An Optical System for Prime Factorization Based on Parallel Processing

Kouichi Nitta and Osamu Matoba

Department of Systems Science
Graduate of System Informatics, Kobe University
Rokkodai-cho 1-1, Nada-ku, Kobe, Hyogo, 657-8501, Japan
{nitta,matoba}@kobe-u.ac.jp

Abstract. A method for optical parallel processing in an algorithm for prime factorization is proposed as a brief announcement. In this method, amplitude modulation is utilized whereas our conventional method is based on phase modulation. The proposed method is suitable for the optical Fourier transform. This feature is considered to be useful in prime factorization. Basic concept of the proposed method is shown in this report.

Keywords: Prime factorization, Spatial parallel processing, Amplitude modulation.

1 Introduction

Some solutions for problems with computational hard is one of the main research topics in the field of optical supercomputing. As is well known, various methods have been reported for the travelling salesman problem, the Hamilton path problem, and so on [1-3].

We have also proposed a method for optical modulo operation [4]. Phase modulation of light wave is utilized in the proposed method. The method can treat modulo multiplication which is an important element in the algorithm for prime factorization. It also executes large scale parallel processing with simple optical hardware. Some optical implementations based on the proposed method have been demonstrated [5] and a system to solve prime factorization has been developed [6]. However, the method requires complex electronic processing to prepare a set of modulo exponentiation from results of optical processing.

In this presentation, we present a novel optical method for prime factorization. This method is based on optical amplitude modulation. Sequence of 4f optical systems is utilized for implementation. First, brief procedure for the prime factorization is described. Next we show simple numerical analysis to demonstrate the proposed method. From this analysis, it is shown that the proposed method is useful for prime factorization.

S. Dolev and M. Oltean (Eds.): OSC 2010, LNCS 6748, pp. 10–15, 2011.

2 Prime Factorization with Modulo Exponentiation

In our study, prime factorization is defined as the process to derive two different prime factors p and q from N (N=pq). The contents of an algorithm used in our method are briefly described as following. First, a specific operation called modulo exponentiation is obtained in $1 \leqq x \leqq 2N^2$-1. Modulo exponentiation $f(x)$ is given by Eq. (1)

$$f(x) = a^x \bmod N \tag{1}$$

In Eq. (1), a is a positive integer and satisfied with Eqs. (2) and (3).

$$1 < a < N \tag{2}$$

$$\gcd(a,N) = 1 \tag{3}$$

Here, $f(x)$ is known to be a periodic function. Also, the period is an integer. The period is given by analysis with the Fourier transform. Using the obtained period r, p and q can be derived as shown in Eqs. (4).

$$\begin{aligned} p &= \gcd(a^{r/2} - 1, N) \\ q &= \gcd(a^{r/2} + 1, N) \end{aligned} \tag{4}$$

This procedure is the same as that of the Shor's quantum algorithm [8]. In the algorithm, $f(x)$ is derived by quantum circuits for parallel processing. Many quantum gates are required in the circuits.

On the other hand, optical signal processing can achieve some complex operations. For example, the Fourier transform is executed by single lens. Based on the characteristics of optical processing, we have proposed parallel processing for modulo multiplication [7]. Modulo multiplication is important to obtain $f(x)$ as described in Sec. 3. In the conventional method, phase modulation of plane wave is utilized. Also, we have reported a system for prime factorization and some improvement of the system [4]. In our conventional method based on optical phase modulation, $f(x)$ is obtained with an optical set up for modulo multiplication. In this case, we have to derive a set of pixels corresponding x in preprocessing. Huge computational costs are required in the preprocessing.

3 Optical Parallel Processing with Amplitude Modulation

This section describes a novel optical parallel method. Let us consider a procedure to obtain a set of $f(x)$. As preprocessing, $l(i)$ defined as Eq. (5) is calculated in i=0, 1, 2, …, n-1.

$$l(i) = a^{2^i} \bmod N \tag{5}$$

Using $l(i)$, $f(x)$ is rewritten as the following equation.

$$f(x) = \prod_{i=0}^{n-1} l(i)^{x_i} \bmod N \tag{6}$$

Here, n is bit length of N. Also, x_i shows an i'th bit value of x. For example, (x_0, x_1, x_2, x_3, x_4) is (0, 1, 1, 0, 0) at x=6. Figure 1 shows principle of the procedure. As described in the figure, a set of $l(i)^{x_i}$ is prepared. And, inductive processing described in Eq. (7) is executed.

$$f_k(x) = \left\{ l(k-1)^{x_{k-1}} f_{k-1}(x) \right\} \bmod N \tag{7}$$

As results of n times iterations, $f(x)$ is obtained.

Our optical method is similar to the procedure. A schematic diagram of the method is shown in Fig. 2 (a). From the figure, optical hardware for the method consists of n'th sequence of 4-f optical systems. In this hardware, spatial amplitude modulators are put at all image planes. Fig. 2 (b) shows a diagram of distribution of amplitude transmittance on the modulators. These distributions in k'th modulator correspond with patterns of $l(k)^{x_k}$ shown in Fig. 1. Here $t(k)$ should be designed to be satisfied with Eq. (8).

