FASTER MULTIPLICATION OF MEDIUM LARGE NUMBERS VIA THE ZECKENDORF REPRESENTATION

Vassil S. Dimitrov
Center for CAD, Technical University of Plovdiv, Bulgaria

Borislav D. Donevsky
IAMI, Technical University of Sofia, P.O. Box 384, Bulgaria
(*Submitted June 1993*)

INTRODUCTION

Multiplication of two integers is a fundamental computational problem. Various authors have found nearly linear-time algorithms for integer multiplication; the best such result is that of Schonhage and Strassen (in [1]), who showed that the product of two n-bit numbers may be computed in $O(n \log n \log\log n)$ steps. Their algorithm involves a recursive application of the Fast Fourier Transform (FFT) and is quite intricate. However, even the simpler multiplication algorithms based on the FFT are not used in practice, unless enormous numbers are involved.

Another multiplication method, published by Karatsuba and Ofman (in [1]) uses $O(n^{1.585})$ operations and outperforms classical multiplication when n exceeds 1200 (i.e., about 360 decimal digits).

In 1972 Zeckendorf [8] introduced a representation of the integers as a sum of generalized Fibonacci numbers defined by the relation

$$\begin{aligned} &F_0^{(r)} = 0,\ F_1^{(r)} = 1,\ F_j^{(r)} = 2^{j-2}, && j = 2, 3, \dots, r-1, \\ &F_i^{(r)} = F_{i-1}^{(r)} + F_{i-2}^{(r)} + \cdots + F_{i-r}^{(r)}, && i \ge r. \end{aligned} \tag{1}$$

The Fibonacci, Tribonacci [5], [7], and Quadranacci [6] numbers arise as a special case of (1) by letting $r = 2$, $r = 3$, and $r = 4$, respectively. Capocelli [3] gives an efficient algorithm for deriving the Zeckendorf representation of integers.

This paper compares the classical multiplication, Karatsuba-Ofman, and Schonhage-Strassen algorithms and multiplication with the Zeckendorf representation, and shows that medium sized numbers can be multiplied (on average) more quickly using the Zeckendorf Quadranacci representation.

ZECKENDORF REPRESENTATION OF THE INTEGERS

Recently, the Zeckendorf representation of the integers has been shown to be a useful alternative to the binary representation. Each nonnegative integer N has the following unique Zeckendorf representation in terms of Fibonacci numbers of degree r (see [7], [8]):

$$N = \alpha_2 F_2^{(r)} + \alpha_3 F_3^{(r)} + \cdots + \alpha_j F_j^{(r)}, \tag{2}$$

where $\alpha_i \in \{0, 1\}$ and $\alpha_i \alpha_{i-1} \alpha_{i-2} \alpha_{i-3} \dots \alpha_{i-r+1} = 0$ (no r consecutive α's are 1).

Like the binary representation of integers, the Zeckendorf representation can be written as a string of 0's and 1's, i.e., $\alpha_j \alpha_{j-1} \alpha_{j-2} \dots \alpha_3 \alpha_2$.

As was proved by Borel [2], almost all numbers have an equal number of zeros and ones in their standard binary representation. More generally we have that, if g is an integer greater than one, then

$$t = \frac{w_1(t)}{g} + \frac{w_2(t)}{g^2} + \cdots, \quad 0 \le t \le 1,$$

where every digit $w_i(t)$ is in $\{0, 1, \ldots, g-1\}$. Borel's theorem states: For almost all t $(0 \le t \le 1)$,

$$\lim_{n\to\infty} \frac{F_n^{(k)}(t)}{n} = \frac{1}{g},$$

where $F_n^{(k)}$ denotes the number of those w from the first n, which are equal to k, $0 \le k \le g-1$.

Such a property is true for the binary representation of integers, that is, the proportions of 0's in strings of length n and the proportion of 1's in strings of length n are both equal to 1/2. In the Zeckendorf representation, this rule does not hold. From [4], we have the following result on the asymptotic proportion of ones.

Theorem 1: The proportion of 1's in the Zeckendorf representation of integers is

$$A_n^{(r)} = \frac{1}{\omega^{(r)}} - \frac{r}{(\omega^{(r)})^{r+1}} \cdot \frac{\omega^{(r)} - 1}{[(r+1)\omega^{(r)} - 2r]} + O(1/n), \tag{3}$$

which tends to 1/2 as r increases. $\omega^{(r)}$ is a real root of the equation

$$x^r - x^{r-1} - \cdots - 1 = 0.$$

This root lies between 1 and 2.

In Table 1 some values for $A_\infty^{(r)}$ are presented (see [4]).

TABLE 1. Asymptotic Values of $A_\infty^{(r)}$

r	2	3	4	5	6	7	8
$A_\infty^{(r)}$	0.2764	0.3816	0.4337	0.4621	0.4782	0.4875	0.4929

The roots $\omega^{(r)}$ form a strictly increasing sequence. That is,

$$1.618\ldots < \omega^{(2)} < \omega^{(3)} < \cdots < 2.$$

Zeckendorf representation of integers requires more space than the binary representation, see Table 2.

