TEST Engineering & Management

May- June 2020
ISSN: 0193-4120 Page No. 6386 - 6390

An Efficient Algorithm For Multiplying Large Binary Numbers Using Vedic Mathematics

Vijeta Iyer[1], V.Sudha[2]
[1]Department of Mathematics, Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India
[2]Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India
.

Article Info
Volume 83
Page Number: 6386 - 6390
Publication Issue:
May- June 2020

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *18 May 2020*

Abstract:
In the field of computer arithmetic, multiplication is considered as one of the key operation. Mostly, the algorithms proposed for multiplying two numbers is based on repeated addition. Also, the number of times the addition operation is performed is dependent on the number of operands supplied for the multiplication operation. In this paper, a multiplication algorithm using the methods of Ancient Indian Vedic Mathematics that makes use of lesser number of addition operations which can be used to multiply any binary number with any number of 1's efficiently is proposed. Vedic Mathematics is an olden scheme of mathematics which leverages the sixteen Sutras to perform calculations using unique techniques.

Keywords*: vedic mathematics, urdhvatriyakbhyam sutra, Booth's algorithm*

Introduction:

Arithmetic operations like addition, subtraction, multiplication and division are important operations as all the functions that need to be completed using computers have to be realized using these operations. Hence we call the above four operations as basic or fundamental operations in computer.

To overcome the needs of the current users, the processor speed is increased tremendously. To match the processor speed, algorithms that does fast arithmetic operations must be used. In previous years, there is no separate circuit for performing multiplication. Mostly, multiplication and division algorithms are realized using repeated addition and subtraction respectively.

Computers can understand only the binary forms. Thus, whatever number is to be passed as input it has to be converted to binary form. Any algorithm when realized using basic gates outperforms than the other algorithm. Arithmetic operations plays a vital role in Cryptography. Until the internet exists in this world, the internet security will also persists. It is a well-known fact that cryptography involves multiplication operation for its computation. Hence, it is required to use a time efficient algorithm for this operation.

Also, the operations such as modular exponentiation and Montgomery modular multiplication gets improved by improving the performance of the multiplication operation.

I. LITERATURE SURVEY

Initially, multiplication operations are realized using repeated binary addition. Later, few algorithms like Booth's algorithm [2], bit-pair recording etc., are proposed. Booth algorithm improves the performance of the binary multiplication by reducing the number of addition that we need to perform. It is known to us that while realizing binary multiplication using repeated addition, the number of addition that we do depends upon the number of 1's present in the multiplier. In Booth algorithm, by using the proposed booth encoding scheme, the iteration to perform addition is reduced. Though, the proposed technique reduces the number of addition,

May- June 2020
ISSN: 0193-4120 Page No. 6386 - 6390

it works well only when the number of 1's present are consecutive in nature.

Recently, the sutras in Vedic mathematics are applied to improve the performance of the multiplication operations

In [2], UrdhvaTiryakbhyam is used for improving the performance of the multiplication operation. In [3], the algorithm that improves the performance of Schonhage-Strassen is proposed.

In [4], the time taken for multiplication algorithm is reduced by applying Nikhilam Sutra, Urdhva Tiryakbhyam and Karatsuba-ofman and performance analysis of these algorithms are done. Multiplication of higher order mantissa part in Floating Point is a time consuming process. An algorithm for improving the above is proposed in [5]. In [6], various sutras used for improving multiplication operations are analysed. Efficient algorithm for improving multiplication operation in embedded system is proposed in [7]. Study and review of Booth Algorithm is done in [8]. An efficient algorithm for performing modular exponentiation is proposed in [9]. In [10], fast algorithms for cryptographic operations are discussed.

In this paper, an algorithm is discussed using Vedic mathematics for reducing the time complexity in multiplication operation.

There are a number of trouble-free and easy schemes that can be employed when multiplying by certain numbers. They are very helpful in their own right but can be even more helpful when pooled with other schemes where they can aid the solution of more difficult problems.

