Simulation Analysis of the Robustness of the Order-finding Circuit against Errors

Takashi Yamada[1 2 *] Jumpei Niwa[1] Fumitaka Yura[2] Hiroshi Imai[1 2]

[1] *Department of Computer Science, Graduate School of Information Science and Technology, University of Tokyo.*
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
[2] *ERATO Quantum Computation and Information Project, JST.*
Hongo White Bldg., 5-28-3 Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan

Abstract. Quantum computers cannot avoid error occurrence, and it is important to investigate the actual behavior of quantum algorithms in the presence of errors. In this paper we implement the quantum order-finding circuit for integer factorization introduced by Beauregard and the existing one on Quantum Computer Simulation System (QCSS), and do simulation on the scalable distributed-memory parallel computer. On this environment we check whether the circuit by Beauregard is useful for factorization on an actual quantum computers by comparing the existing circuits. As a result we find that Beauregard's circuit is more robust against decoherence error but less robust against operational error than the existing circuits.

Keywords: simulation for quantum computing, Shor's factorization algorithm, decoherence error, operational error.

Actual quantum computers cannot avoid error occurrence. It is of importance to investigate the behaviors of quantum circuits in the presence of errors. However, there are few theoretical analysis of them. In addition, with current technologies, it is still hard to make actual quantum computers dealing with many qubits. Therefore, to simulate quantum algorithms in the presence of errors on classical computers plays an important role because it can deal with much more qubits.

In this paper, we focus on a quantum algorithm for integer factorization and do simulation on classical computers in a large scale. Integer factorization is considered to be intractable on classical computers. In 1994, however, P. Shor proposed a polynomial-time quantum algorithm for order-finding [7], and showed an integer factorization quantum algorithm by using it.

The major cost in the quantum order-finding circuit used in arbitrary L-bit number factorization, is not the QFT (quantum Fourier transform) but the modular exponentiation, which has $O(L^3)$ depth. For example, a modular exponentiation circuit realized today requires $2L + 6$ additional working qubits [3]. In this approach, $5L+6$ qubits are totally required to construct the quantum order-finding circuit.

Last year, Beauregard improved the order-finding circuit [1]. The number of qubits required to construct the circuit is reduced to $2L + 3$ to factorize an arbitrary L-bit number. In this improved circuit, the following two techniques were used:

Addition by QFT [2]: This uses QFT and reduces the number of qubits necessary for addition by removing temporary carry bits.

One control quantum bit trick [5]: It is shown that the (inverse) Fourier transform preceding the final measurement can be calculated in a semiclassical way.

By using these techniques, it becomes possible to implement the whole quantum order-finding circuit used in arbitrary number factorization.

Simulation is useful for investigating the behavior of the whole quantum order-finding circuit for large numbers (that is, for many qubits cases). Many qubits simulation requires more computational power than is usually available.

We have adopted the Quantum Computation Simulation System (QCSS) [4] as a simulation platform and performed it on SCoreIII [6], a fast parallel computer. On this environment, we have implemented the Shor's factorization algorithm and the two order-finding circuits (by Beauregard [1], and one more circuits for comparison) on QCSS. Besides, We have checked the robustness of the new order-finding circuit against errors specific to quantum computers by comparing with the other circuit. As a result we have found that the new order-finding circuit was more robust against decoherence error but less robust against operational error.

Error model

QCSS can represent decoherence and operational errors. By using it we can analyze robustness of some quantum circuits in the presence of decoherence and operational errors.

Decoherence error: The simulator implements *depolarizing channel* as the decoherence error model. In this channel, at each computational step, with probability $1 - d$ each qubit is left alone, and with probability d one of the error gate σ_x, σ_y or σ_z (Pauli's X, Y, Z) are applied to each qubit independently. The error rate d is determined by users.

Operational error: The simulator represents operational error by adding small deviations to each element of the unitary operator. Each error angle is drawn from Gaussian distribution with the standard deviation σ, which is also determined by users.

Implementation

We have implemented the two order-finding circuits, advanced one by Beauregard (Circuit A) and one more circuit for comparison (Circuit C). Table 1 shows the leading terms of the numbers of the quantum gates of these circuits. The depth of both circuits for L-bit number factorization is $O(L^3)$, and the number of measurement gates is $2L$ in the both circuits.

As Circuit A adopt the adder by QFT and have $O(L^2)$ QFT gates, there are much more controlled rotate gates than Circuit C. On the other hand, there are more controlled NOT gates in Circuit C because in these circuit addition gate is realized as a combination of controlled NOT gates.

*tyamada@is.s.u-tokyo.ac.jp

Table 1: Features of the order-finding circuits used in factorization of a L-bit number.

	#qubits	one control qubit trick	addition by QFT	#gates				
				Had.	NOT	C-NOT	phaseshift	C-phaseshift
A	$2L+3$	YES	YES	$16L^3$	$8L^2$	$8L^3$	$4L^3$	$\boldsymbol{8L^4}$
C	$3L+7$	YES	NO	$2L$	$2L$	$\boldsymbol{800L^3}$	$2L$	0

Robustness for decoherence error

We selected 21 (5 bit) as a number to factorize with the circuits on QCSS, for an appropriate number of trials are required for statistics.

