An Optical Interferometer for Parallel Modulo Operation

Kouichi NITTA, Nobuto KATSUTA, and Osamu MATOBA

Department of Computer Science and Systems Engineering,

Graduate School of Engineering, Kobe University

1-1, Rokkodai-cho, Nada, Kobe, Hyogo 657-8501

(Received January 18, 2008)

An optical processor for modulo operations is estimated. Large scale information processing for modulo operations is effective in an algorithm in prime factorization. This processor is based on a method for modulo multiplication using phase modulation of light wave. And it consists of a Michelson interferometer. Desired interference fringes are obtained by tilting reflection mirrors put at optical arms in the interferometer. Target operations are executed in parallel by measuring fringe patterns with photodetector array. One of the features of the processor is that it achieves parallel data processing for modulo multiplication with only simple operation. In terms of optical implementation, the presented processor seems to give us correct results even though there are some misalignment and noise signals in the processor. Therefore, error tolerance of the presented processor is discussed analytically. Influence of random noises in plane wave is analyzed. As results of analysis, it is verified that the presented processor has robustness against alignment and random errors.

Key Words: Prime factorization, Optical parallel processing, Interference, Noise analysis

1. Introduction

Recently, single-instruction-stream multi-data-stream (SIMD) parallel processing is attractive in various research fields. In a super computer, SIMD processors are utilized as key components and contribute to large scale simulations such as bio simulation, environmental simulation, and so on.

Also, quantum computing and molecular computing are studied as novel schemas. In these technologies, effective algorithms have been presented for some problems not to be solved in polynomial time with electronics. Shor's quantum method for prime factorization and DNA computation for Hamilton-path problem are mentioned as famous examples[1,2].

On the other hand, optical parallel processing has been researched. This is because light has various characteristics useful for large scale information processing. Especially, the inherent spatial parallelism of light is one of the most attractive features. A lot of methods for data processing have been developed. Two-dimensional parallel processing (2D) or three-dimensional parallel processing is used in almost of such methods.

In last year, some interesting optical methods for the traveling salesman (TSP) problem have been presented. One is to solve it with low coherence interferometry[3] and another utilizes on an optical system for the joint transform correlator[4]. The TSP is well-known as a problem not to be able to solve in polynomial time. These proposals seem to be important as novel optical methods for information processing requiring huge computational costs.

In such a situation, we study on a novel optical method for prime factorization. And a novel optical method for realizing modulo multiplication has been presented[5]. Modulo multiplication is one of the key operations in a factorization algorithm with SIMD processing. The method executes the operations with phase modulation of light waves. In the method, a divisor and a dividend in a modulo operation are mapped to the wavelength and phase of monochromatic plane wave, respectively. The method is implemented on an Michelson interferometer. Results of modulo are provided by measuring interference fringes and analyzing the optical phase corresponding to target divisors. Because various phase information is detected simultaneously by using simple phase modulation, the form of implementation is suitable for parallel processing.

In Ref. 5, we report a demonstration with the constructed prototype interferometer. As the principle of the presented method is simple, it is improved easily. As one of the improvements, 2D parallel processor has been developed [6]. This architecture is suitable for an area sensor. From the experiments, it is found that the prototype gives us correct results even though the prototype is affected by some misalignment and noise signals.

In this paper, therefore, error tolerance of the presented processor is discussed analytically. Influence of random noises in plane wave is investigated. As results of analysis, it is verified that the presented processor has robustness against alignment and random errors.

