Easy Multiple-Precision Divisors and Word-RAM Constants

Torben Hagerup

Abstract. For integers $b \geq 2$ and $w \geq 1$, define the (b, w) *cover size* of an integer A as the smallest nonnegative integer k such that A can be written in the form $A = \sum_{i=1}^{k} (-1)^{\sigma_i} b^{\ell_i} d_i$, where σ_i, ℓ_i and d_i are nonnegative integers and $0 \leq d_i < b^w$, for $i = 1, \ldots, k$. We study the efficient execution of arithmetic operations on (multiple-precision) integers of small (b, w) cover size on a word RAM with words of w b-ary digits and constant-time multiplication and division. In particular, if A is an n-digit integer and B is a nonzero m-digit integer of (b, w) cover size k, then AB and $\lfloor A/B \rfloor$ can be computed in $O(1 + (kn + m)/w)$ time. Our results facilitate a unified description of word-RAM algorithms operating on integers that may occupy a fraction of a word or several words.
As an application, we consider the fast generation of integers of a special form for use in word-RAM computation. Many published word-RAM algorithms divide a w-bit word conceptually into equal-sized fields and employ full-word constants whose field values depend in simple ways on the field positions. The constants are either simply postulated or computed with ad-hoc methods. We describe a procedure for obtaining constants of the following form in constant time: The ith field, counted either from the right or from the left, contains $g(i)$, where g is a constant-degree polynomial with integer coefficients that, disregarding mild restrictions, can be arbitrary. This general form covers almost all cases known to the author of word-RAM constants used in published algorithms.