A Method for Modulo Operation by Use of Spatial Parallelism

Kouichi Nitta, Nobuto Katsuta, and Osamu Matoba

Department of Computer Science and Systems Engineering,
Graduate School of Engineering, Kobe University
Rokkodai 1-1, Nada, Kobe 657-8501, Japan
nitta@kobe-u.ac.jp, katsuta@brian.cs.kobe-u.ac.jp,
matoba@kobe-u.ac.jp

Abstract. An optical method for modulo operations has been proposed. This method utilizes phase modulation of light wave. This method can be applied to modulo multiplication which is an important operation in an algorithm for prime factorization. Optical parallel processing based on the method is implemented with a Michelson interferometer. This report shows that this method is effective in prime factorization. Especially, we study on suitability between large scale data processing for the prime factorization and the proposed method.

Keywords: Parallel processing, phase modulation, optical interference, modulo operation, prime factorization, spatial parallelism.

1 Introduction

As is well known, optical signals have various advantaged features for information processing. Broad bandwidth and huge capability for data storage are mentioned as examples of such features. Also, spatial parallelism is one of the promising characteristics in optical information processing.

Recently, some optical methods for problems requiring exponential computational costs with electronic processing have been proposed. In Ref. [1], a method for the Hamiltonian path problem is reported. This method utilizes delay of the rays. Also, two solutions for the traveling salesman problem have been developed. One is based on white light interferometry with fiber optics [2]. In the other methods, a set of network is represented as a binary matrix and the output is obtained by a matrix vector multiplication [3]. The multiplication process is realized with a joint transform correlator.

In such a situation, we have proposed an optical method for parallel modulo operations [4]. One of the advantaged features of the proposed method is based on spatial parallelism of light. This method gives wave fields corresponding to results of modulo operation by modulating phase of light wave. Moreover, this method is applied to modulo multiplication. Massive data processing for modulo multiplication is important in an algorithm for prime factorization [5]. The proposed method has been verified to be useful for prime factorization.

S. Dolev, T. Haist, and M. Oltean (Eds.): OSC 2008, LNCS 5172, pp. 98–103, 2008.

In this report, the principle of the method is described. And, some advantaged features of the system are discussed.

2 Modulo Operation with Optical Phase Modulation

In the factoring algorithm reported in Ref. [5], two prime numbers of a target integer are obtained with the period of modulo exponentiation as described in Eq. (1).

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

In this equation, N shows a target integer (N=pq). And a is an integer selected in preprocessing. Here, a should be satisfied with inequality (2) and Eq. (3), respectively.

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

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

In Eq. (3), gcd (a, N) indicates the greatest common devisor between a and N. In case that the period of $f(x)$ is an odd number, p and q are given by the following two equations.

$$p = \gcd(a^{r/2} - 1, N) \tag{4}$$

$$q = \gcd(a^{r/2} + 1, N) \tag{5}$$

In the algorithm, $f(x)$ is derived in accordance with the Shonhage-Strassen algorithm [7]. Note that modulo exponentiation is derived with sequence of modulo multiplication represented as Eq. (6).

$$g(x) = yx \bmod N \tag{6}$$

Let us consider a sinusoidal wave defined as Eq. (7).

$$U(\phi) = \cos(2\pi\phi) \tag{7}$$

In Eq. (7), by setting $\varphi = yx/N$, Eq. (7) is modified as shown in Eq. (8).

$$\begin{aligned} U(\phi) &= \cos\left(2\pi \frac{yx}{N}\right) \\ &= \cos\left(2\pi \frac{kN + g(x)}{N}\right) \\ &= \cos\left(\frac{2\pi}{N} g(x)\right) \end{aligned} \tag{8}$$

Eq. (3) shows that wave fields corresponding to remainder are obtained by simple phase modulation.

3 Optical Hardware and Improved Solutions

3.1 Basic Architecture for Optical Implementation

An optical system for parallel processing based on the above scheme can be constructed with a Michelson interferometer as described in Fig. 1. In the system, the mirror put at one optical arm is tilted to generate desired interference signals. A tilt angle to execute parallel processing shown in Eq. (7) is given by Eq. (8).

$$\theta = \frac{1}{2}\sin^{-1}\left(\frac{y\lambda}{DN}\right) \tag{8}$$

In this equation, λ and D show wavelength of the light source and pixel pitch of PD array, respectively. Interference signals are observed with photodetector array. Optical path difference between pixels is $(y\lambda/N)$. In accordance with procedure reported in Ref. [4], prime factorization is executed with the optical system and post processing. We have developed and demonstrated an optical system based on the architecture described in Fig. 1.

