Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 9, Number 6 (2013), pp. 539–544

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

Quantum Algorithm for Perfect Matching Problem by Numbering Method

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 perfect matching problem by a numbering method and its example are reported. When each of two groups is consisted of n persons, it is decided whether there are n pairs or not. A computational complexity of a classical computation is $n!$. The computational complexity becomes about $3(log_2 n)n$ 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 68R10, 68W40.
Keywords: Quantum algorithm, perfect matching problem, numbering method, computational complexity, polynomial time.

1. Introduction

The very first steps towards building a quantum computer were made 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 vertex coloring problem by the central limit theorem has recently been reported by Fujimura [8]. Its computational complexity becomes a polynomial time. The perfect matching problem [9] is examined this time. Therefore, its result is reported.

2. Perfect Matching Problem

When each of two groups is consisted of n persons, it is decided whether there are n pairs or not.

3. Quantum Algorithm

It is assumed that there are the s-th person M_s [$1 \leq s \leq n$. s is an integer.] in one group and the t-th person F_t [$1 \leq t \leq n$. t is an integer.] in another group. When M_s selects F_t, $x_{s,t}$ is 1, or when M_s doesn't select F_t, $x_{s,t}$ is 0. When F_t selects M_s, $y_{t,s}$ is 1, or when F_t doesn't select M_s, $y_{t,s}$ is 0.

(1) The number of the repeated permutation of n persons is n^n.

(2) The number of the permutation of n persons is $n!$.

When n persons are $M_1(F_{a_1}), M_2(F_{a_2}), \cdots, M_{n-1}(F_{a_{n-1}})$ and $M_n(F_{a_n})$, $a_1 n^{n-1} + a_2 n^{n-2} + \cdots + a_{n-1} n^1 + a_n n^0 = U$ is the numbering datum from 0 to $n^n - 1$ [The 0-th datum is $0, 0, \cdots, 0$ and 0. The $(n^n - 1)$-th datum is $(n-1), (n-1), \cdots, (n-1)$ and $(n-1)$.] in (1). In (2), it is assumed that the first datum is $0, 1, \cdots, n-1$, and the $n!$-th datum is $(n-1), (n-2), \cdots, 0$, the V-th datum is obtained from $v_1(n-1)! + v_2(n-2)! + \cdots + v_{n-1}1!$. Each of φ_i [$1 \leq i \leq n$. i is an integer.] is 1 piece of permutation from 0 to $n-1$. When v_i is 0 from $i = 1$ to $i = n-2$ sequentially, φ_i is the smallest number in remained numbers. When v_i isn't 0 from $i = 1$ to $i = n-2$ sequentially, and $v_{i+1}, v_{i+2}, \cdots, v_{n-2}$ and v_{n-1} are 0, φ_i is the v_i-th small number in remained numbers, and $\varphi_{i+1} > \varphi_{i+2} > \cdots > \varphi_{n-1} > \varphi_n$ is selected in remained numbers. When v_i isn't 0 from $i = 1$ to $i = n-2$ sequentially, and there are $v_{i+1} \neq 0$ or $v_{i+2} \neq 0$ or $\cdots$ or $v_{n-2} \neq 0$ or $v_{n-1} \neq 0$, φ_i is the $(v_i + 1)$-th small number in remained numbers. When v_{n-1} is 1, $\varphi_{n-1} < \varphi_n$ is selected in remained numbers. Therefore, $\varphi_1 n^{n-1} + \varphi_2 n^{n-2} + \cdots + \varphi_{n-1} n^1 + \varphi_n n^0$ is $U(V)$. This method is named a numbering method for this problem. g that is the minimum integer follows $n!/1 \leq 2^{2g} = 4^g$. $U(V = 1), U(V = (n!/4) - 1), U(V = (n!/16) - 1), \cdots, U(V = (n!/4^{g-1}) - 1)$ and $U(V = n!/4^g)$ are computated.

Next, a quantum algorithm is shown as the following.

First of all, quantum registers $|a_1>, |a_2>, \cdots, |a_n>, |b_1>, |b_2>, \cdots, |b_{n-1}>, |c_1>, |c_2>, |d>$ and $|e>$ are prepared. When α is the minimum integer that is $log_2 n$ or more, each of $|a_f>$ that f is an integer from 1 to n is consisted of α quantum bits [= qubits]. States of $|a_1>, |a_2>, \cdots, |a_n>, |b_1>, |b_2>, \cdots, |b_{n-1}>, |c_1>, |c_2>, |d>$ and $|e>$ are $a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_{n-1}, c_1, c_2, d$ and e, respectively.

Step 1: Each qubit of $|a_1>, |a_2>, \cdots, |a_n>, |b_1>, |b_2>, \cdots, |b_{n-1}>, |c_1>, |c_2>, |d>$ and $|e>$ is set $|0>$.

Step 2: The Hadamard gate $\boxed{\text{H}}$ [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 $(2^\alpha)^n$.

Step 3: It is assumed that a quantum gate (A) doesn't change $|b_1>$ in $a_f < n$, or it changes $|b_1>$ for $|b_1 + 1>$ in the others of a_f. As a target state for $|b_1>$ is 0, quantum phase inversion gates (PI) and quantum inversion about mean gates (IM) [3, 6, 7] act on $|b_1>$. When β is the minimum even integer that is $(2^\alpha/n)^{1/2}$ or more, the total number that (PI) and (IM) act on $|b_1>$ is β, because they are a couple. Next, an observation gate (OB) observes $|b_1>$. These actions are repeated sequentially from $|a_1>$ to $|a_n>$. Therefore, each state of $|a_f>$ is $0, 1, \cdots, n-2$ and $n-1$, and the total states become n^n.

Step 4: It is assumed that a quantum gate (B) changes $|b_1>, |b_2>, \cdots, |b_{n-2}>$ and $|b_{n-1}>$ for $|b_1+1>, |b_2+1>, \cdots, |b_{n-2}+1>$ and $|b_{n-1}+1>$ in $a_f = 0, 1, \cdots, n-3$ and $n-2$, respectively. This action repeats from $|a_1>$ to $|a_n>$. As the target state for $|b_1>$ is 1, (PI) and (IM) act on $|b_1>$. When γ_1 is the minimum even integer that is $(n/(n-1))^{(n-1)/2}$ or more, the total number that (PI) and (IM) act on $|b_1>$ is γ_1. Next, (OB) observes $|b_1>$. Therefore, only the orders that contain 1 piece of 0 remain. The number of data is $n(n-1)^{n-1}$. As the target state for $|b_2>$ is 1, (PI) and (IM) act on $|b_2>$. When γ_2 is the minimum even integer that is $((n-1)/(n-2))^{(n-2)/2}$ or more, the total number that (PI) and (IM) act on $|b_2>$ is γ_2. Next, (OB) observes $|b_2>$. Therefore, only the orders that contain 1 piece of 1 remain. The number of data is $n(n-1)(n-2)^{n-2}$. Similarly, these actions are repeated sequentially from $|b_3>$ to $|b_{n-1}>$. Only the orders that contain 1 piece of number from 0 to $n-1$, respectively, remain. The number of data is $n![=W_0]$.

Step 5: It is assumed that a quantum gate (C_1) changes $|c_1>$ and $|c_2>$ for $|c_1 + x_{1,a_1}y_{a_1,1}>$ and $|c_2 + a_1 n^{n-1}>$, respectively, from $|a_1>$. Similarly, (C_i) [$2 \leq i \leq n-1$. i is the integer.] changes $|c_1>$ and $|c_2>$ for $|c_1 + x_{i,a_i}y_{a_i,i}>$ and $|c_2 + a_i n^{n-i}>$, respectively, from $|a_i>$. This action is repeated sequentially from $|a_2>$ to $|a_{n-1}>$. (C_n) changes $|c_1>$ and $|c_2>$ for $|c_1 + x_{n,a_n}y_{a_n,n}>$ and $|c_2 + a_n n^0>$, respectively, from $|a_n>$. Therefore, $|c_1>$ and $|c_2>$ become $|x_{1,a_1}y_{a_1,1} + x_{2,a_2}y_{a_2,2} + \cdots + x_{n,a_n}y_{a_n,n}>$ and $|U>$, respectively.

Step 6: It is assumed that a quantum gate (D) changes $|d>$ for $|d + c_1>$ in $c_1 = n$, or it changes $|d>$ for $|d + n + c_2>$ in the others of c_1.