2. Parallel modulo operations in an algorithm for prime factorization

Prime factorization is a process to extract prime factors from a target positive integer N. In our research, as represented as Eq. (1), N is assumed to consist of only two factors.

$$N = pq \tag{1}$$

An algorithm to obtain prime factors has been presented[5]. In the algorithm, an integer a is selected. a should satisfy both $0<a<N$. The greatest common divisor between a and N should be 1. Next process is to derive the period r of the function $f(x)$ called modulo exponentiation. Eq. (2) represents $f(x)$.

$$f(x) = a^x \bmod N \tag{2}$$

If r is an even number, p' and q' are obtained by Eqs. (3) and (4), respectively.

$$p' = \gcd(a^{r/2} - 1, N) \tag{3}$$
$$q' = \gcd(a^{r/2} + 1, N) \tag{4}$$

In these equations, gcd(x, y) shows the greatest common divisor of x and y. In case of p', $q' \neq N$, p' and q' are output as the results. Figure 1 summarizes of the procedure.

In this algorithm, process for derivation of $f(x)$ requires huge computation costs. In digital electronics, a method with polynomial time costs has been not reported. Shor has presented a polynomial time algorithm for the derivation[2]. In the algorithm, $f(x)$ is provided in parallel with sequence of the circuits for modulo multiplication[7]. Considering present hardware technology for quantum computer, however, it is difficult to demonstrate massive data processing.

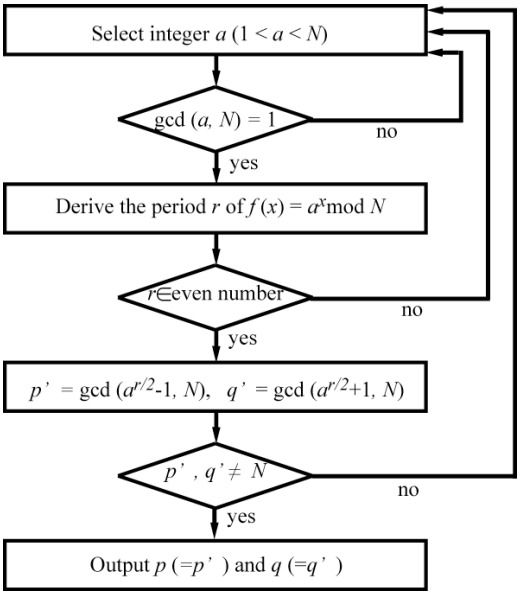

Fig.1 Flow chart of an algorithm for prime factorization.

3. An optical method for parallel modulo multiplication

3.1 Principle of modulo operations by use of phase modulation

We have been presented an optical method for parallel modulo operation[3]. This method is based on phase modulation of plane wave.

Here, positive integer s defined as Eq. (5) is considered.

$$s = tu + v \tag{5}$$

In this equation, it is assumed that t, u, and v are integers. Therefore, Eq. (5) shows that s is divisible by u with a remainder of v.

Next, a monochromatic wave represented as Eq. (6) is analyzed.

$$U(\phi) = A\exp\left(\frac{2\pi i}{\lambda}\varphi\right) \tag{6}$$

In Eq. (6), A, λ, and ϕ indicate the amplitude, the wavelength, the phase of the light wave, respectively. As described in Eq. (7), specific optical fields can be generated by setting $\phi = s\lambda/u$.

$$\begin{aligned} U(s) &= A\exp\left(\frac{2\pi i}{\lambda}\frac{\lambda s}{u}\right) \\ &= A\exp\left(2\pi i\left\{t + \frac{v}{u}\right\}\right) \\ &= A\exp\left(2\pi i\frac{v}{u}\right) \end{aligned} \tag{7}$$

From Eq. (7), $U(s)$ corresponds with v. Moreover, in case of $s = ax$, $U(s)$ provides wave fields depending on the result of modulo multiplication.

3.2 Optical hardware for modulo multiplication

Based on the relation between optical fields and modulo operations, we have developed architecture for modulo multiplication. A brief diagram of the architecture is shown in Fig. 1. From this figure, a Michelson interferometer is utilized for parallel processing. In the interferometer, plane wave is generated and divided into two signals. Both signals are reflected at mirrors.