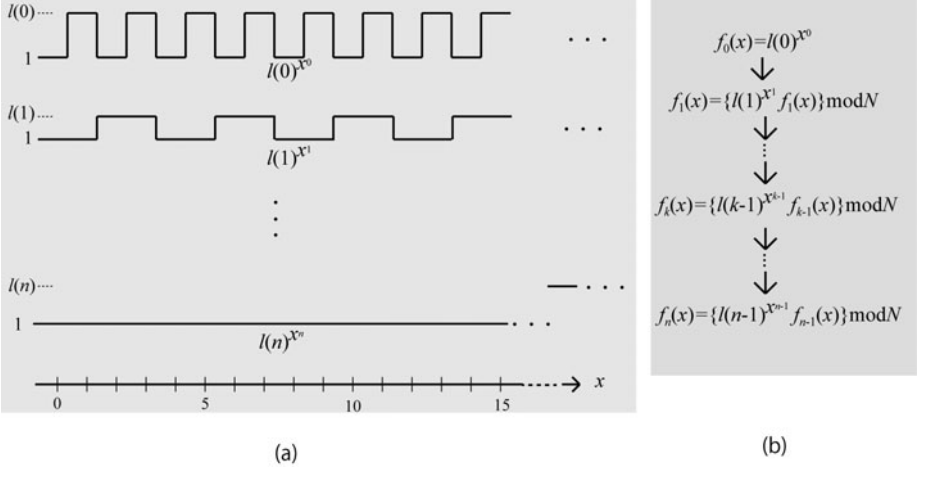


Fig. 1. (a) Structure of $l(i)^{x_i}$ and (b) the procedure to derive $f(x)$

$$t(0) - t_b : t(1) - t_b : \ldots : t(k) - t_b : \ldots : t(n-1) - t_b = l(0) : l(1) : \ldots : l(k) : \ldots : l(n-1) \tag{8}$$

Patterns measured at the detector plane correspond with distribution represented as Eq. (9).

$$f'(x) = \prod_{i=0}^{n-1} l(i)^{x_i} \tag{9}$$

In comparison with Eqs. (6) and (9), our optical method cannot implement modulo operations. However, our method seems to be useful to extracted the period of $f(x)$ as described in the next section.

4 Numerical Analysis

Usefulness of our proposed method is confirmed by numerical analysis. In the analysis, t_b is set to 0.5. $t(k)$ is determined in accordance with Eq. (10).

$$t(k) = \frac{l(k)}{\max\{l(i)\}} \times 0.5 + 0.5 \tag{10}$$

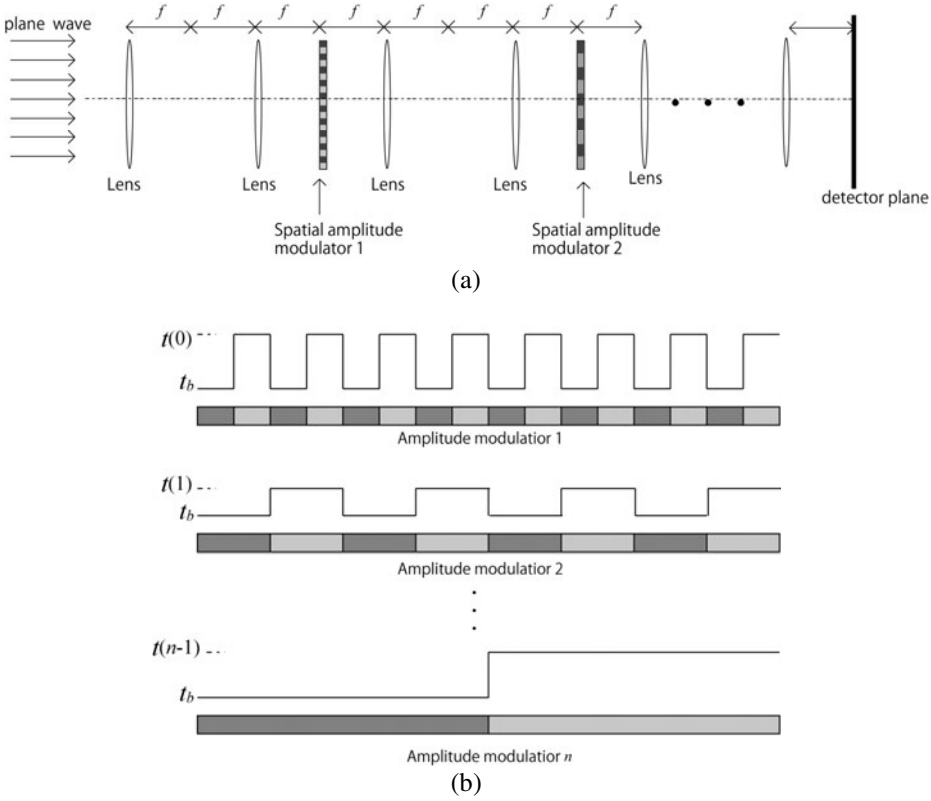
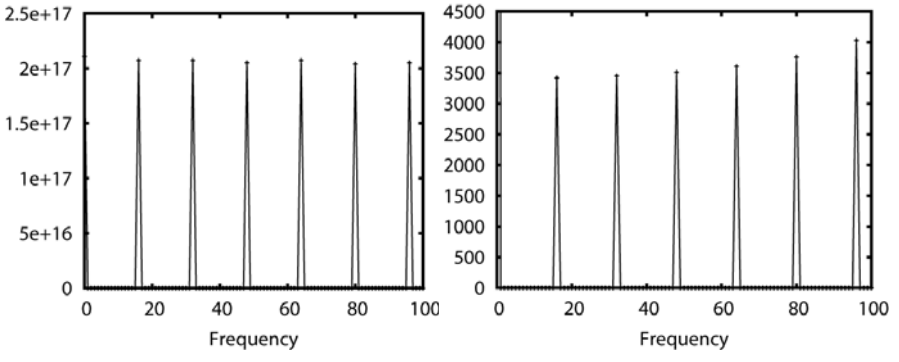