Step 7: It is assumed that a quantum gate (E_1) doesn't change $|e>$ in $d = n$ and $n + U(V=1) \leq d \leq n + U(V=(n!/4)-1)$, or it changes $|e>$ for $|e+1>$ in the others of d. As the target state for $|e>$ is 0, (PI) and (IM) act on $|e>$. The number of the data that is included in $d = n$ and $n + U(V=1) \leq d \leq n + U(V=(n!/4)-1)$ is $W_1 \approx n!/4$. When δ_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 $|e>$ is $\delta_1 \approx 2$. Next, (OB) observes $|e>$, and the data of W_1 remain. Similarly, (E_i) [$2 \leq i \leq g-1$. i is the integer.] doesn't change $|e>$ in $d = n$ and $n + U(V=1) \leq d \leq n + U(V=(n!/4^i)-1)$, or it changes $|e>$ for $|e+1>$ in the others of d. As the target state for $|e>$ is 0, (PI) and (IM) act on $|e>$. The number of the data that is included in $d = n$ and $n + U(V=1) \leq d \leq n + U(V=(n!/4^i)-1)$ is $W_i \approx n!/4^i$. When δ_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 $|e>$ is $\gamma_i \approx 2$. Next, (OB) observes $|e>$, and the data of W_i remain. These actions are repeated sequentially from 2 to $g-1$ at i. (E_g) doesn't change $|e>$ in $d = n$, or it changes $|e>$ for $|e+1>$ in the others of d. As the target state for $|e>$ is 0, (PI) and (IM) act on $|e>$. The number of the data that is included in $d=n$ is $W_g \approx 1$. When δ_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 $|e>$ is $\delta_g \approx 2$. Next, (OB) observes $|a_1>, |a_2>, \cdots, |a_n>, |b_1>, |b_2>, \cdots, |b_{n-1}>, |c_1>, |c_2>, |d>$ and $|e>$, and one of the data of W_g remains. Therefore, one example of orders that are $d=n$ is obtained.

4. Numerical Computation

It is assumed that there are $n=5$, the s-th person M_s $[1 \le s \le 5]$ in one group, the t-th person F_t $[1 \le t \le 5]$ in another group, $x_{1,1}=x_{1,3}=x_{1,4}=x_{1,5}=x_{2,1}=x_{2,3}=x_{2,5}=x_{3,1}=x_{3,2}=x_{3,4}=x_{4,1}=x_{4,5}=x_{5,2}=x_{5,3}=x_{5,4}=1$, (the others of $x_{s,t}$) $=0$, $y_{1,2}=y_{1,3}=y_{1,4}=y_{2,1}=y_{2,2}=y_{2,4}=y_{2,5}=y_{3,1}=y_{3,3}=y_{4,2}=y_{4,3}=y_{4,5}=y_{5,1}=y_{5,4}=1$, (the others of $y_{t,s}$) $=0$, $g=4[5!/1=120 \le 4^4=256]$, $U(V=1)=194$, $U(V=(5!/4)-1=29)=738$ [for examle, $V=29=1\cdot4!+0\cdot3!+2\cdot2!+1\cdot1!$, $U=738=1\cdot5^4+0\cdot5^3+4\cdot5^2+2\cdot5^1+3\cdot5^0$], $U(V=(5!/16)-1\approx7)=294$, and $U(V=(5!/64)-1\approx1)=194$.

First of all, $|a_1>, |a_2>, |a_3>, |a_4>, |a_5>, |b_1>, |b_2>, |b_3>, |b_4>, |c_1>, |c_2>, |d>$ and $|e>$ are prepared. When α is the minimum integer that is $log_2 n = log_2 5 \approx 2.3 \le 3 = \alpha$, each of $|a_f>$ that f is the integer from 1 to 5 is consisted of $\alpha=3$ qubits. States of $|a_1>, |a_2>, |a_3>, |a_4>, |a_5>, |b_1>, |b_2>, |b_3>, |b_4>, |c_1>, |c_2>, |d>$ and $|e>$ are $a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, c_1, c_2, d$ and e, respectively.

