ANALYSIS OF THE BINARY EUCLIDEAN ALGORITHM

RICHARD P. BRENT

Abstract

The classical Euclidean algorithm for finding the greatest common divisor of two positive integers has been exhaustively analyzed since the time of Gauss. The theory of binary Euclidean algorithms is less well-developed. We analyze the "right-shift" binary Euclidean algorithm of Silver and Terzian [11] and Stein [12]. In particular, we show that the expected number of iterations for uniformly distributed inputs in $\{1, 2, 3, \ldots, N\}$ is asymptotic to $K \log_2 N$ as $N \to \infty$, where $K \simeq 0.706$.

We introduce another binary Euclidean algorithm, the "left-shift" algorithm, and consider its expected behaviour on random inputs. The expected number of iterations for the left-shift algorithm is slightly greater than for the right-shift algorithm, but the left-shift algorithm is worth considering for use on a computer with a "normalize" instruction, as then the left-shifting loop may be replaced by a single instruction. Either of the binary algorithms could be implemented in hardware (or microcode) with approximately the same expense as integer division.

Comments

Only the Abstract is given here. The full paper appeared as [2]. Binary Euclidean algorithms were later applied to give linear-time systolic algorithms for integer GCD computation [6, 8, 7, 1]. The polynomial GCD problem [5] is simpler because of the lack of carries.

The probabilistic assumptions of [2] were given a rigorous foundation by Vallée [13, 14].

Minor Errata

In the definition of $D_0(x)$ on the last line of page 326

$$D_0(x) = 0 \text{ should be replaced by } D_0(x) = 1 .$$

In equation (6.3) on page 342, the term

$$-\frac{x}{2(1+x)} \text{ should be replaced by } -\frac{1}{2(1+x)} .$$

Major Errata

Some of the results are incorrect. For example, (3.1), (3.29), (3.34), (3.35) are wrong (though a close approximation to the truth). Further details are given in [3, 4]. See also [10, §4.5.2].

1991 *Mathematics Subject Classification.* Primary 68Q25; Secondary 65Y10, 68Q35.

Key words and phrases. Euclidean algorithm, binary Euclidean algorithm, greatest common divisor, GCD, continued fraction, left shift, right shift, systolic algorithm.

This research was supported in part by the National Science Foundation under Grant MCS75-222-55 and the Office of Naval Research under Contract N0014-76-C-0370, NR 044-422.

The author thanks Frank de Hoog and Don Knuth for their assistance and encouragement.

 rpb037a typeset using $\mathcal{AMS}$-LaTeX.

Acknowledgements

Thanks to Don Knuth, Philippe Flajolet and Brigitte Vallée for their assistance in correcting and extending my 1976 results [2].

References

[1] A. W. Bojanczyk and R. P. Brent, "A systolic algorithm for extended GCD computation", *Comput. Math. Applic.* 14 (1987), 233–238. rpb096.

[2] 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. Also appeared as a Technical Report, Department of Computer Science, Carnegie-Mellon University (June 1976), 35 pp. Extended abstract appeared in *SIGSAM Bulletin* (May 1976). rpb037.

[3] R. P. Brent, "Twenty years' analysis of the binary Euclidean algorithm", *Proc. Symposium in Celebration of the Work of C. A. R. Hoare*, Oxford, Sept. 1999, to appear. rpb183.

[4] R. P. Brent, *Further analysis of the Binary Euclidean algorithm*, Tech. Report, Oxford University Computing Laboratory, to appear. rpb183tr

[5] R. P. Brent and H. T. Kung, "Systolic VLSI arrays for polynomial GCD computation", *IEEE Trans. on Computers* C–33 (1984), 731–736. rpb073.

[6] 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.

[7] 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.

[8] R. P. Brent, H. T. Kung and F. T. Luk, "Some linear-time algorithms for systolic arrays", in *Information Processing 83* (edited by R.E.A. Mason), North-Holland, Amsterdam, 1983, 865–876. rpb079.

[9] D. E. Knuth, *The Art of Computer Programming, Volume 2*, Addison-Wesley, Menlo Park, first edition, 1969.

[10] D. E. Knuth, *The Art of Computer Programming, Volume 2*, Addison-Wesley, Menlo Park, third edition, 1997.

[11] R. Silver and J. Terzian, unpublished, 1962. See Knuth [9, §4.5.2–4.5.3].

[12] J. Stein, "Computational problems associated with Racah algebra", *J. Comput. Phys.* 1 (1967), 397–405.

[13] B. Vallée, The complete analysis of the binary Euclidean algorithm, *Proc. ANTS'98*, *Lecture Notes in Computer Science* 1423, Springer-Verlag, 1998, 77–94.

[14] B. Vallée, Dynamics of the binary Euclidean algorithm: functional analysis and operators, manuscript, Feb. 1998 (to appear in *Algorithmica*). `http://www.info.unicaen.fr/~brigitte/Publications/bin-gcd.ps`

Australian National University and Carnegie-Mellon University