SYSTOLIC VLSI ARRAYS FOR POLYNOMIAL GCD COMPUTATION

R. P. BRENT AND H. T. KUNG

Abstract

The problem of finding a *greatest common divisor* (GCD) of any two nonzero polynomials is fundamental to algebraic and symbolic computations, as well as to the decoder implementation for a variety of error-correcting codes. This paper describes new systolic arrays that can lead to efficient VLSI solutions to both the GCD problem and the extended GCD problem.

Comments

Only the Abstract is given here. The full paper appeared as [1]. For the (more difficult) integer GCD problem, see [2, 3].

References

[1] R. P. Brent and H. T. Kung, "Systolic VLSI arrays for polynomial GCD computation", *IEEE Trans. on Computers* C–33 (1984), 731–736. Also appeared as Report TR-CS-82-05, Department of Computer Science, ANU; and as Report CMU-CS-82-118, Department of Computer Science, CMU, May 1982, 16 pp. rpb073.

[2] 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. rpb077.

[3] 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

1991 *Mathematics Subject Classification.* Primary 68Q22; Secondary 11A05, 11T55, 65Y05, 65Y10, 68Q25, 68Q35, 94B35.

Key words and phrases. Algorithms, error-correcting codes, finite field, greatest common divisor, GCD, special-purpose hardware, systolic arrays, VLSI.

Manuscript received August 4, 1982; revised December 12, 1983.

This work was supported in part by the Office of Naval Research under Contracts N00014-76-C-0370, NR 044-422 and N00014-80-C-0236, NR 048-659, in part by the National Science Foundation under Grant MCS 78-236-76, and in part by the Defense Advanced Research Projects Agency, ARPA Order 3597, monitored by the Air Force Avionics Laboratory under Contract F33615-81-K-1539.

rpb073a typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX.