Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 8, Number 4 (2012), pp. 365–369

http://www.ripublication.com/gjpam.htm

# Quantum Algorithm for Modified One-dimensional Random Walk Problem by Central Limit Theorem

**Toru Fujimura**
*Chemical Department,*
*Industrial Property Cooperation Center,*
*1-2-15, Kiba, Koto-ku, Tokyo 135-0042, Japan*
*E-mail: tfujimura8@gmail.com*

**Abstract**

A quantum algorithm for a modified one-dimensional random walk problem by the central limit theorem and its example are reported. When a random variable $X_i$ [$1 \leq i \leq n$. $i$ and $n$ are integers.] becomes $d_t$ and $-d_t$ [$d_t$ is a distance. $1 \leq t \leq k$. $t$ and $k$ are integers.] as each probability $1/(2k)$, an example in paths that arrive at a point on a straight line is obtained. A computational complexity of a classical calculation is $(2k)^n$. The computational complexity becomes about $3(log_2 2k)n$ by the quantum algorithm that uses quantum phase inversion gates, quantum inversion about mean gates, and the standard normal distribution. Therefore, a polynomial time process becomes possible.

**AMS subject classification:** Primary 81-08; Secondary 68R05, 68W40.
**Keywords:** Quantum algorithm, modified one-dimensional random walk problem, central limit theorem, computational complexity, standard normal distribution, polynomial time.

## 1. Introduction

A quantum computer can solve a problem at high speed by a parallel computation that uses quantum entangled states. Deutsch-Jozsa's algorithm for the rapid solution [1–3], Shor's algorithm for the factorization [2–4], Grover's algorithms for the database search [2,5,6], and so on are known. A quantum algorithm for the vertex coloring problem by the central limit theorem has recently been reported by Fujimura [7]. Its computational complexity becomes a polynomial time. In the one-dimensional random walk problem [8], its modified problem that is set up is examined this time. Therefore, its result is reported.

## 2. Modified One-dimensional Random Walk Problem

When a random variable $X_i$ [$1 \leq i \leq n$. $i$ and $n$ are integers.] becomes $d_t$ and $-d_t$ [$d_t$ is a distance. $1 \leq t \leq k$. $t$ and $k$ are integers.] as each probability $1/(2k)$, an example in paths that arrive at a point on a straight line is searched.

## 3. Quantum Algorithm

It is assumed that $X_i$ [$1 \leq i \leq n$. $i$ and $n$ integers.] becomes $d_t$ and $-d_t$ [$d_t$ is a distance. $1 \leq t \leq k$. $t$ and $k$ are integers.] as each probability $1/(2k)$, a mean is 0, and a dispersion is $(d_1^2 + d_2^2 + \cdots + d_k^2)/k$. Therefore, when a total mean is 0 and a total dispersion $\sigma^2 = (d_1^2 + d_2^2 + \cdots + d_k^2)n/k$, $(\sum_{i=1}^{n} X_i)/\sigma$ follows the normal distribution from the central limit theorem. When the standard normal distribution $f(z)$ is $\int_0^z (e^{-z^2/2}/(2\pi)^{1/2})dz$, and values of $\int_{u_p}^{v_p} (e^{-z^2/2}/(2\pi)^{1/2})dz$ are $1/2^2, 1/2^4, 1/2^6, 1/2^8, \cdots$, and $1/2^{2p}$ [$p$ is a positive integer], each value of $z$ is assumed $u_p$ and $v_p$ that these range are contained a value $M$ of a point on a straight line that is searched. $u_p$ and $v_p$ are obtained from the table of $f(z)$. Each total number of the data between $u_p\sigma$ and $v_p\sigma$ is $(2k)^n/2^2, (2k)^n/2^4, (2k)^n/2^6, (2k)^n/2^8, \cdots$, respectively. A height at $m$ is $(2k)^n e^{-(m/\sigma)^2/2}/((2\pi)^{1/2}\sigma)[= H(m)]$.

Next, a quantum algorithm is shown as the following.

First of all, quantum registers $|a_1>, |a_2>, \cdots, |a_n>, |b>$, and $|c>$ are prepared. When $\alpha$ is a minimum integer that is $log_2 2k$ or more, each of $|a_f>$ that $f$ is an integer from 1 to $n$ is consisted of $\alpha$ quantum bits [= qubits]. States of $|a_1>, |a_2>, \cdots, |a_n>$, $|b>$, and $|c>$ are $a_1, a_2, \cdots, a_n, b$, and $c$, respectively.

