Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 10, Number 1 (2014), pp. 145-148

http://www.ripublication.com

Quantum Algorithm for Minimum Sum of Squares Problem by Numbering Method

Toru Fujimura

Department of Chemistry, 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 by a numbering method 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 $\sum_{i=0 \to k-1} {s_i}^2$ is a natural number M or less or not. A computational complexity of a classical computation is k^n. The computational complexity becomes about $3(log_2 k)n$ by the quantum algorithm that uses quantum phase inversion gates, quantum inversion about mean gates and the numbering method. Therefore, a polynomial time process becomes possible.

***AMS subject classification*:** Primary 81-08; Secondary 68R05, 68W40.

***Keywords*:** Quantum algorithm, minimum sum of squares problem, numbering method, computational complexity, polynomial time.

1. Introduction

Haroche and Wineland [1] made the very first steps towards building a quantum computer. On the other hand, Deutsch and Jozsa [2−4] discovered the quantum algorithm of a high-speed process by a parallel computation that uses quantum entangled states. After that, Shor [3−5] found the method of solving the factoring in a polynomial time, and Grover [3, 6, 7] showed the algorithm for the database search in a square root time. A quantum algorithm for the traveling salesman problem by a numbering method has recently been reported by Fujimura [8]. Its computational complexity becomes a polynomial time. The minimum sum of squares problem [9, 10] is examined by the numbering method 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 $\sum_{i=0\rightarrow k-1} s_i{}^2$ is a natural number M or less or not.

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, and a sum of numbers in the i-th group [$0 \leq i \leq k - 1$. i is the integer.] is s_i, it is decided whether $\sum_{i=0\rightarrow k-1} s_i{}^2$ is the natural number M or less or not. Therefore, it is assumed that T is the minimum integer that follows $(1/k)\sum_{j=0\rightarrow n-1} x_j \leq (M/k)^{1/2} \leq T$. When the number of the n times repeated permutation of 0, 1, $\cdots$, $k - 2$ and $k - 1$ is k^n, $a_0\ k^{n-1} + a_1\ k^{n-2} + \cdots + a_{n-1}\ k^0 = \sum_{j=0\rightarrow n-1} a_j\ k^{n-1-j} = U$ is the numbering datum from 0 to $k^n - 1$ [The 0-th datum is 0, 0, $\cdots$, 0 and 0. The $(k^n - 1)$-th datum is $(k - 1)$, $(k - 1)$, $\cdots$, $(k - 1)$ and $(k - 1)$.]. This method is named the numbering method for this problem. g is the minimum integer that follows $k^n/k! \leq 4^g = 2^{2g}$, because a number of combinations of an answer is at least $k!$.

First of all, quantum registers $|a_0\rangle$, $|a_1\rangle$, $\cdots$, $|a_{n-1}\rangle$, $|b_1\rangle$, $|b_2\rangle$, $|c_0\rangle$, $|c_1\rangle$, $\cdots$, $|c_{k-1}\rangle$, $|d\rangle$, $|e_1\rangle$ and $|e_2\rangle$ are prepared. When □ is the minimum integer that is $log_2\ k$ or more, each of $|a_j\rangle$ that j is an integer from 0 to $n-1$ is consisted of □ quantum bits [= qubits]. States of $|a_j\rangle$, $|b_1\rangle$, $|b_2\rangle$, $|c_i\rangle$, $|d\rangle$, $|e_1\rangle$ and $|e_2\rangle$ are a_j, b_1, b_2, c_1, c_i, d, e_1 and e_2, respectively.

Step 1: Each qubit of $|a_j\rangle$, $|b_1\rangle$, $|b_2\rangle$, $|c_i\rangle$, $|d\rangle$, $|e_1\rangle$ and $|e_2\rangle$ is set $|0\rangle$.

Step 2: The Hadamard gate H [3, 4] acts on each qubit of $|a_j\rangle$. It changes them for entangled states. The total states are $(2^{□})^n$.

