THE AREA-TIME COMPLEXITY OF BINARY MULTIPLICATION

R. P. BRENT AND H. T. KUNG

Abstract

The problem of performing multiplication of n-bit numbers on a chip is considered. Let A denote the chip area and T the time required to perform multiplication. By using a model of computation which is a realistic approximation to current and anticipated LSI or VLSI technology, it is shown that

$$\left(\frac{A}{A_0}\right)\left(\frac{T}{T_0}\right)^{2\alpha} \geq n^{1+\alpha}$$

for all $\alpha \in [0, 1]$, where A_0 and T_0 are positive constants which depend on the technology but are independent of n. The exponent $1 + \alpha$ is the best possible. A consequence of this result is that binary multiplication is "harder" than binary addition. More precisely, if $(AT^{2\alpha})_M(n)$ and $(AT^{2\alpha})_A(n)$ denote the minimum area-time complexity for n-bit binary multiplication and addition, respectively, then

$$\begin{aligned}\frac{(AT^{2\alpha})_M(n)}{(AT^{2\alpha})_A(n)} &= \begin{cases}\Omega(n^{1-\alpha}) & \text{for } 0 \leq \alpha \leq 1/2\\ \Omega(n^{\alpha}/\log^{2\alpha} n) & \text{for } 1/2 < \alpha \leq 1\\ \Omega(n/\log^{2\alpha} n) & \text{for } \alpha > 1\end{cases}\\ &= \Omega(n^{1/2}) \qquad \text{for all } \alpha \geq 0.\end{aligned}$$

1991 *Mathematics Subject Classification.* Primary 68Q35; Secondary 65Y05, 68M07, 68Q25.

Key words and phrases. Area-time complexity, binary multiplication, chip design, chip layout, circuit design, combinational logic, chip complexity, lower bounds, VLSI.

CR Categories. 5.25, 6.1, 6.32.

Received August 1979; revised March 1980; accepted April 1980.

This research was supported in part by the National Science Foundation under Grant MCS 78-236-76 and the Office of Naval Research under Contracts N00014-76-C-0370 and N00014-80-C-0236. Most of this work was carried out at the Australian National University while H. T. Kung was there as a Visiting Fellow during May 1979.

rpb055a typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX.

Comments

Only the Abstract is given here. The full paper appeared as [3]. Similar results for the case $\alpha = 1$ were obtained independently by Abelson and Andreae [1] (using a more restrictive model than ours). A preliminary version, which contains some additional material on upper bounds, appeared as [2]. For an extension of the results to problems with only a 1-bit output, see [4].

Let

$$\mu(N) = |\{ij \mid 0 \le i < N,\ 0 \le j < N\}|$$

be the number of distinct products of nonnegative integers each less than N. As pointed out in the Corrigendum to [3], our conjecture [3, page 528] that

$$\lim_{N\to\infty} \frac{\mu(N)\log_2 \log N}{N^2} = 1$$

is false. In fact, it follows from a result of Pál Erdős [5] that

$$\mu(N) = \frac{N^2}{(\log N)^{c+o(1)}},$$

where

$$c = 1 - (1 + \ln\ln 2)/\ln 2 \simeq 0.086.$$

Fortunately, none of the results of [3] depend on the conjecture.

Acknowledgement. We thank P. Erdős, D. J. Newman, A. M. Odlyzko and C. Pomerance for bringing the result [5] to our attention.

References

[1] H. Abelson and P. Andreae, "Information transfer and area-time trade-offs for VLSI multiplication", *Communications of the ACM* 23 (1980), 20–23.

[2] R. P. Brent and H. T. Kung, "The chip complexity of binary arithmetic" *Proc. Twelfth Annual ACM Symposium on the Theory of Computing*, ACM, New York, 1980, 190–200. rpb053.

[3] R. P. Brent and H. T. Kung, "The area-time complexity of binary multiplication", *Journal of the ACM* 28 (1981), 521–534. CR 22#38242, MR 82i:68027. Corrigendum: *ibid* 29 (1982), 904. MR 83j:68046. Also appeared as Report TR-CS-79-05, Department of Computer Science, ANU; and as Report TR CMU-CS-79-136, Department of Computer Science, CMU (July 1979), 25 pp. rpb055.

[4] R. P. Brent and L. M. Goldschlager, "Some area-time tradeoffs for VLSI", *SIAM J. on Computing* 11 (1982), 737–747. MR 83k:68024. rpb064.

[5] P. Erdős, *Leningrad Universitet Vestnik (Matematika, Mekhanika, Astronomiia)* 15 (1960), 41–49.

(Brent) Department of Computer Science, Australian National University, Canberra

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