**Step 1:** Each qubit of $|a_1>, |a_2>, \cdots, |a_n>, |b>$, and $|c>$ is set $|0>$.

**Step 2:** The Hadamard gate $\boxed{H}$ [2, 3] acts on each qubit of $|a_1>, |a_2>, \cdots, |a_{n-1}>$, and $|a_n>$. It changes them for entangled states. The total states are $(2^\alpha)^n$.

**Step 3:** It is assumed that a quantum gate $(A)$ changes $|b>$ for $|b+1>$ at $a_f \geq 2k$, or it doesn't change $|b>$ at $a_f < 2k$. As a target state for $|b>$ is 0, quantum phase inversion gates $(PI)$ and quantum inversion about mean gates $(IM)$ [2,5,6] act on $|b>$. When $\beta$ is a minimum even integer that is $(2^\alpha/(2k))^{1/2}$ or more, the total number that $(PI)$ and $(IM)$ act on $|b>$ is $\beta$ because they are a couple. Next, an observation gate $(OB)$ observes $|b>$. These actions are repeated sequentially from $|a_1>$ to $|a_n>$. Therefore, each state of $|a_f>$ is $0, 1, \cdots, 2k-2$, and $2k-1$, and the total states become $(2k)^n[= W_0]$.

**Step 4:** It is assumed that a quantum gate $(B)$ changes $|b>$ for $|b+d_1>, |b-d_1>$, $|b+d_2>, |b-d_2>, \cdots, |b+d_k>$, and $|b-d_k>$ at $a_1 = 0, 1, 2, 3, \cdots, 2k-2$, and $2k-1$, respectively. This action repeats to $|a_n>$. Therefore, $|b>$ becomes from $|-nd_{max}>$ to $|nd_{max}>$ [$d_{max}$ is a maximum value in $d_t$].

**Step 5:** It is assumed that a quantum gate $(C_1)$ doesn't change $|c>$ in $u_1\sigma \le b \le v_1\sigma$, or it changes $|c>$ for $|c+1>$ in the others of $b$. As the target state for $|c>$ is 0, $(PI)$ and $(IM)$ act on $|c>$. The number of the data that is included in $u_1\sigma \le b \le v_1\sigma$ is $W_1 \approx (2k)^n/2^2$. When $\gamma_1$ is a minimum even integer that is $(W_0/W_1)^{1/2}$ or more, the total number that $(PI)$ and $(IM)$ act on $|c>$ is $\gamma_1 \approx 2$. Next, $(OB)$ observes $|c>$, and the data of $W_1$ remain.

Similarly, $(C_R)$ [$2 \le R \le g-1$. $R$ is an integer. $g$ that is an integer follows $W_0/H(M) = 1/(e^{-(M/\sigma)^2/2}/(2\pi)^{1/2}\sigma) \approx 2^{2g}$.] doesn't change $|c>$ in $u_R\sigma \le b \le v_R\sigma$, or it changes $|c>$ for $|c+1>$ in the others of $b$. As the target state for $|c>$ is 0, $(PI)$ and $(IM)$ act on $|c>$. The number of the data that is included in $u_R\sigma \le b \le v_R\sigma$ is $W_R \approx (2k)^n/2^{2R}$. When $\gamma_R$ is the minimum even integer that is $(W_{R-1}/W_R)^{1/2}$ or more, the total number that $(PI)$ and $(IM)$ act on $|c>$ is $\gamma_R \approx 2$. Next, $(OB)$ observes $|c>$, and the data of $W_R$ remain. These actions are repeated sequentially from 2 to $g-1$ at $R$.

$(C_g)$ doesn't change $|c>$ at $b = M$ [$u_g\sigma \approx M \le b \le v_g\sigma \approx M$], or it changes $|c>$ for $|c+1>$ in $b \ne M$. As the target state for $|c>$ is 0, $(PI)$ and $(IM)$ act on $|c>$. The number of the data that is included at $b = M$ is $W_g \approx (2k)^n e^{-(M/\sigma)^2/2}/((2\pi)^{1/2}\sigma)[=H(M)] \approx (2k)^n/2^{2g}$. When $\gamma_g$ is the minimum even integer that is $(W_{g-1}/W_g)^{1/2} \approx (((2k)^n/2^{2(g-1)})/((2k)^n/2^{2g}))^{1/2} = 2 \le 2 = \gamma_g$, the total number that $(PI)$ and $(IM)$ act on $|c>$ is $\gamma_g \approx 2$. Next, $(OB)$ observes $|a_1>, |a_2>, \cdots, |a_n>, |b>$, and $|c>$, and one of the data of $W_g$ remain. Therefore, one example of paths that arrive at the point $M$ on the straight line is obtained.

