Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 9, Number 3 (2013), pp. 301–305

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

Quantum Algorithm for Partition 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 partition problem by a numbering method and its example are reported. When n natural numbers are parted by two groups, it is decided whether a sum of natural numbers of one group is equal to it of another group or not. A computational complexity of a classical computation is $2^n - 1$. The computational complexity becomes about $4n$ 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, partition problem, numbering method, computational complexity, polynomial time.

1. Introduction

The methods for the very first steps towards building a quantum computer were developed by Haroche and Wineland [1]. Deutsch-Jozsa's algorithm for the rapid solution [2–4], Shor's algorithm for the factorization [3–5], Grover's algorithms for the database search [3,6,7] and so on are known. A quantum algorithm for the traveling salesman problem by a numbering metod has recently been reported by Fujimura [8]. Its computational complexity becomes a polynomial time. The partition problem [9,10] is examined by the numbering method this time. Therefore, its result is reported.

2. Partition Problem

When n natural numbers are parted by two groups, it is decided whether a sum of numbers of one group is equal to it of another group or not.

3. Quantum Algorithm

It is assumed that n natural numbers are x_i $[1 \le i \le n.\ i$ is an integer.], M is $(1/2)\sum_{i=1}^{n} x_i$, and a_i $[1 \le i \le n.\ i$ is the integer.] is 0 or 1. When the number of the n times repeated permutation of 0 and 1 is 2^n, $a_1 2^{n-1} + a_2 2^{n-2} + \cdots + a_n 2^0 = \sum_{i=1}^{n} a_i 2^{n-i} = U$ is the numbering datum from 0 to $2^n - 1$ [The 0-th datum is $0, 0, \cdots, 0$ and 0. The $(2^n - 1)$-th datum is $1, 1, \cdots, 1$ and 1.]. This method is named the numbering method for this problem. g is the minimum integer that follows $(n-1)/2 \le g$ $[2^n/2 = 2^{n-1} \le 4^g = 2^{2g}]$, because a number of combinations of an answer is 2 at least.

First of all, quantum registers $|a_1>, |a_2>, \cdots, |a_n>, |b_1>, |b_2>, |c>$ and $|d>$ are prepared. States of $|a_1>, |a_2>, \cdots, |a_n>, |b_1>, |b_2>, |c>$ and $|d>$ are $a_1, a_2, \cdots, a_n, b_1, b_2, c$ and d, respectively.

Step 1: Each quantum bit [=qubit] of $|a_1>, |a_2>, \cdots, |a_n>, |b_1>, |b_2>, |c>$ and $|d>$ is set $|0>$.

Step 2: The Hadamard gate $\boxed{\mathrm{H}}$ [3, 4] 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 $2^n[= W_0]$.

Step 3: It is assumed that a quantum gate (A) changes $|b_1>$ and $|b_2>$ for $|b_1 + a_i x_i>$ and $|b_2 + a_i 2^{n-i}>$, respectively, at $|a_i>$. These actions are repeated sequentially from $|a_1>$ to $|a_n>$. Therefore, $|b_1>$ and $|b_2>$ become $|\sum_{i=1}^{n} a_i x_i>$ and $|\sum_{i=1}^{n} a_i 2^{n-i} = U>$, respectively.

Step 4: It is assumed that a quantum gate (B) doesn't change $|c>$ at $b_1 = M$, or it changes $|c>$ for $|c + 1 + b_2>$ in others of b_1 from $|b_1>$ and $|b_2>$.

Step 5: It is assumed that a quantum gate (C_1) changes $|d>$ for $|1>$ in $0 \le c \le (2^n/4) - 2$, or it changes $|d>$ for $|0>$ in the others of c. As the target state for $|d>$ is 1, quantum phase inversion gates (PI) and quantum inversion about mean gates (IM) [3,6,7] act on $|d>$. The number of the data that is included in $0 \le c \le (2^n/4) - 2$ is $W_1 \approx 2^n/4$. When γ_1 is the minimum even integer that is $(W_0/W_1)^{1/2}$ or more, the total number that (PI) and (IM) act on $|d>$ is $\gamma_1 \approx 2$

because they are a couple. Next, an observation gate (OB) observes $|d>$, and the data of W_1 remain.

Similarly, (C_i) [$2 \leq i \leq g-1$. i is the integer.] changes $|d>$ for $|1>$ in $0 \leq c \leq (2^n/4^i)-2$, or it changes $|d>$ for $|0>$ in others of c. As the target state for $|d>$ is 1, (PI) and (IM) act on $|d>$. The number of the data that is included in $0 \leq c \leq (2^n/4^i)-2$ is $W_i \approx 2^n/4^i$. When γ_i is the minimum even integer that is $(W_{i-1}/W_i)^{1/2}$ or more, the total number that (PI) and (IM) act on $|d>$ is $\gamma_i \approx 2$. Next, (OB) observes $|d>$, and the data of W_i remain. These actions are repeated sequentially from 2 to $g-1$ at i.

(C_g) changes $|d>$ for $|1>$ at $c=0$, or it changes $|d>$ for $|0>$ in the others of c. As the target state for $|d>$ is 1, (PI) and (IM) act on $|d>$. The number of the data that is included at $c=0$ is $W_g \approx 2^n/4^g \approx 2$. When γ_g is the minimum even integer that is $(W_{g-1}/W_g)^{1/2}$ or more, the total number that (PI) and (IM) act on $|d>$ is $\gamma_g \approx 2$. Next, (OB) observes $|a_1>, |a_2>, \cdots, |a_n>, |b_1>, |b_2>, |c>$ and $|d>$, and one of the data of W_g remains. Therefore, one example of combinations that are $b_1 = M$ is obtained.

