Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume7, Number 4 (2011), pp. 397–400

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

Quantum Algorithm for Minimum Sum of Squares Problem

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 the minimum sum of squares problem and its example are reported. When n numbers are parted by k groups, and a sum of numbers in the i-th group [$0 \leq i \leq k-1$. i is an integer.] is s_i, it is decided whether $\sum_{i=0}^{k-1} s_i^2$ is a natural number M or less or not. A computational complexity of a classical calculation is k^n. The computational complexity becomes about $k^{n/2}$ by the quantum algorithm that uses quantum phase inversion gates and quantum inversion about mean gates.

AMS Subject Classification: Primary 81-08; Secondary 68R05, 68W40.
Keywords: Quantum algorithm, minimum sum of squares problem, computational complexity.

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 knapsack problem has recently been reported by Fujimura [7]. The minimum sum of squares problem [8] is examined this time. Therefore, its result is reported.

2. Minimum Sum of Squares Problem

When n numbers are parted by k groups, and a sum of numbers in the i-th group [$0 \leq i \leq k-1$. i is an integer.] is s_i, it is decided whether $\sum_{i=0}^{k-1} s_i^2$ is a natural number M or less or not [8].

3. Quantum Algorithm

It is assumed that n numbers are $x_0, x_1, \cdots, x_{n-1}$ that are natural numbers, and when they are parted by k groups [$1 \leq k \leq n$. k is an integer.], and a sum of numbers in the i-th group [$0 \leq i \leq k-1$. i is an integer.] is s_i, it is decided whether $\sum_{i=0}^{k-1} s_i^2$ is a natural number M or less or not.

First of all, the quantum registers $|a_0>$, $|a_1>$, $\cdots$, $|a_{n-1}>$, $|b>$, $|c>$, and $|d>$ are prepared. When α is a minimum integer that is $log_2 k$ or more, each of $|a_f>$ that f is an integer from 0 to $n-1$ is consisted of α quantum bits [=qubits]. States of $|a_f>$, $|b>$, $|c>$, and $|d>$ are a_f, b, c, and d, respectively.

Step 1: Each qubit of $|a_f>$, $|b>$, $|c>$, and $|d>$ is set $|0>$.

Step 2: The Hadamard gate $\boxed{\mathrm{H}}$ [2, 3] acts on each qubit of $|a_f>$. 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 $a_f \geq k$, or it doesn't change $|b>$ at $a_f < k$. 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 β is a minimum even integer that is $(2^\alpha/k)^{1/2}$ or more, the total number that (PI) and (IM) act on $|b>$ is β because they are a couple. Next, an observation gate (OB) observes $|b>$. These actions are repeated sequentially from $|a_0>$ to $|a_{n-1}>$. Therefore, each state of $|a_f>$ is 0, 1, $\cdots$, $k-2$, or $k-1$, and the total states become k^n.

Step 4: It is assumed that a quantum gate (B_0) changes $|c>$ for $|c+x_0>$ at $a_0 = 0$, or it doesn't change $|c>$ at $a_0 \neq 0$. It changes $|c>$ for $|c+x_1>$ at $a_1 = 0$, or it doesn't change $|c>$ at $a_1 \neq 0$. This action repeats to a_{n-1}. Next, it is assumed that a quantum gate (C) changes $|d>$ for $|d+c^2>$, and $|c>$ is set $|0>$. Similarly, (B_u) [$1 \leq u \leq k-1$. u is an integer.] changes $|c>$ for $|c+x_0>$ at $a_0 = u$, or it doesn't change $|c>$ at $a_0 \neq u$. It changes $|c>$ for $|c+x_1>$ at $a_1 = u$, or it doesn't change $|c>$ at $a_1 \neq u$. This action repeats to a_{n-1}. Next, (C) changes $|d>$ for $|d+c^2>$, and $|c>$ is set $|0>$. These actions are repeated sequentially from 1 to $k-1$ at u.

Step 5: It is assumed that a quantum gate (D) changes $|b>$ for $|b+1>$ at $d > M$, or it doesn't change $|b>$ at $d \leq M$. As a target state for $|b>$ is 0, (PI) and (IM) act on $|b>$. When γ is a minimum even integer that is $k^{n/2}$ or more, the total number that (PI) and

(IM) act on $|b>$ is γ. Next, (OB) observes $|a_0>, |a_1>, \cdots, |a_{n-1}>, |b>, |c>$, and $|d>$. By these actions, $a_0, a_1, \cdots, a_{n-1}, b, c$, and d are obtained. Therefore, when b is 0, optimal k groups are obtained.

4. Numerical Calculation

It is assumed that there are $n = 12, x_0 = 5, x_1 = 2, x_2 = 7, x_3 = 11, x_4 = 6, x_5 = 9, x_6 = 3, x_7 = 8, x_8 = 12, x_9 = 1, x_{10} = 10, x_{11} = 4, k = 5$, and $M = 1219$.