## 4. Numerical Computation

It is assumed that there are $k = 3, d_1 = 1, -d_1 = -1, d_2 = 2, -d_2 = -2, d_3 = 3, -d_3 = -3, d_{max} = 3, n = 3, \sigma = 3.742, M = 5, H(5) \approx 9, g = 3, u_1 = 0.4103, u_2 = 1.023, u_3 = 1.246$, and $v_1 = v_2 = v_3 = 1.336$ [$u_1\sigma \approx 2$, $u_2\sigma \approx 4$, $u_3\sigma \approx 5$, $v_1\sigma = v_2\sigma = v_3\sigma \approx 5$].

First of all, $|a_1>, |a_2>, |a_3>, |b>$, and $|c>$ are prepared. When $\alpha$ is the minimum integer that is $log_2 2k = log_2 6 \approx 2.6 \le 3 = \alpha$, each of $|a_f>$ that $f$ is the integer from 1 to 3 is consisted of 3 qubits. States of $|a_1>, |a_2>, |a_3>, |b>$, and $|c>$ are $a_1, a_2, a_3, b$, and $c$, respectively.

**Step 1:** Each qubit of $|a_1>, |a_2>, |a_3>, |b>$, and $|c>$ is set $|0>$.

**Step 2:** $\boxed{\text{H}}$ acts on each qubit of $|a_1>, |a_2>$, and $|a_3>$. It changes them for entangled states. The total states are $(2^3)^3$.

**Step 3:** $(A)$ changes $|b>$ for $|b+1>$ at $a_f \ge 6$, or it doesn't change $|b>$ at $a_f < 6$. As the target state for $|b>$ is 0, $(PI)$ and $(IM)$ act on $|b>$. When $\beta$ is the minimum even integer that is $(2^{\alpha}/(2k))^{1/2} = (2^3/6)^{1/2} \approx 1.2 \leq 2 = \beta$, the total number that $(PI)$ and $(IM)$ act on $|b>$ is $\beta = 2$. Next, $(OB)$ observes $|b>$. These actions are repeated sequentially from $|a_1>$ to $|a_3>$. Therefore, each state of $|a_f>$ is 0, 1, 2, 3, 4, and 5, and the total states become $6^3[=W_0]$.

**Step 4:** $(B)$ changes $|b>$ for $|b+1>, |b-1>, |b+2>, |b-2>, |b+3>$, and $|b-3>$ at $a_1 = 0, 1, 2, 3, 4$, and 5, respectively. This action repeats to $|a_3>$. Therefore, $|b>$ becomes from $|-nd_{max}>=|-9>$ to $|nd_{max}>=|9>$.

**Step 5:** $(C_1)$ doesn't change $|c>$ in $u_1\sigma \approx 2 \leq b \leq v_1\sigma \approx 5$, or it changes $|c>$ for $|c+1>$ in the others of $b$. As the target state for $|c>$ is 0, $(PI)$ and $(IM)$ act on $|c>$. The number of the data that is included in $2 \leq b \leq 5$ is $W_1 \approx 6^3/2^2$. When $\gamma_1$ is the minimum even integer that is $(W_0/W_1)^{1/2} \approx (6^3/(6^3/2^2))^{1/2} = 2 \leq 2 = \gamma_1$, the total number that $(PI)$ and $(IM)$ act on $|c>$ is $\gamma_1 \approx 2$. Next, $(OB)$ observes $|c>$, and the data of $W_1$ remain.

$(C_2)$ doesn't change $|c>$ in $u_2\sigma \approx 4 \leq b \leq v_2\sigma \approx 5$, or it changes $|c>$ for $|c+1>$ in the others of $b$. As the target state for $|c>$ is 0. $(PI)$ and $(IM)$ act on $|c>$. The number of the data that is included in $4 \leq b \leq 5$ is $W_2 \approx 6^3/2^4$. When $\gamma_2$ is the minimum even integer that is $(W_1/W_2)^{1/2} \approx (6^3/2^2/(6^3/2^4))^{1/2} = 2 \leq 2 = \gamma_2$, the total number that $(PI)$ and $(IM)$ act on $|c>$ is $\gamma_2 \approx 2$. Next, $(OB)$ observes $|c>$, and the data of $W_2$ remain.