TABLE 2. Zeckendorf Space/Binary Space

r	2	3	4	5	6	7
$\log_{\omega^{(r)}} 2$	1.44	1.13	1.05	1.02	1.01	1.005

Let us fix the dynamic range of the input data to be n-bits in the binary number system (BNS). The number of one's for n-bit BNS numbers in the Zeckendorf representation will have an average at

$$N_{\text{ones}}^{(r)} = \log_{\omega^{(r)}} 2 \cdot A_{\infty}^{(r)} \cdot n.$$

The initial values of the function $Z(r) = N_{\text{ones}}^{(r)} / n$ are printed in Table 3.

TABLE 3. Average Proportion of One's for n-bit BNS Numbers in the Proposed Number System

r	2	3	4	5	6	7	8	9
$Z(r)$	0.398	0.434	0.458	0.474	0.484	0.494	0.497	0.499

It is clear that the representation using classical Fibonacci numbers requires 20% fewer 1's in comparison with BNS, which can be employed in many practical situations.

MULTIPLICATION OF THE NUMBERS IN ZECKENDORF REPRESENTATION

Let us consider the multiplication of two integers having a Zeckendorf representation. The multiplier may have only $A_{\infty}^{(r)}$ of its digits equal to 1, but it has $\log_{\omega^{(r)}} 2$ more digits. Hence, multiplication using Zeckendorf representation involves $A_{\infty}^{(r)} \cdot \log_{\omega^{(r)}} 2$ more additions than in the BNS case. Therefore, there are $A_{\infty}^{(r)} \cdot (\log_{\omega^{(r)}} 2)^2$ times as many digit operations. Because the final result may have more than r consecutive ones, it must be transformed into normal form. That is, every string ...01...10... must be replaced by 10...0. This transformation can be accomplished in $2 \cdot \log_{\omega^{(r)}} 2 \cdot n$ steps. Hence, using the Zeckendorf representation will require, on average,

$$S_n^{(r)} = \log_{\omega^{(r)}}^2 2 \cdot A_{\infty}^{(r)} \cdot n^2 + 2 \cdot \log_{\omega^{(r)}} 2 \cdot n \approx H(r) \cdot n^2$$

bit operations to perform multiplication, if the classical algorithm is used. In Table 4 the initial values for the function $H(r) = \log_{\omega^{(r)}}^2 2 \cdot A_{\infty}^{(r)}$ are tabulated.

TABLE 4. Initial Values of the Function $H(r)$

r	2	3	4	5	6	7	8	9
$H(r)$	0.574	0.494	0.484	0.486	0.490	0.493	0.497	0.499

$H(r)$ attains its minimum when $r = 4$. Thus, the Quadranacci number system seems to be faster than other generalized Fibonacci number systems and faster than the BNS from a multiplicative complexity point of view.

If the time for transformation to normal form was included, it was computed that Quadranacci multiplication outperformed binary multiplication when the number of bits exceeded 130 (about 43 decimal digits). The last conclusion follows from the solution of the inequality

$S_n^{(4)} < 0 \cdot 5n^2$. In Table 5 we printed the values for the dynamic range and the corresponding fastest algorithm for multiplication.

TABLE 5. Comparison among Different Algorithms for Multiplication

Range (bits)	0-130	131-1200	1201-4096	4097-∞
Algorithm	Standard	Zeckendorf	Karatsuba-Ofman	Schonhage-Strassen

CONCLUSIONS

A comparison between well-known algorithms for standard binary multiplication and multiplication using the Zeckendorf representation has been considered. It was shown that some of the proposed number systems (Fibonacci, Tribonacci, Quadranacci) possess advantages for performing multiplication. The hybrid between the classical multiplication algorithm and the above nonstandard number systems can be used for fast multiplication of medium large integers.

REFERENCES

1. A. V. Aho, J. E. Hopcroft, & J. D. Ullman, eds. *The Design and Analysis of Computer Algorithms.* Reading, Mass.: Addison-Wesley, 1974.
2. E. Borel. "Les probabilites denumbrables et leurs application arithmétiques." *Rend. Circ. Math. Palermo* **27** (1909):247-71.
3. R. M. Capocelli. "A Generalization of Fibonacci Trees." In *Applications of Fibonacci Numbers* **3:**37-56. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecht: Kluwer, 1988.
4. R. M. Capocelli, G. Cerbone, P. Cull, & J. L. Hollaway. "Fibonacci Facts and Formulas," "Sequences," In *Int. Conf. on Combinatorics, Compression, Security and Transmission,* pp. 133-37. Ed. R. M. Capocelli. New York: Springer Verlag, 1990.
5. M. Feinberg. "Fibonacci-Tribonacci." *The Fibonacci Quarterly* **1.1** (1963):71-74.
6. D. Gries & G. Levin. "Computing Fibonacci Numbers (and Similarly Defined Functions) in Log Time." *Information Processing Letters* **11** (1980):68-69.
7. V. E. Hoggatt, Jr., & M. Bicknell. "Generalized Fibonacci Polynomials and Zeckendorf Representation." *The Fibonacci Quarterly* **11.5** (1973):399-419.
8. E. Zeckendorf. "Representations des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas." *Bulletin de la Societe Royale des Sciences de Liege* (1972): 179-82.

AMS Classification Numbers: 11B37, 11B75