One mirror is tilted with angle θ whereas the other is put to perpendicular to optical axis. These two signals are defined the following equations.

$$U_o(r + \Delta r(\theta, p)) = A\exp\left\{\frac{2\pi i}{\lambda}\left(r + \Delta r(\theta, p)\right)\right\} \tag{8}$$

$$U_r(r) = A\exp\left(\frac{2\pi i}{\lambda}r\right) \tag{9}$$

In Eq. (8), $\Delta r(\theta, p)$ indicates the optical path difference between the $U_o(r+\Delta r(\theta, p))$ and $U_r(r)$ at a pixel p on a photodetector array. As a result, $I(p)$ is detected at the detector array.

$$I(p) = 2A^2\left(1 + \cos\left[\frac{2\pi}{\lambda}\Delta r(\theta, p)\right]\right) \tag{10}$$

From Fig. 2, $\Delta r(\theta, p)$ is represented as Eq. (11).

$$\Delta r(\theta, p) = pD\sin 2\theta \tag{11}$$

Here D shows the pixel pitch of the detector array. We can obtain the modulo multiplication represented as Eq. (12) by setting $\theta = 1/2\ \sin^{-1}(a/DN)$.

$$g(p) = ap \bmod N \tag{12}$$

In Ref. 5, a basic concept has been presented. A prototype system is reported to show experimental verifications of the concept. Prime factorization is demonstrated with the prototype and post digital signal processing.

Also, 2D parallel processing based on the presented concept has been presented in Ref. 6. In this processing, both θ rotation stage and α rotation one are used for 2D phase modulation. An experimental hardware has been constructed. 2D parallel processing is considered to be suitable for area sensor. From verification results, it has been confirmed that the hardware is suitable for large scale information processing.

In terms of optical parallel processor, the presented method has some advantaged features. One is that the hardware system consists of only simple optical devices. A large array of emitters or a spatial light modulator with ultra-high resolution is not required. This feature is effective as practical hardware configuration.

Another is robustness against unavoidable misalignments and noise components. It is caused by characteristics of the factorization algorithm. In the algorithm, we should derive only the period of $f(x)$. The presented method does not give a remainder directly, but instead gives a corresponding distribution of optical intensity. From the experimental results in our previous works, correct period seems to be obtained even though there are miss alignment and noise signal in the optical system.

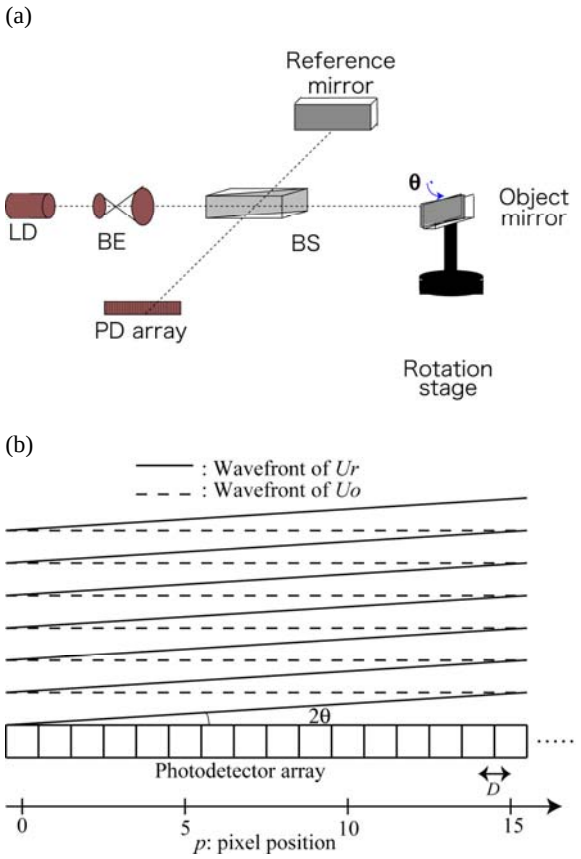

Fig.2 Modulo multiplication with optical interference: (a) Schematic diagram of optical hardware based on a Michelson interferometer and (b) the relation between phase difference and a pixel p.