We investigated the robustness of Circuit A and C for decoherence error by Monte Carlo simulation. On Circuit A and C, 20000 and 2000 trials were done, respectively, with each decoherence error rate d. Note that it takes much more time for Circuit C to factorize a number on our implementation than Circuit A, due to the number of qubits.

Figure 1 shows the result. In this figure, "Ideal" line means the expected success probability without errors, and "lower bound" line means the success probability when the distribution of the quantum state is uniform.

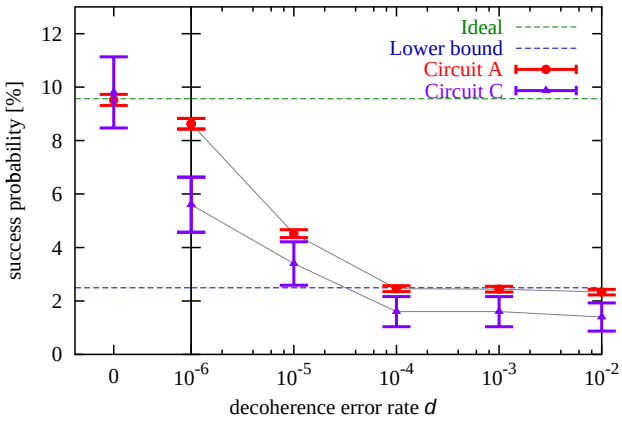

Figure 1: Relation between decoherence error rate d and success probability.

From Figure 1 we can see the following two points:

1. Circuit A is more robust against decoherence error than Circuit C when $10^{-6} < d < 10^{-4}$.
2. On both Circuit A and C, when $d \geq 10^{-4}$, the success probability is almost constant, near the "lower bound" line. This means that both the circuits are not useful for order-finding.

In our decoherence error model, the number of the gates applied as error gate depends on the area (the product of the number of qubits and the depth) of the circuit. We consider that the robustness of Circuit A is came from the reduction of the number of qubits with keeping the depth of the circuit.

Robustness for operational error

We also investigated the robustness of the circuits for operational error in the same way as decoherence error.

On Circuit A and C, we factorized 21 on QCSS. With each σ (the standard daviation of operatinal error), 20000 and 2000 trials were done, respectively. Then we calculated the success probability.

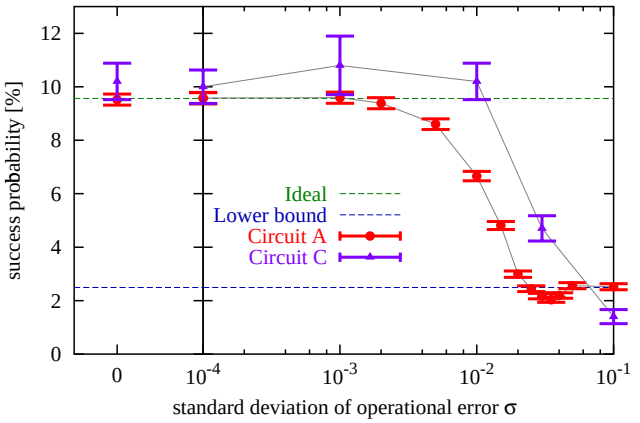

Figure 2: Relation between standard deviation of operational error σ and success probability.

Figure 2 shows the result. As for Circuit A and C, when the standard deviation of operational error σ is less than $10^{-3} \approx \pi/2^{11}$, we find that the circuit is not affected by the operational error at all. However, when σ is around 10^{-2}, we can see that the success probability of Circuit C is higher than that of Circuit A. In addition, when σ is more around 10^{-1}, the success probabilities of the both circuits are near or below the "lower bound" line.

In operational error, the influence of the error depends on the kind of the quantum gate. From the result we can see that operational error affects more strongly controlled phase shift gates than controlled NOT gates.

Concluding Remarks

From the experimental results, we have found that the quantum circuit introduced by Beauregard was more robust against decoherence error but less robust against operational error than the circuit we have prepared for comparison.

In addition, we have also found that if decoherence error rate d was more than 10^{-4}, both the order-finding circuits were not useful for order-finding and that if the standard deviation of operational error σ was less than 10^{-3}, operational error did not affect the order-finding circuits at all.

References

[1] S. Beauregard. *Quantum Information and Computation*, 3(2):175–185, 2003.

[2] T. G. Draper. quant-ph/0008033, 2000.

[3] C. Miquel, J. P. Paz, and R. Perazzo. quant-ph/9601021, 1996.

[4] J. Niwa, K. Matsumoto, and H. Imai. *Physical Review A* 66, 062317, 2002.

[5] S. Parker and M. B. Plenio. *Phys. Rev. Lett.*, 85:3049–3052, 2000.

[6] PC Cluster Consortium. http://www.pccluster.org.

[7] P. W. Shor. *SIAM J. Comp.*, 26:1484–1509, 1997.