II. VEDIC MATHEMATICS

Vedic Mathematics deals with shortcut schemes which carryout Numerical Calculations more rapidly. It is a compilation of Schemes/Sutras which facilitate to work out numerical calculations in a more efficient way. 16 Sutras (Formulae) and 13 sub-sutras (Sub Formulae) form the basis on which the problems concerned in arithmetic, geometry, algebra, calculus, etc. are solved. A great Indian mathematician named **Jagadguru Shri Bharathi Krishna Tirthaji** revealed this stream of mathematics between A.D. 1911 and 1918 and his findings are available in a book entitled Vedic Mathematics by Tirthaji Maharaj [1]. In Sanskrit, Veda means 'Knowledge' and hence the name 'Vedic Mathematics', meaning 'Knowledge of Mathematics'.

Solving mathematical problems by means of classical techniques are sometime difficult, tedious and time consuming. But by means of Vedic Mathematics' General Schemes (valid for any type of numbers) and Specific Schemes (valid to specific type of numbers), arithmetic calculations can be performed like a streak of lightning.

In this paper, Vedic mathematics technique to multiply binary number with 11 has been discussed to improve the efficiency.

III. DESIGN OF VEDIC MULTIPLIER

Procedure for Multiplying any number by 11 using Vedic Mathematics

General multiplication formula, known as **"vertically and crosswise"** or "**Urdhva - tiryagbhyam**" in vedic maths is appropriate for multiplying any two numbers is illustrated in the following example of $(ab * uv)$, where ab and uv are two digit numbers, and the sutra is applied as follows:

```
  a       b
    u       v
 -------------------------
 a * u | av + ub | b * v
```

(Here '|' is used as separator)

Here the answer is split into three parts:

- upright =(b x v)
- criss-cross multiplication and addition =(a x v) + (b x u)

May- June 2020
ISSN: 0193-4120 Page No. 6386 - 6390

- upright =(a x u)

While multiplication with 11, u=1 and v=1, so:

a	b
1	1

a	a + b	b

Similar method is followed to multiply any number with more than 2 digits also. Working from right to left, write down the rightmost digit of the multiplicand and continue adding the adjacent two numbers for middle parts by moving right to left. Add each pair of digits and write down the answer (carrying digits wherever required right to left). Finally put in writing the left most digit of the multiplicand (adding any final carry if required).

Let us see the procedure to multiply 4072 by 11.

Firstly, the right most digit of 4072 is 2. Write it down as the right most digit of the answer. So we have

2

Secondly, the look for the last digit of 4072 i.e. 7 and 2 Sum up these two. Write the answer 9 to the left of the answer obtained in previous step. So we have

92

Next, move towards left and drop the number 2 and add the 0 and 7. Sum of these two numbers is 7. Note it down as the leftmost digit of the answer obtained in step 2. So we have

792

Next, move further left and drop the number 7 and consider 0 and 4 and add them to get answer 4. Write it down on the left of the result we got in previous step. So we have

4792

Finally, after moving further left and dropping 0, only 4 is left. Pen it down as the leftmost digit of the number obtained in previous step. So we have

44792

Hence the required product of 4072 and 11 is 44792, which has been obtained by just carrying out additions in each step.

IV. DEPLOYMENT OF VEDIC MULTIPLIER

The multiplication algorithm using vedic mathematics is proposed in Algorithm 1.
Let $M = m_n m_{n-1} \ldots m_1$ be the multiplicand of size n and Q be the multiplier(11)
Assume that variable P, S and C be the variables for holding final product, intermediate product and carry respectively.

Algorithm 1 Binary Multiplication

```
1: procedure MULTIPLY(M, Q)
2:     s_1 = m_1
3:     c_1 = 0
4:     i = 2
5:     for i ≤ n do
6:         s_i = m_{i-1} ⊕ m_i
7:         c_i = m_{i-1} ∧ m_i
8:     end for
9:     s_{n+1} = m_n
10:    r_0 = 0
11:    p_1 = s_1
12:    i = 2
13:    for i ≤ n + 1 do
14:        p_i = s_i ⊕ c_{i-1} ⊕ r_{i-1}
15:        r_i = s_i ∧ c_{i-1} ∨ r_{i-1}
16:    end for
17: end procedure
```

The work flow of the algorithm is explained in detailed in Example 1.