3.2 Previous Works

In the first prototype reported in Ref. [4], 640 points of $g(x)$ can be achieved in parallel. The performance of parallel processing directly depends on the array size of detectors. It has been shown that proposed method is able to give correct period of $f(x)$ with post processing even though noise signals are included in measured interference signals.

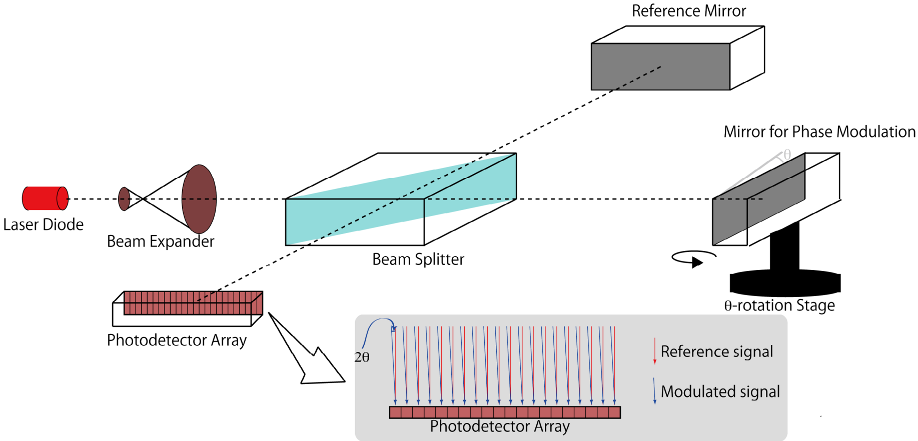


Fig. 1. Schematic diagram of an optical parallel processor for modulo operations

A method for two-dimensional parallel processing has been reported as improvement of the proposed method [6]. In the two-dimensional parallel system, both mirrors in the interferometer are controlled. One is rotated at θ-direction. And, the other is turned at α-direction. Interference patterns are generated and measured with two dimensional array of photo sensors. Note that this architecture is suitable for an area sensor. Fig. 2 shows a photograph of the constructed system. This system can achieve 1344x1024 points of parallel operations. It is shown that two dimensional processing is useful to improve processing performance dramatically.

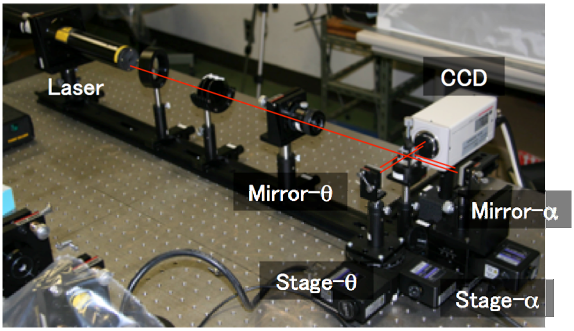
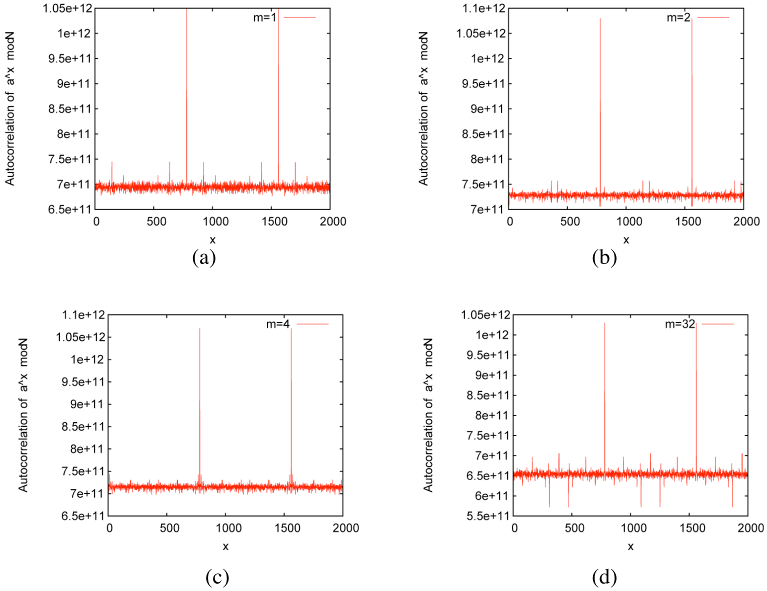


Fig. 2. Photograph of the experimental system for two dimensional parallel processing



(a) (b)

(c) (d)

Fig. 3. Numerical analysis for auto correlation of modulo exponentiation obtained by the improved method with Eq. (9). (a)~(d) show those in case of *m*=1, 2, 4, 32, respectively.

