A SYSTOLIC ALGORITHM FOR INTEGER GCD COMPUTATION

R. P. BRENT AND H. T. KUNG

Abstract

It is shown that the greatest common divisor of two n-bit integers (given in the usual binary representation) can be computed in time $O(n)$ on a linear systolic array of $O(n)$ cells.

Comments

Only the Abstract is given here. The full paper appeared as [3]. The method used is a variant of the binary Euclidean algorithms considered earlier in [1]. For the extended integer GCD problem, see [5]. The (easier) polynomial GCD problem is considered in [2, 4].

References

1. R. P. Brent, "Analysis of the binary Euclidean algorithm," in *New Directions and Recent Results in Algorithms and Complexity* (edited by J. F. Traub), Academic Press, New York, 1976, 321–355. MR 54#14417, 55#11701; Zbl 363.00013, 373.68040. rpb037.
2. R. P. Brent and H. T. Kung, "Systolic VLSI arrays for polynomial GCD computation", *IEEE Trans. on Computers* C–33 (1984), 731–736. rpb073.
3. R. P. Brent and H. T. Kung, "A systolic VLSI array for integer GCD computation", in *ARITH-7, Proc. Seventh Symposium on Computer Arithmetic* (edited by K. Hwang), IEEE/CS Press, 1985. Also appeared as Report TR-CS-82-11, Department of Computer Science, ANU, December 1982 (revised April 1984); and as Report CMU-CS-84-135, Department of Computer Science, Carnegie-Mellon University, April 1984, 33 pp. rpb077.
4. R. P. Brent and H. T. Kung, "Systolic VLSI arrays for linear-time GCD computation", in *VLSI 83* (edited by F. Anceau and E. J. Aas), North-Holland, Amsterdam, 1983, 145–154. rpb082.
5. A. W. Bojanczyk and R. P. Brent, "A systolic algorithm for extended GCD computation", *Comput. Math. Applic.* 14 (1987), 233–238. MR 88m:11110. rpb096.

(Brent) Centre for Mathematical Analysis, Australian National University, Canberra

(Kung) Department of Computer Science, Carnegie-Mellon University, Pittsburgh, PA 15213, USA

1991 *Mathematics Subject Classification.* Primary 68Q22; Secondary 11A05, 65Y05, 65Y10, 68Q25, 68Q35.

Key words and phrases. Euclidean algorithm, greatest common divisor, GCD, systolic algorithm, parallel algorithm, linear-time algorithm.

H. T. Kung was sponsored in part by the Office of Naval Research under Contract N00014-80-C-0236, NR 048-659.

 rpb077a typeset using $\mathcal{AMS}$-LaTeX