Step 1: Each qubit of $|a_1>, |a_2>, |a_3>, |a_4>, |a_5>, |b_1>, |b_2>, |b_3>, |b_4>, |c_1>, |c_2>, |d>$ and $|e>$ is set $|0>$.

Step 2: $\boxed{\text{H}}$ acts on each qubit of $|a_1>, |a_2>, |a_3>, |a_4>$ and $|a_5>$. It changes them for entangled states. The total states are $(2^\alpha)^n=(2^3)^5=8^5$.

Step 3: (A) doesn't change $|b_1>$ in $a_f<n=5$, or it changes $|b_1>$ for $|b_1+1>$ in the others of a_f. As the target state for $|b_1>$ is 0, (PI) and (IM) act on $|b_1>$. When β is the minimum even integer that is $(2^\alpha/n)^{1/2}=(8/5)^{1/2}\approx1.3\le2=\beta$, the total number that (PI) and (IM) act on $|b_1>$ is $\beta\approx2$. Next, (OB) observes $|b_1>$. These actions are repeated sequentially from $|a_1>$ to $|a_5>$. Therefore, each state of $|a_f>$ is 0, 1, 2, 3 and 4, and the total states become $n^n=5^5$.

Step 4: (B) changes $|b_1>, |b_2>, |b_3>$ and $|b_4>$ for $|b_1+1>, |b_2+1>, |b_3+1>$ and $|b_4+1>$ in $a_f=0,1,2$ and 3, respectively. This action is repeated from $|a_1>$ to $|a_5>$. As the target state for $|b_1>$ is 1, (PI) and (IM) act on $|b_1>$. When γ_1 is the minimum even integer that is $(n/(n-1))^{(n-1)/2}=(5/4)^2\approx1.6\le2=\gamma_1$, the total number that (PI) and (IM) act on $|b_1>$ is γ_1. Next, (OB) observes $|b_1>$. Therefore, only the orders that contain 1 piece of 0 remain. The number of data is $n(n-1)^{n-1}=5\cdot4^4$. As the target state for $|b_2>$ is 1, (PI) and (IM) act on $|b_2>$. When γ_2 is the minimum even integer that is $((n-1)/(n-2))^{(n-2)/2} = (4/3)^{1.5} \approx 1.5 \leq 2 = \gamma_2$, the total number that (PI) and (IM) act on $|b_2>$ is γ_2. Next, (OB) observes $|b_2>$. Therefore, only the orders that contain 1 piece of 1 remain. The number of data is $n(n-1)(n-2)^{n-2} = 5 \cdot 4 \cdot 3^3$. Similarly, these actions are repeated sequentially from $|b_3>$ to $|b_4>$. Only the orders that contain 1 piece of number from 0 to 4, respectively, remain. The number of data is $n! = 5![= W_0]$.

Step 5: (C_1) changes $|c_1>$ and $|c_2>$ for $|c_1 + x_{1,a_1} y_{a_1,1}>$ and $|c_2 + a_1 5^4>$, respectively, from $|a_1>$. Similarly, (C_i) [$2 \leq i \leq 4$. i is the integer.] changes $|c_1>$ and $|c_2>$ for $|c_1 + x_{i,a_i} y_{a_i,i}>$ and $|c_2 + a_i 5^{5-i}>$, respectively, from $|a_i>$. This action is repeated sequentially from $|a_2>$ to $|a_4>$. (C_5) changes $|c_1>$ and $|c_2>$ for $|c_1 + x_{5,a_5} y_{a_5,5}>$ and $|c_2 + a_5 5^0>$, respectively, from $|a_5>$. Therefore, $|c_1>$ and $|c_2>$ become $|x_{1,a_1} y_{a_1,1} + x_{2,a_2} y_{a_2,2} + \cdots + x_{5,a_5} y_{a_5,5}>$ and $|U>$, respectively.

Step 6: (D) changes $|d>$ for $|d + c_1>$ in $c_1 = n = 5$, or it changes $|d>$ for $|d + 5 + c_2>$ in the others of c_1.