Step 3: It is assumed that a quantum gate (A) changes $|b_1\rangle$ for $|1\rangle$ in $a_j < k$, or it changes $|b_1\rangle$ for $|0\rangle$ in the others of a_j, it changes $|b_2\rangle$ for $|b_2 + a_j\ k^{n-1-j}\rangle$ at $|a_j\rangle$, and it changes $|c_i\rangle$ for $|c_i + x_j\rangle$ at $a_j = i$. As a target state for $|b_1\rangle$ is 1, quantum phase inversion gates (PI) and quantum inversion about mean gates (IM) [3, 6, 7] act on $|b_1\rangle$. When β is the minimum even integer that is $(2^{□}/k)^{1/2}$ or more, the total number that (PI) and (IM) act on $|b_1\rangle$ is β because they are a couple. Next, an observation gate (OB) observes $|b_1\rangle$. These actions are repeated sequentially from $|a_0\rangle$ to $|a_{n-1}\rangle$. Therefore, each state of $|a_j\rangle$ is 0, 1, $\cdots$, $k - 2$ and $k - 1$, and the total states become k^n [$=W_0$].

Step 4: It is assumed that a quantum gate (B) changes $|d\rangle$ for $|d + 1\rangle$ in $c_i \leq T$, or it doesn't change $|d\rangle$ in the others of c_i. These actions are repeated sequentially from $|c_0\rangle$ to $|c_{k-1}\rangle$.

Step 5: It is assumed that a quantum gate (C) changes $|e_1\rangle$ for $|e_1 + 0\rangle$ at $d = k$, or it changes $|e_1\rangle$ for $|e_1 + 1 + b_2\rangle$ in the others of d.

Step 6: It is assumed that a quantum gate (D_1) changes $|e_2\rangle$ for $|1\rangle$ in $0 \leq e_1 \leq (k^n/4) - k!$, or it changes $|e_2\rangle$ for $|0\rangle$ in the others of e_1. As the target state for $|e_2\rangle$ is 1, (PI) and (IM) act on $|e_2\rangle$. The number of the data that is included in $0 \leq e_1 \leq (k^n/4) - k!$ is $W_1 \approx k^n/4$. When γ_1 is the minimum even integer that is $(W_0/W_1)^{1/2} \approx (k^n/(k^n/4))^{1/2}$ or more, the total number that (PI) and (IM) act on $|e_2\rangle$ is $\gamma_1 \approx 2$. Next, (OB) observes $|e_2\rangle$, and the data of W_1 remain. Similarly, (D_f) [$2 \leq f \leq g - 1$. f is an integer.] changes $|e_2\rangle$ for $|1\rangle$ in $0 \leq e_1 \leq (k^n/4^f) - k!$, or it changes $|e_2\rangle$ for $|0\rangle$ in the others of e_1. As the target state for $|e_2\rangle$ is 1, (PI) and (IM) act on $|e_2\rangle$. The number of the data that is included in $0 \leq e_1 \leq (k^n/4^f) - k!$ is $W_f \approx k^n/4^f$. When γ_f is the minimum even integer that is $(W_{f-1}/W_f)^{1/2} \approx ((k^n/4^{f-1})/(k^n/4^f))^{1/2}$ or more, the total number that (PI) and (IM) act on

$|e_2\rangle$ is $\gamma_f \approx 2$. Next, (*OB*) observes $|e_2\rangle$, and the data of W_f remain. These actions are repeated sequentially from 2 to $g - 1$ at *f*. (D_g) changes $|e_2\rangle$ for $|1\rangle$ at $e_1 = 0$, or it changes $|e_2\rangle$ for $|0\rangle$ in the others of e_1. As the target state for $|e_2\rangle$ is 1, (*PI*) and (*IM*) act on $|e_2\rangle$. The number of the data that is included at $e_1 = 0$ is $W_g \approx k! \approx k^n/4^g$. When γ_g is the minimum even integer that is $(W_{g-1}/W_g)^{1/2} \approx ((k^n/4^{g-1})/(k^n/4^g))^{1/2}$ or more, the total number that (*PI*) and (*IM*) act on $|e_2\rangle$ is $\gamma_g \approx 2$. Next, (*OB*) observes $|a_j\rangle$, $|b_1\rangle$, $|b_2\rangle$, $|c_i\rangle$, $|d\rangle$, $|e_1\rangle$ and $|e_2\rangle$, and one of the data of W_g remains. Therefore, one example of combinations that are $c_i \leq T$ is obtained.