4. Numerical noise analysis

The relations between output results and noise signals are investigate to discuss the robustness of the presented method. Considering inference components of $I(p)$ in Eq. (10), detected signal with noise components are defined as Eq. (13).

$$I'(p) = 2A^2\left(\cos\left[\frac{2\pi}{\lambda} pD\sin 2\theta\right] + \chi\gamma\right) \tag{13}$$

Here, χ is the coefficient of noise signals, and γ shows a uniform random number satisfying Eq. (14).

$$0 < \gamma < 1 \tag{14}$$

In the numerical analysis, distribution of modulo exponentiation is derived from a set of $I'(p)$. The procedure of the derivation is in accordance with our previous work [5].

First, we show an analytical result without noise signal. Fig. 3 (a) and (b) depict the result of modulo exponentiation and the power spectrum of (a), respectively. In this case, N and a are set to be 15 and 7. From Fig. 3 (a), it is found that periodical profile is obtained. Also, From Fig. 3 (b), peak signals correctly appears at u=105, 210, 315, respectively.

Next, the results containing the noise components are discussed. Figs. 4 and 5 show the analytical results in cases of χ = 0.1 and 1.0, respectively. From Fig. 5 (a), especially, periodicity of the profile cannot be observed due to added noise signals. However, peak signals in Fig. 5 (b) appear clearly. Prime factors of 15 can be given as 3 and 5 by analysis of peak signals.

These results show that the presented optical system is high robust against noise signals. In other words, process to derive the period of modulo exponentiation is suitable for optical implementation.

This analysis is the first approach to estimate processing performance. As future issues, we should discuss on robustness against misalignment of optical components. Moreover, accuracy of prime factorization should be estimated when the value of N is much larger.

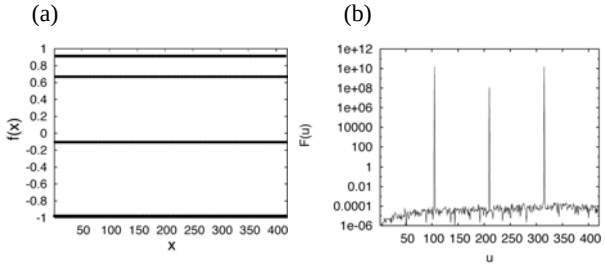

Fig. 3 (a) Modulo exponentiation (at N=15, a=7) without noise signals (χ=0) and (b) Power spectrum of (a).