4. Numerical Computation

It is assumed that there are $n=7, x_1=15, x_2=3, x_3=2, x_4=7, x_5=10, x_6=13, x_7=16, M=33$ and $g=3$ [$(7-1)/2=3 \leq 3=g$].

First of all, $|a_1>, |a_2>, \cdots, |a_7>, |b_1>, |b_2>, |c>$ and $|d>$ are prepared. States of $|a_1>, |a_2>, \cdots, |a_7>, |b_1>, |b_2>, |c>$ and $|d>$ are $a_1, a_2, \cdots, a_7, b_1, b_2, c$ and d, respectively.

Step 1: Each qubit of $|a_1>, |a_2>, \cdots, |a_7>, |b_1>, |b_2>, |c>$ and $|d>$ is set $|0>$.

Step 2: $\boxed{\text{H}}$ acts on each qubit of $|a_1>, |a_2>, \cdots, |a_6>$ and $|a_7>$. It changes them for entangled states. The total states are $2^7[=W_0]$.

Step 3: (A) changes $|b_1>$ and $|b_2>$ for $|b_1+a_ix_i>$ and $|b_2+a_i2^{n-i}>$, respectively, at $|a_i>$. These actions are repeated sequentially from $|a_1>$ to $|a_n>$. Therefore, $|b_1>$ and $|b_2>$ become $|\sum_{i=1}^{7} a_ix_i>$ and $|\sum_{i=1}^{7} a_i2^{7-i} = U>$, respectively.

Step 4: (B) doesn't change $|c>$ in $b_1=33$, or it changes $|c>$ for $|c+1+b_2>$ in the others of b_1 from $|b_1>$ and $|b_2>$.

Step 5: (C_1) changes $|d>$ for $|1>$ in $0 \leq c \leq (2^7/4)-2$, or it changes $|d>$ for $|0>$ in the others of c. As the target state for $|d>$ is 1, (PI) and (IM) act on $|d>$. The number of the data that is included in $0 \leq c \leq (2^7/4)-2$ is $W_1 \approx 2^7/4$. When γ_1 is the minimum even integer that is $(W_0/W_1)^{1/2}$ or more, the total number that (PI) and (IM) act on $|d>$ is $\gamma_1 \approx 2$. Next, (OB) observes $|d>$, and the data of W_1 remain.

(C_2) changes $|d>$ for $|1>$ in $0 \leq c \leq (2^7/4^2) - 2$, or it changes $|d>$ for $|0>$ in the others of c. As the target state for $|d>$ is 1, (PI) and (IM) act on $|d>$. The number of the data that is included in $0 \leq c \leq (2^7/4^2) - 2$ is $W_2 \approx 2^7/4^2$. When γ_2 is the minimum even integer that is $(W_1/W_2)^{1/2}$ or more, the total number that (PI) and (IM) act on $|d>$ is $\gamma_2 \approx 2$. Next, (OB) observes $|d>$, and the data of W_2 remain.

(C_3) changes $|d>$ for $|1>$ at $c = 0$, or it changes $|d>$ for $|0>$ in others of c. As the target state for $|d>$ is 1, (PI) and (IM) act on $|d>$. The number of the data that is included at $c = 0$ is $W_3 \approx 2^7/4^3 \approx 2$. When γ_3 is the minimum even integer that is $(W_2/W_3)^{1/2}$ or more, the total number that (PI) and (IM) act on $|d>$ is $\gamma_3 \approx 2$. Next, (OB) observes $|a_1>, |a_2>, \cdots, |a_7>, |b_1>, |b_2>, |c>$ and $|d>$, and one of the data of W_3 remains. For example, when $a_1, a_2, a_3, a_4, a_5, a_6, a_7, b_1, b_2, c$ and d are 0, 1, 0, 1, 1, 1, 0, 33, 46, 0 and 1 , respectively, it is obtained that $a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5 + a_6x_6 + a_7x_7$ is $0\times15+1\times3+0\times2+1\times7+1\times10+1\times13+0\times16 = 33 = M$.

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 n at $\boxed{\mathrm{H}}$, n at (A), 2 at (B), g at (C_i) [$1 \leq i \leq g$. i is the integer.], $\sum_{i=1}^{g} \gamma_i \approx 2g$ at (PI) and (IM), and g at (OB). Therefore, S becomes $2n + 2 + 4g$. In the example of the section 4, S is 28. The computational complexity of the classical computation [$= Z$] is $2^n - 1 = 2^7 - 1 = 127$. After all, S/Z becomes about 1/4. When n is large enough, S becomes about $2n + 2 + 2(n - 1) = 4n$, where g is about $(n - 1)/2$, and S/Z is about $4n/2^n \approx n/2^n$. For example, as for $n = 100$, S/Z is about $100/2^{100} \approx 1/10^{28}$.

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, 2013, [to be published].

[9] Karp R.M., Reducibility Among Combinatorial Problems, Complexity of Computer Computations, Ed. , Miller R.E., and Thatcher J.W., Plenum Press, New York, U.S.A., pp. 85–103, 1972.

[10] Fujimura T., Quantum algorithm for partition problem by central limit theorem, *Glob. J. Pure Appl. Math.*, 7:415–419, 2011.