4. Numerical Computation

It is assumed that there are $n = 11$, $x_0 = 4$, $x_1 = 8$, $x_2 = 10$, $x_3 = 2$, $x_4 = 6$, $x_5 = 12$, $x_6 = 7$, $x_7 = 11$, $x_8 = 5$, $x_9 = 3$, $x_{10} = 9$, $k = 5$, $M = 1190$, $T = 16$, $g = 10$, $0 \leq i \leq 4$ [*i* is the integer.] and $0 \leq j \leq 10$ [*j* is the integer.].

First of all, $|a_j\rangle$, $|b_1\rangle$, $|b_2\rangle$, $|c_i\rangle$, $|d\rangle$, $|e_1\rangle$ and $|e_2\rangle$ are prepared. When □ is the minimum integer that is $log_2 5 \approx 2.3 \leq 3 =$ □, each of $|a_j\rangle$ that *j* is the integer from 0 to 10 is consisted of 3 qubits. States of $|a_j\rangle$, $|b_1\rangle$, $|b_2\rangle$, $|c_i\rangle$, $|d\rangle$, $|e_1\rangle$ and $|e_2\rangle$ are a_j, b_1, b_2, c_i, d, e_1, and e_2, respectively.

Step 1: Each qubit of $|a_j\rangle$, $|b_1\rangle$, $|b_2\rangle$, $|c_i\rangle$, $|d\rangle$, $|e_1\rangle$ and $|e_2\rangle$ is set $|0\rangle$.

Step 2: H acts on each qubit of $|a_j\rangle$. It changes them for entangled states. The total states are $(2^3)^{11}$.

Step 3: (*A*) changes $|b_1\rangle$ for $|1\rangle$ in $a_j < 5$, or it changes $|b_1\rangle$ for $|0\rangle$ in the others of a_j, it changes $|b_2\rangle$ for $|b_2 + a_j\, 5^{10-j}\rangle$ at $|a_j\rangle$, and it changes $|c_i\rangle$ for $|c_i + x_j\rangle$ at $a_j = i$. As the target state for $|b_1\rangle$ is 1, (*PI*) and (*IM*) act on $|b_1\rangle$. When β is the minimum even integer that is $(2^3/5)^{1/2} \approx 1.265 \leq 2 = \beta$, the total number that (*PI*) and (*IM*) act on $|b_1\rangle$ is $\beta \approx 2$. Next, (*OB*) observes $|b_1\rangle$. These actions are repeated sequentially from $|a_0\rangle$ to $|a_{10}\rangle$. Therefore, each state of $|a_j\rangle$ is 0, 1, 2, 3 or 4, and the total states become 5^{11} [$= W_0$].

Step 4: (*B*) changes $|d\rangle$ for $|d + 1\rangle$ in $c_i \leq 16$, or it doesn't change $|d\rangle$ in the others of c_i. These actions are repeated sequentially from $|c_0\rangle$ to $|c_4\rangle$.

Step 5: (*C*) changes $|e_1\rangle$ for $|e_1 + 0\rangle$ at $d = 5$, or it changes $|e_1\rangle$ for $|e_1 + 1 + b_2\rangle$ in the others of *d*.

