1.40
(2) with 32-bit integers (12s with single-precision floating point numbers, 17s with 64-bit integers, and 32s with double-precision floating point numbers)
(3) problem with directed roundings

The following three figures compare the multiplication of GMP, Apfloat and Threeway on Alpha, PC/Linux and UltraSparc. The x-axis gives the number of bits of the operands, and the y-axis gives the times in seconds.

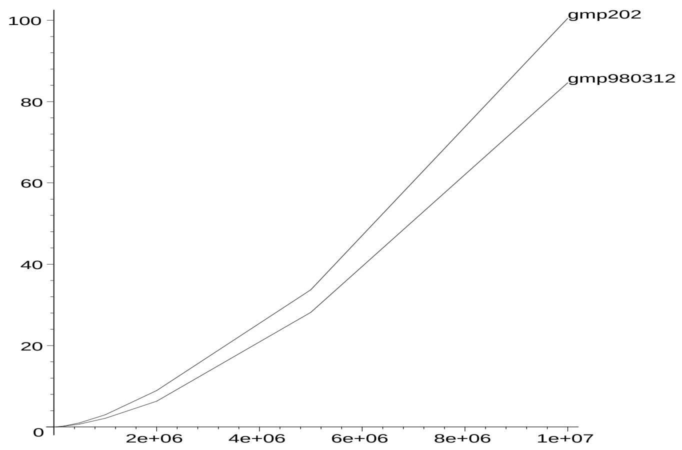

Figure 1: Results on the DecAlpha

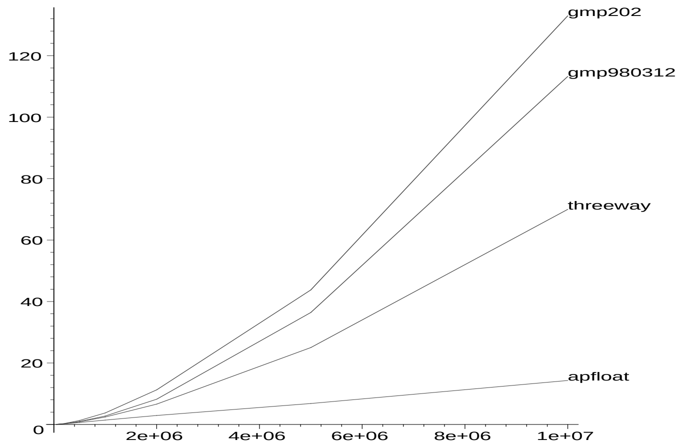

Figure 2: Results on a PC/Linux

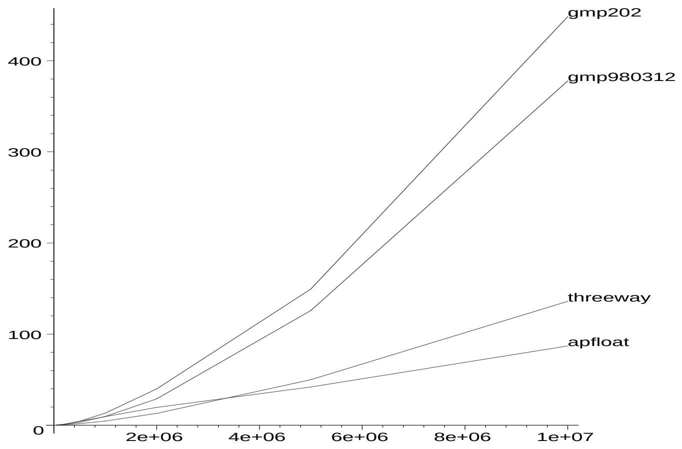

Figure 3: Results on the UltraSparc