Another method has been proposed. This method improves processing performance without change of device. In the method θ is set as described in Eq. (9).

$$\theta = \frac{1}{2}\sin^{-1}\left(\frac{m}{D}\frac{a\lambda}{N}\right) \tag{9}$$

Here, m must be a natural number. Therefore, this method can achieve m times of parallel processing in comparison with the first system described in Fig. 1. Fig. 3 shows an example of the improved method. There are results of numerical analysis. Horizontal and vertical axes show x and auto correlation of $f(x)$, respectively. In this case, N and a are 1643 and 300 respectively. From the graphs, it is confirmed that correct period (=780) is derived in case of $m \leqq 32$.

On the other hands, noise robustness of an optical system described in Fig. 1 is estimated [9]. In an interferometer, misalignment and noise components are unavoidable. Therefore, error tolerance of the optical system is important for estimation of the proposed method. As results of estimations, we show that the proposed method has high robustness against noise signals.

4 Discussion about Spatial Parallelism and Suitability of Mathematical Property

In Ref. [4], we discuss on characteristics of the optical system shown in Fig. 1. Only single emitter and single modulator are required to construct the system. Note that two modulators are used for two dimensional parallel processing. The reason of the characteristics is described. In our method, plane wave corresponds to input statements for parallel processing. That means that input datum can be generated optically and passively. Almost of conventional optical parallel processors requires huge numbers of emitters. Therefore, our method seems to be effective for practical use. Moreover, the improved method using Eq. (9) executes modulo operations with fewer photodetectors. By use of the improved method, large scale information processing can be implemented at less device costs.

In the studied prime factorization, also, desired prime factors can be derived even though measured optical signals have noise components caused by misalignment. The reason of that is described. In our scheme, period of $f(x)$ is obtained with the optical system and post signal processing. One of the reasons of the feature, mathematical property is mentioned. $f(x)$ is known to be periodical function. And the period is an integer. By use of these characteristics, results obtained by the optical system can be compensated in the post processing. Therefore, it may be permitted that results of optical processing have slight errors. Suitability between required exactness in the target signal processing and accuracy of optical hardware is considered to be important to develop a practical optical system utilizing spatial parallelism.

5 Summary

We have reported an optical method for parallel processing. This method is based on optical interference and is effective in prime factorization. Reasons of the effectiveness of the method have been discussed. In the discussion, we especially focus on the spatial parallelism of optical processing and suitability between mathematical characteristics and optical operations.

However, we have not yet developed a solution to execute prime factorization in polynomial time costs. To construct the solution is final goal of our research and a challenging issue.

References

1. Oltean, M.: Solving the Hamiltonian path problem with a light-based computer. Nat. Comput. 7, 57–70 (2008)
2. Haist, T., Osten, W.: An optical solution for the traveling salesman problem. Opt. Exp. 15, 10473–10482 (2007)
3. Shaked, N.T., Messika, S., Dolev, S., Rosen, J.: Optical solutions for bound NP-complete problems. Appl. Opt. 46, 711–724 (2007)
4. Nitta, K., Matoba, O., Yoshimura, T.: Parallel processing for multiplication modulo by means of phase modulation. Appl. Opt. 47, 611–616 (2008)
5. 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)
6. Katsuta, N., Nitta, K., Matoba, O.: Parallel processor for modulo multiplication with optical interference. In: Technical Digest of The 13th Microoptics Conference, pp. 84–185 (2007)
7. Vedral, J., Barenco, A., Ekert, A.: Quantum networks for elementary arithmetic operations. Phys. Rev. A 54, 147–153 (1996)
8. Nitta, K., Katsuta, N., Matoba, O.: Study on processing performance of optical modulo operations J. Conf. Series (submitted)
9. Nitta, K., Katsuta, N., Matoba, O.: An optical interferometer for parallel modulo operation The review of laser engineering (accepted)