Journal of Science and Technology ***49,*** *Number 5 (2011) 25-34*

QUANTUM ALGORITHM FOR SOLVING THE TRAVELING SALESMAN PROBLEM

Huynh Van Duc[1,2], Bui Doan Khanh[3], and Do Ngoc Diep[4]

[1] *University of Economics HCMC, Viet Nam*

[2]*University of Science HCMC, Vietnam National University - HCMC, Viet Nam*

[3]*University of Paris VI, Paris, France*

[4]*Institute of Mathematics, Vietnam Academy of Science and Technology, Viet Nam*

Received September 30, 2011

ABSTRACT

We propose a new quantum algorithm for the Traveling Salesman Problem (TSP). The algorithm is an extension of our recently introduced pattern search algorithm, which based on Hough transformation and Grover algorithm. Based on Lehmer code we directly build the circuit of acted elements of the symmetric group S_n, and have a chance to add some heuristic informations. The result is a way of re-indexing elements of S_n, so that a permutation that is a solution could be found at small indexes. The pattern search algorithm is then applied on a searching space that its size was reduced significantly.

Keywords. Black-box, query complexity, pattern searching, TSP, symmetric group, Lehmer code.

1. INTRODUCTION

Let us consider the following problem [6], [7]. Denote $F = \{f : X \to Y\}$, where $X = \{0,1\}^n, Y = \{0,1\}^m$ and m, n two positive integers. Assume that G is a group acting on X, then G generates an action group $\tilde{G}$ on F, for each $g \in G$ there is a $\tilde{g} \in \tilde{G}$ defined by [9]

$$f_{\tilde{g}}(x) = f(x_{g^{-1}}).$$

Problem 1. Given $f, h \in F$, find $g \in G$ such that $f(x) = h_{\tilde{g}}(x), \forall x, x_{g^{-1}} \in B$, where $B = \{x \mid h(x) > 0\}$.

In the black-box model, the inputs to the problem are provided by black-boxes have the form:

$$|x\rangle|y\rangle \mapsto U_f|x\rangle|y\rangle = |x\rangle|y + f(x)\rangle, \quad (1)$$

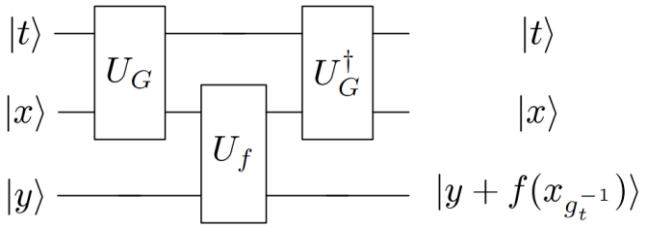
where $f \in F$.

Let us remind that the *query complexity* [11] of a black-box algorithm is the number of queries to black-boxes used by the algorithmand in general, the query complexity of a problem is the number of queries needed to solve the problem.

According to (1), it is well-known the black-box group $\mathbb{H} = \{U_f \mid f \in F\}$ a subgroup of group $U(2^{n+m})$. Group G acts as $\bar{G}$ on $\mathbb{H}$, for each $g \in G$ there is a $\bar{g} \in \bar{G}$ defined by

$$(U_f)_{\bar{g}}|x\rangle|y\rangle = |x\rangle|y + f(x_{g^{-1}})\rangle.$$

Assume that $G = \{g_t\}_{t \in T}$ is a group depends on parameters. The above transformation can be constructed as follows.



Where

$$(U_G)|t\rangle|x\rangle = |t\rangle|x_{g_t^{-1}}\rangle. \quad (2)$$

Denote the tranformation by G_f, we have

$$(G_f)|t\rangle|x\rangle|y\rangle = |t\rangle|x\rangle|y + f(x_{g_t^{-1}})\rangle.$$

Using the ideas of the *voting technique based on Hough transformation* [3, 4, 5, 12, 16] and the *Grover's algorithm* [8, 10, 11], we constructed a quantum algorithm for solving problem (1) with the query complexity $O\left(|B|\sqrt{|G|/k}\right)$, where k is the number of the solutions, see [7]. In [6], we applied the algorithm for searching Hamiltonian cycles. However, the complexity is too large when G is the symmetric group.

In this paper we show how to build the transformation (2) in the case of G is the symmetric group of X, by using the Lehmer code [15], then apply it to solve the TSP by effectively reducing the size of searching space. The main results is exposed in Section 3.