Example 1

Let M = 1101 and Q = 11. For value of n = 4

Initially, 1st bit of the carry is set to 0 and the first bit of the multiplier (here 1) is copied to s_1. For the

TEST Engineering & Management

May- June 2020
ISSN: 0193-4120 Page No. 6386 - 6390

remaining bits the process flow will be as given below,

$s_2 = 0 \oplus 1$ (here XOR operation is performed)

$c_2 = 0 \wedge 1 = 0$ (here and operation is performed)

$s_3 = 0 \oplus 1$

$c_3 = 1 \wedge 0 = 0$

The above steps are performed using the operations defined in the statements 6 and 7.

Finally, the last bit in *M* is copied to *S* as shown below $s_4 = m_4$ usingstep 9.

Thus, we have performed bit wise addition generating partial products and carry. Now, this partial product and carry has to be added to generate the actual product using steps 13 and 14.

V. RESULT AND DISCUSSION

As discussed in the above algorithm, the size of the for loop is equal to the size of the multiplicand. Here, the size of the multiplicand is generalized to be n. There are two for loops each with n as the upper bound. Hence, the complexity of the algorithm will be n+n which is equal to O(n). Thus, the algorithm proposed in this paper performs better the traditional multiplication. Also, it out performs the famous Booth algorithm by simplifying the number of multiplication operation performed when the input is 11.

CONCLUSION

In this paper, an efficient algorithm for performing fast multiplication is proposed using vertically and crosswise sutra in Vedic mathematics. The quick algorithm for multiplying any binary number with 1's exhibits better efficiency with respect to speed. The performance of the proposed algorithm gets improved by reducing the number of multiplication required for multiplying two numbers. It is known that the number of multiplication increases with the increasing number of 1's in multiplier. Thus the proposed algorithm improves the performance by overcoming the above constraint.

REFERENCES

1. Bharati Krishna Tirthaji Maharaja, "Vedic Mathematics"
2. Booth, A.D., "A signed binary multiplication technique," Quarterly Journal of Mechanics and Applied Mathematics, Vol. 4, pt. 2, pp. 236–240, (1951).
3. De, Anindya & P Kurur, Piyush & Saha, Chandan & Saptharishi, Ramprasad, 'Fast Integer Multiplication Using Modular Arithmetic', SIAM Journal on Computing. Vol.42, (2008).
4. G.Ganesh Kumar, V.Charishma, "Design of High Speed Vedic Multiplier using Vedic Mathematics Techniques", International Journal of Scientific and Research Publications, Volume 2, Issue 3, (2012).
5. Geetanjali Wasson , "IEEE-754 compliant Algorithms for Fast Multiplication of Double Precision Floating Point Numbers", International Journal of Research in Computer Science, Vol. 1, Issue 1, pp. 1-7, (2011).
6. Kavita, Umesh Goyal, "Performance Analysis of Various Vedic Techniques for Multiplication", International Journal of Engineering Trends and Technology, Vol. 4, Issue 3, (2013).
7. Mohammed Mosab Asad, Ibrahim Marouf, Qasem Abu Al-Haija, "Review Of Fast Multiplication Algorithms For Embedded Systems Design", International Journal of Scientific and Technology Research, Vol. 6, Issue 8, (2017).
8. Neha Goyal , Khushboo Gupta, Renu Singla, "Study of Combinational and Booth Multiplier", International Journal of Scientific and Research Publications, Vol. 4, Issue 5, (2014).
9. Seong-Min Hong, Sang-Yeop Oh, and Hyunsoo Yoon, "New modular multiplication algorithms for fast modular exponentiation", In Advances in Cryptology Proceedings of Eurocrypt '96, pp- 166-177, (1996).

May- June 2020
ISSN: 0193-4120 Page No. 6386 - 6390

10. Shahram Jahani, Azman Samsudin, and Kumbakonam Govindarajan Subramanian, “Efficient Big Integer Multiplication and Squaring Algorithms for Cryptographic Applications”, Hindawi Publishing Corporation, Journal of Applied Mathematics, Volume 2014.