Fig. 2. Diagram of a scheme for of 2D binary images with image compression

Fig. 3 shows an example of results in the analysis. N and a are set to 203 and 106, respectively. Fig. 3 (a) is the part of the power spectrum of the result provided by the proposed procedure, and (b) is that of $f(x)$. From these figures, peak positions in the both profiles are the same coordinates in the horizontal direction. With analysis of

peak positions in the power spectrum, it is found that the value of r is 28. From the value, two prime numbers 7 and 29 are derived from Eq. (4). This analysis is quite same as the post processing in Shor's algorithm. Therefore, it is shown that the proposed procedure seems to be useful in large scale information processing for prime factorization. Note that aberration of lens and the point spread function of the optical system are not considered.



(a) (b)

Fig. 3. (a) Parts of power spectrum of a profile given by our method at (N, a)=(203, 106), and (b) that of $f(x)$

5 Discussions

As optical processing for factorization, the TWINKLE device is mentioned [8]. The TWINKLE gives two prime factors in accordance with the quadratic sieve (QS) algorithm and the number field sieve (NFS) one. These two algorithms are known to be practical for prime factorization in the present technology. Therefore, this device is considered to be suitable for high speed processing with optical and electronic implementations.

On the other hand, the purpose of Shor's quantum method is achievement of the system to solve prime factorization with polynomial time costs. The goal of our research is the same as that. Parallel processing is our optical system seems to be more practical than that based on quantum parallel processing. This is because physical implementation of massive data processing for quantum operations is difficult due to limitation of decoherence time.

Therefore, we should estimate computational costs of the proposed method. However, it is not found that our method can treat huge scale processing. Before the estimation, there are many issues in our research. Strictly speaking, the method cannot gives us $f(x)$ correctly. Also, influence on point spread function of imaging optics and that on unavoidable misalignment should be discussed. Based on the discussions, we would be able to clarify computational costs required in our optical procedure.

6 Comments and Summary

A novel optical method for the solution for prime factorization has been proposed as a brief announcement. By numerical analysis, it is demonstrated that the method can provide correct results. One of the features of this method is to implement simple optical set up. Another is suitability of optical Fourier transform. The latter is effective in comparison with our conventional method. Accuracy of our method should be estimated with detail analysis. Also, experimental demonstration is required.

References

1. Shaked, N.T., Messika, S., Dolev, S., Rosen, J.: Optical solution for bounded NP-complete problems. Appl. Opt. 46, 711–724 (2007)
2. Haist, T., Osten, W.: An Optical Solution For The Traveling Salesman Problem. Opt. Express 15, 10473–10482 (2007)
3. Oltean, M.: Solving the Hamiltonian path problem with a light-based computer. Natural Computing 7, 57–70 (2008)
4. Nitta, K., Matoba, O., Yoshimura, T.: Parallel processing for multiplication modulo by means of phase modulation. Appl. Opt. 47, 611–616 (2008)
5. Nitta, K., Katsuta, N., Matoba, O.: An Optical Parallel System for Prime Factorization. Jpn J. Appl. Phy. 48, 09LA02-1-5 (2009)
6. Nitta, K., Katsuta, N., Matoba, O.: Improvement of a system for prime factorization based on optical interferometer. In: Dolev, S., Oltean, M. (eds.) OSC 2009. LNCS, vol. 5882, pp. 124–129. Springer, Heidelberg (2009)
7. Shor, P.: Algorithms for quantum computation: Discrete logarithms and factoring Algorithms for quantum computation: Discrete logarithms and factoring. In: Proc. 35th Ann. Symp. on Foundations of Comput. Sci., vol. 1898, pp. 124–134 (1994)
8. Shamir, A.: Factoring Large Numbers with the TWINKLE Device. In: Koç, Ç.K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 2–12. Springer, Heidelberg (1999)