Step 7: (E_1) doesn't change $|e>$ in $d = n = 5$ and $n + U(V = 1) = 5 + 194 = 199 \leq d \leq n + U(V = (5!/4) - 1 = 29) = 5 + 738 = 743$, or it changes $|e>$ for $|e + 1>$ in the others of d. As the target state for $|e>$ is 0, (PI) and (IM) act on $|e>$. The number of the data that is included in $d = 5$ and $199 \leq d \leq 743$ is $W_1 \approx 5!/4 = 30$. When δ_1 is the minimum even integer that is $(W_0/W_1)^{1/2} \approx 4^{1/2} = 2 \leq 2 = \delta_1$, the total number that (PI) and (IM) act on $|e>$ is $\delta_1 \approx 2$. Next, (OB) observes $|e>$, and the data of W_1 remain.

Similarly, (E_i) [$2 \leq i \leq g - 1 = 3$. i is the integer.] doesn't change $|e>$ in $d = 5$ and $199 \leq d \leq 5 + U(V = (5!/4^i) - 1)$, or it changes $|e>$ for $|e+1>$ in the others of d. As the target state for $|e>$ is 0, (PI) and (IM) act on $|e>$. The number of the data that is included in $d = 5$ and $199 \leq d \leq 5 + U(V = (5!/4^i) - 1)$ is $W_i \approx 5!/4^i$. When δ_i is the minimum even integer that is $(W_{i-1}/W_i)^{1/2} \approx 4^{1/2} = 2 \leq 2 = \delta_i$, the total number that (PI) and (IM) act on $|e>$ is $\delta_i \approx 2$. Next, (OB) observes $|e>$, and the data of W_i remain. These actions are repeated sequentially from 2 to 3 at i. (E_4) doesn't change $|e>$ in $d = 5$, or it changes $|e>$ for $|e + 1>$ in the others of d. As the target state for $|e>$ is 0, (PI) and (IM) act on $|e>$. The number of the data that is included in $d = 5$ is $W_4 \approx 1$. When δ_4 is the minimum even integer that is $(W_3/W_4)^{1/2} \approx 4^{1/2} = 2 \leq 2 = \delta_4$, the total number that (PI) and (IM) act on $|e>$ is $\delta_4 \approx 2$. Next, (OB) observes $|a_1>$, $|a_2>, |a_3>, |a_4>, |a_5>, |b_1>, |b_2>, |b_3>, |b_4>, |c_1>, |c_2>, |d>$ and $|e>$, and one of the data of W_4 remains. Therefore, $a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, c_1, c_2, d$ and e are $2, 0, 3, 4, 1, 1, 1, 1, 1, 5, U(V = 52) = 1346, 5$ and 0, respectively. As a result, a combination of a perfect matching that is $(M_1, F_3), (M_2, F_1), (M_3, F_4), (M_4, F_5)$ and (M_5, F_2) is obtained.

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 $\boxed{\text{H}}$, n at (A), $\beta n \approx 2n$ at (PI) and (IM), n at (OB), n at (B), $\sum_{i=1}^{n-1} \gamma_i \approx 2(n-1)$ at (PI) and (IM), $n-1$ at (OB), n at (C_i) [$1 \leq i \leq n$. i is the integer.], 2 at (D), g at (E_i) [$1 \leq i \leq g$.], $\sum_{i=1}^{g} \delta_i \approx 2g$ at (PI) and (IM), and g at (OB). Therefore, S becomes $(\alpha+9)n-1+4g$. In the example of the section 4, S is 75. The computational complexity of the classical computation [$= Z$] is $n! = 5! = 120$. After all, S/Z becomes about $2/3$. When n is large enough, S becomes about $3(log_2 n)n$, where α is about $log_2 n$, g is about $(1/2)log_2 n!$, and $n!$ is about $n^n e^{-n}(2\pi n)^{1/2}$ [Stirling's formula], and S/Z is about $3(log_2 n)n/n!$. For example, as for $n = 50$, S/Z is about $1/10^{62}$. Therefore, a polynomial time process becomes possible.

References

[1] Kungl. Vetenskapsakademien (The Royal Swedish Academy of Sciences), The Nobel Prize in Physics 2012, [Online], 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), Nihonhyoronsha, 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 vertex coloring problem by central limit theorem, *Glob. J. Pure Appl. Math.*, 7:401–405, 2011.

[9] Weisstein E.W., Perfect matching, [Online], Available: http: //mathworld. wolfram.com/PerfectMatching.html, 2011.