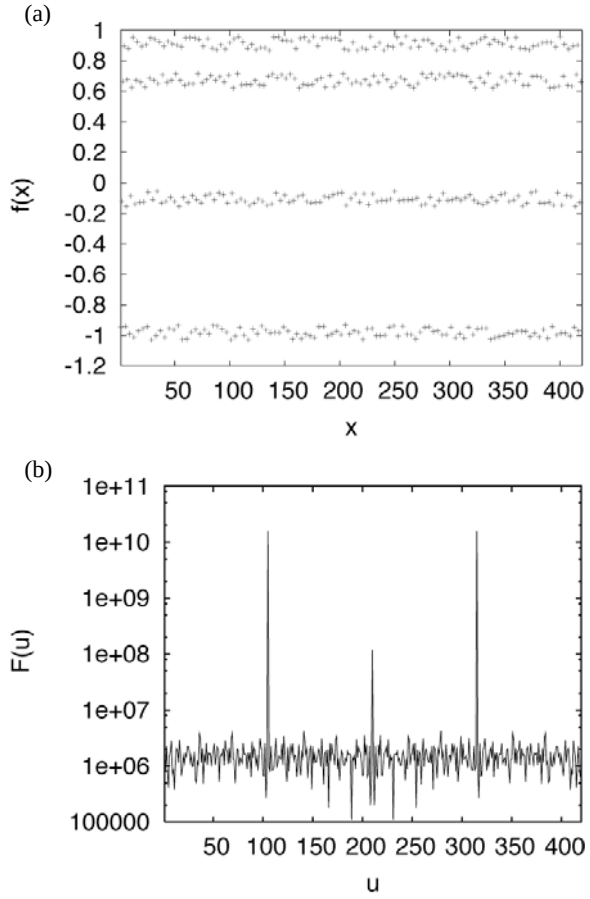

Fig. 4 (a) modulo exponentiation (at N=15, a=7) in case of (χ=0.1) and (b) Power spectrum of (a).

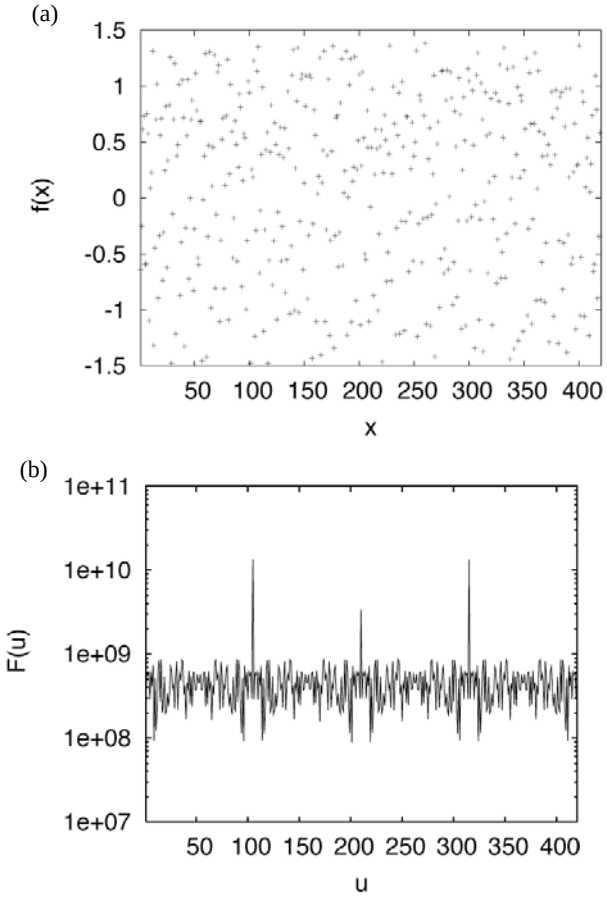

Fig. 5 (a) modulo exponentiation (at N=15, a=7) in case of (χ=1.0) and (b) Power spectrum of (a).

5. Conclusion

An optical method for modulo multiplication was summarized and advantaged characteristics of the method was described. We have shown numerical analysis to estimate robustness against random noises. From the analysis, it is verify that correct prime factors are given with our optical method.

Part of this work was supported by Grant-in-Aid for Scientific Research No. 17760047 from the Japanese Ministry of Education, Culture, Sports, Science, and Technology and by the Hyogo Science and Technology Association.

References

1) P. Shor: *Proc. of 35th Ann. Sympo. on the Foundations of Computer Science*, **1898** (1994) 124.
2) L. M. Adleman: Science, **266** (1994) 1021.
3) T. Haist and W. Osten: Opt. Exp.**15** (2007) 10473.
4) N. T. Shaked, S, Messika, S. Dolev, and J. Rosen: Appl. Opt. **46** (2007) 711.
5) K. Nitta, O. Matoba, and T. Yoshimura: SPIE, **6311** (2006) 631109.
6) N. Katsuta, K. Nitta, and O. Matoba: *Tech. Dig. of 13th Microoptics Conference* (2007) p.184.
7) T. H. Cormen, C. E. Leiserson, and R. L. Rivest: *Introduction to algorithm* (MIT Press, 1990) p. 849.