First of all, $|a_0>, |a_1>, \cdots, |a_{11}>, |b>, |c>$, and $|d>$ are prepared. As $log_2 k$ is $log_2 5 \approx 2.3 \leq 3 = \alpha$, each of $|a_f>$ that f is an integer from 0 to 11 is consisted of 3 qubits.

Step 1: Each qubit of $|a_f>, |b>, |c>$, and $|d>$ is set $|0>$.

Step 2: $\boxed{\text{H}}$ acts on each qubit of $|a_f>$. It changes them for entangled states. The total states are $(2^\alpha)^n = (2^3)^{12}$.

Step 3: (A) changes $|b>$ for $|b+1>$ at $a_f \geq 5$, or it doesn't change $|b>$ at $a_f < 5$. As a target state for $|b>$ is 0, (PI) and (IM) act on $|b>$. When β is a minimum even integer that is $(2^\alpha/k)^{1/2} = (2^3/5)^{1/2} \approx 1.3 \leq 2 = \beta$, the total number that (PI) and (IM) act on $|b>$ is 2. Next, (OB) observes $|b>$. These actions are repeated sequentially from $|a_0>$ to $|a_{11}>$. Therefore, each state of $|a_f>$ is 0, 1, 2, 3, or 4, and the total states become $k^n = 5^{12}$.

Step 4: (B_0) changes $|c>$ for $|c + x_0>$ at $a_0 = 0$, or it doesn't change $|c>$ at $a_0 \neq 0$. It changes $|c>$ for $|c + x_1>$ at $a_1 = 0$, or it doesn't change $|c>$ at $a_1 \neq 0$. This action repeats to a_{11}. Next, it is assumed that (C) changes $|d>$ for $|d + c^2>$, and $|c>$ is set $|0>$. Similarly, (B_u) $[1 \leq u \leq 4]$ changes $|c>$ for $|c + x_0>$ at $a_0 = u$, or it doesn't change $|c>$ at $a_0 \neq u$. It changes $|c>$ for $|c + x_1>$ at $a_1 = u$, or it doesn't change $|c>$ at $a_1 \neq u$. This action repeats to a_{11}. Next, (C) changes $|d>$ for $|d + c^2>$, and $|c>$ is set $|0>$. These actions are repeated sequentially from 1 to 4 at u.

Step 5: (D) changes $|b>$ for $|b+1>$ at $d > M = 1219$, it doesn't change $|b>$ at $d \leq M$. As a target state for $|b>$ is 0, (PI) and (IM) act on $|b>$. When γ is a minimum even integer that is $k^{n/2} = 5^6 = 15625 \leq 15626 = \gamma$, the total number that (PI) and (IM) act on $|b>$ is $\gamma = 15626$. Next, (OB) observes $|a_0>, |a_1>, \cdots, |a_{11}>, |b>, |c>$, and $|d>$. For example, when $a_0, a_1, \cdots, a_{11}, b, c$, and d are 2, 1, 3, 2, 0, 3, 4, 4, 1, 1, 0, 4, 0, 0, and 1218, respectively, it is obtained that a total sum is 1218, and combinations from the 0th group to the 4th group are $(x_4 = 6, x_{10} = 10)$, $(x_1 = 2, x_8 = 12, x_9 = 1)$, $(x_0 = 5, x_3 = 11)$, $(x_2 = 7, x_5 = 9)$, and $(x_6 = 3, x_7 = 8, x_{11} = 4)$, respectively.

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 αn at $\boxed{\mathrm{H}}$, n at (A), $\beta n = 2n$ at (PI) and (IM), n at (OB), kn at (B_v) [$0 \leq v \leq k-1$. v is an integer.], k at (C), 1 at (D), γ at (PI) and (IM), and 1 at (OB). Therefore, S becomes $(k+\alpha+4)n+k+\gamma+2$. In the example of the section 4, S is 15777. The computational complexity of the classical calculation [$= Z$] is $k^n = 5^{12} \approx 2.4 \times 10^8$. After all, S/Z becomes about $1/(1.5 \times 10^4)$. When n is large enough, S becomes about $\gamma \approx k^{n/2}$, and S/Z is about $1/(k^{n/2})$. For example, as for $k = 5$ and $n = 100$, S/Z is about $1/(8.9 \times 10^{34})$.

Therefore, a high-speed 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 knapsack problem, *Glob. J. Pure Appl. Math.*, 6:263–266, 2010.

[8] Crescenzi P., and Kann V., Eds., A compendium of NP optimization problems, 2005 [Online], Available: http://www.csc.kth.se/~viggo/wwwcompendium/.