Step 6: (D_1) changes $|e_2\rangle$ for $|1\rangle$ in $0 \leq e_1 \leq (5^{11}/4) - 5!$, or it changes $|e_2\rangle$ for $|0\rangle$ in the others of e_1. As the target state for $|e_2\rangle$ is 1, (*PI*) and (*IM*) act on $|e_2\rangle$. The number of the data that is included in $0 \leq e_1 \leq (5^{11}/4) - 5!$ is $W_1 \approx 5^{11}/4$. When γ_1 is the minimum even integer that is $(W_0/W_1)^{1/2} \approx (5^{11}/(5^{11}/4))^{1/2} \approx 2 \leq 2 = \gamma_1$, the total number that (*PI*) and (*IM*) act on $|e_2\rangle$ is $\gamma_1 \approx 2$. Next, (*OB*) observes $|e_2\rangle$, and the data of W_1 remain. Similarly, (D_f) [$2 \leq f \leq 9$. *f* is the integer.] changes $|e_2\rangle$ for $|1\rangle$ in $0 \leq e_1 \leq (5^{11}/4^f) - 5!$, or it changes $|e_2\rangle$ for $|0\rangle$ in the others of e_1. As the target state for $|e_2\rangle$ is 1, (*PI*) and (*IM*) act on $|e_2\rangle$. The number of the data that is included in $0 \leq e_1 \leq (5^{11}/4^f) - 5!$ is $W_f \approx 5^{11}/4^f$. When γ_f is the minimum even integer that is $(W_{f-1}/W_f)^{1/2} \approx ((5^{11}/4^{f-1})/(5^{11}/4^f))^{1/2} \approx 2 \leq 2 = \gamma_f$, the total number that (*PI*) and (*IM*) act on $|e_2\rangle$ is $\gamma_f \approx 2$. Next, (*OB*) observes $|e_2\rangle$, and the data of W_f remain. These actions are repeated sequentially from 2 to 9 at *f*. (D_{10}) changes $|e_2\rangle$ for $|1\rangle$ at $e_1 = 0$, or it changes $|e_2\rangle$ for $|0\rangle$ in the others of e_1. As the target state for $|e_2\rangle$ is 1, (*PI*) and (*IM*) act on $|e_2\rangle$. The number of the data that is included at $e_1 = 0$ is $W_{10} \approx 5! \approx 5^{11}/4^{10}$. When γ_{10} is the minimum even integer that is $(W_9/W_{10})^{1/2} \approx ((5^{11}/4^9)/(5^{11}/4^{10}))^{1/2} \approx 2 \leq 2 = \gamma_{10}$, the total

number that (*PI*) and (*IM*) act on $|e_2\rangle$ is $\gamma_{10} \approx 2$. Next, (*OB*) observes $|a_j\rangle$, $|b_1\rangle$, $|b_2\rangle$, $|c_i\rangle$, $|d\rangle$, $|e_1\rangle$ and $|e_2\rangle$, and one of the data of W_{10} remains. For example, when a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, b_1, b_2, c_0, c_1, c_2, c_3, c_4, d, e_1 and e_2 are 3, 4, 0, 4, 0, 2, 1, 3, 4, 2, 1, 1, $\sum_{j=0\to10} a_j 5^{10-j}$, 16, 16, 15, 15, 15, 5, 0 and 1, respectively, it is obtained that 5 groups are (10, 6), (7, 9), (12, 3), (4, 11) and (8, 2, 5).

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 □*n* at H, *n* at (*A*), $\beta n \approx 2n$ at (*PI*) and (*IM*), *n* at (*OB*), *k* at (*B*), 2 at (*C*), *g* at (D_f) [$1 \le f \le g$. *f* is the integer.], $\sum_{f=1\to g} \gamma_f \approx 2g$ at (*PI*) and (*IM*), and *g* at (*OB*). Therefore, *S* becomes (□ + 4)*n* + *k* + 2 + 4*g*. In the example of the section 4, *S* is 124. The computational complexity of the classical computation [= *Z*] is $k^n = 5^{11} \approx 5\times10^7$. After all, *S*/*Z* becomes about $1/(4\times10^5)$. When *n* is large enough, *S* becomes about $3(log_2\, k)n$, where □ is about $log_2\, k$, *g* is about $(1/2)log_2\,(k^n/k!) \approx (n/2)log_2\, k$, and *k*! is about $k^k e^{-k}(2k)^{1/2}$ [Stirling's formula]. And then, *S*/*Z* is about $3(log_2\, k)n/k^n \approx n/k^n$. For example, as for $n = 100$ and $k = 5$, *S*/*Z* is about $100/5^{100} \approx 1/10^{68}$.

Therefore, the polynomial time process becomes possible.

References

[1] Kungl. Vetenskapsakademien (The Royal Swedish Academy of Sciences), The Nobel Prize in Physics 2012, [On line], Available: http: //www. kva. se /en /pressroom /Press-releases-2012 /The-Nobel-Prize-in-Physics-2012/, 2012.

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

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

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

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

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

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

[8] Fujimura T., Quantum algorithm for traveling salesman problem by numbering method, *Glob. J. Pure Appl. Math.*, 9:545-551, 2013.

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

[10] Fujimura T., Quantum algorithm for minimum sum of squares problem by central limit theorem, *Glob. J. Pure Appl. Math.*, 7:407-413, 2011.