$(C_3)$ doesn't change $|c>$ at $b = M = 5$ $[u_3\sigma \approx 5 \leq b \leq v_3\sigma \approx 5]$, or it changes $|c>$ for $|c+1>$ in $b \neq 5$. As the target state for $|c>$ is 0, $(PI)$ and $(IM)$ act on $|c>$. The number of the data that is included at $b = 5$ is $W_3 \approx H(5) \approx 9$. When $\gamma_3$ is the minimum even integer that is $(W_2/W_3)^{1/2} \approx (13.5/9)^{1/2} \approx 1.2 \leq 2 = \gamma_3$, the total number that $(PI)$ and $(IM)$ act on $|c>$ is $\gamma_3 = 2$. Next, $(OB)$ observes $|a_1>, |a_2>, |a_3>, |b>$, and $|c>$, and one of the data of $W_3$ remain. For example, when $a_1, a_2, a_3, b$, and $c$ are 4, 1, 4, 5, and 0, respectively, it is obtained that an example of paths is $3 \to -1 \to 3$ $[3 - 1 + 3 = 5 = M]$.

## 5. Discussion and Summary

The computational complexity of this quantum algorithm $[=S]$ becomes the following. In the order of the actions by the gates, the number of them is $\alpha n$ at $\boxed{\mathrm{H}}$, $n$ at $(A)$, $\beta n = 2n$ at $(PI)$ and $(IM)$, $n$ at $(OB)$, $n$ at $(B)$, about $g$ at $(C_R)$ $[1 \leq R \leq g$. $R$ is an integer.], about $\sum_{R=1}^{g} \gamma_R = 2g$ at $(PI)$ and $(IM)$, and about $g$ at $(OB)$. Therefore, $S$ becomes about $(\alpha+5)n + 4g$. In the example of the section 4, $S$ is 36. The computational complexity of the classical computation $[=Z]$ is $(2k)^n = 6^3 = 216$. After all, $S/Z$ becomes 1/6. When $n$ is large enough, $S$ becomes about $(\alpha+5)n + 4g \approx \alpha n + 4g \approx (log_2 2k)n + 2(log_2 2k)n = 3(log_2 2k)n$, where a maximum value of $g$ is about $(n/2)log_2 2k$, and $S/Z$ is about $3(log_2 2k)n/(2k)^n \approx n/(2k)^n$. For example, as for $n = 100$ and $k = 3$, $S/Z$ is about $100/6^{100} \approx 100/10^{78} = 1/10^{76}$.

Therefore, a polynomial time process becomes possible.

## References

[1] Deutsch D., and Jozsa R., Rapid solution of problems by quantum computation, *Proc. Roy. Soc. Lond. A*, 439:553–558, 1992.

[2] Takeuchi S., Ryoshi Konpyuta (Quantum Computer), Kodansha, Tokyo, Japan, 2005 [in Japanese].

[3] Miyano K., and Furusawa A., Ryoshi Konpyuta Nyumon (An Introduction to Quantum Computation), Nihonhyoronsha, Tokyo, Japan, 2008 [in Japanese].

[4] Shor P.W., Algorithms for quantum computation: discrete logarithms and factoring, *Proc. 35th Annu. Symp. Foundations of Computer Science*, IEEE, pp. 124–134, 1994.

[5] Grover L.K., A fast quantum mechanical algorithm for database search, *Proc. 28th Annu. ACM Symp. Theory of Computing*, pp. 212–219, 1996.

[6] Grover L.K., A framework for fast quantum mechanical algorithms, *Proc. 30th Annu. ACM Symp. Theory of Computing*, pp. 53–62, 1998.

[7] Fujimura T., Quantum algorithm for vertex coloring problem by central limit theorem, *Glob. J. Pure Appl. Math.*, 7:401–405, 2011.

[8] Weisstein E.W., Random Walk–1-Dimensional, 2011, [Online], Available: http://mathworld.wolfram.com/RandomWalk1-Dimensional.html.