The paper is organized as follows. First, in Section 2, we briefly review the main quantum algorithm produced in [7]. Then, in Section 3, we show the way of building (2) and apply to solve the TSP. The details of the quantum algorithms and Hough transformation can be found in the documents cited [1 - 5, 11, 13, 14, 16].

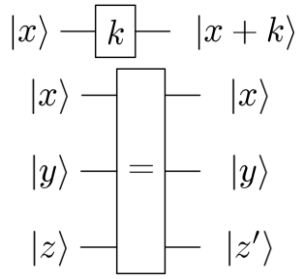
2. PRELIMINARIES

The main idea of the algorithms built in [6], [7] is to build the black-box U_d to evaluate the decision function d is defined by

$$\left(d(t)=1\right) \Leftrightarrow \left(h_{\widetilde{g_t}}(x) = f(x), \forall x, x_{g_t^{-1}} \in B\right). \tag{3}$$

Based on Hough transformation, g_t is voted by the voting function $v(t,x)$ and then the total number of votes $s(t)$ used to build U_d (the Theorem (1) below).

In process of building U_v, we used the input black-boxes (U_h, U_f) and following unitary tranformations.



where $z' = \begin{cases} z+1 \text{ if } x = y \\ z \text{ otherwise} \end{cases}$.

2.1. The voting black-box

Let $C \subset X$, denote by χ_C the characteristic function of C.

Lemma 1. *[6] Suppose $C \subset X$ and $g_t \in G,$, let $C_t = \{x_{g_t} \mid x \in X\}$, then $\chi_{C_t}(x) = \chi_C(x_{g_t^{-1}})$*

Back to the problem (1), in the case $m=1, B=\{x \mid h(x)=1\}$, let $A=\{x \mid f(x)=1\}$. Based on Hough transformation, the function $s_{B,A}$ determines the total number of votes of B for g_t corresponding to A is defined by [7]

$$s_{B,A}(t) = \sum_{x \in B} \left(\chi_A\right)_{\widetilde{g_t}}(x) = \sum_{x \in B} \chi_{A_t}(x).$$

In the general case, $m>0$, let $B_y = h^{-1}(y), A_y = f^{-1}(y), \forall y>0$, then $\{B_y\}_{y>0}$ is an finite partition of B. The function $s_{h,f}$ determines the total number of votes of h for g_t corresponding to f is defined as follows [7]

$$s_{h,f}(t) = \sum_{y>0} s_{B_y, A_y}(t).$$

The following result is used to build the black-box U_d to evaluate the function d for if t is a solution. The black-box U_d is then used for building the transform G for Grover algorithm.

Theorem 1. [7]

$$\left(h_{\tilde{g}_t}(x) = f(x), \forall x, x_{g_t^{-1}} \in B\right) \Leftrightarrow \left(s_{h,f}(t) = |B|\right). \tag{4}$$

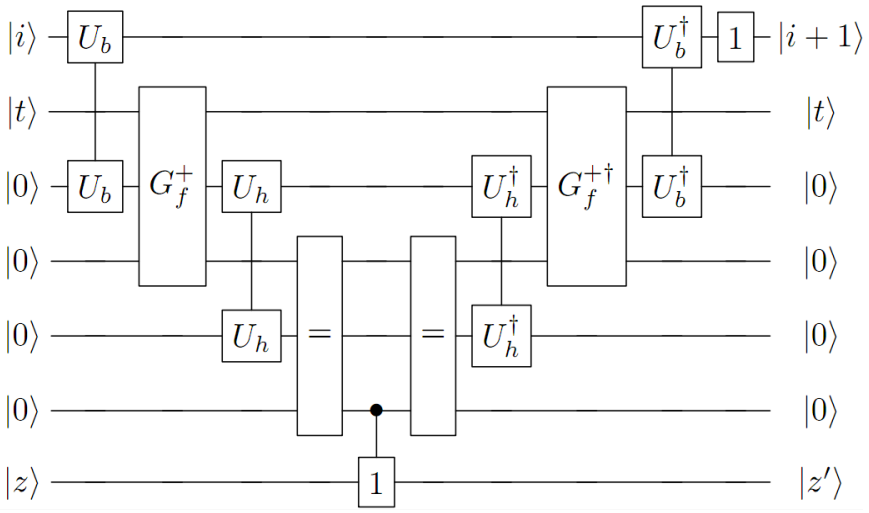
Notice

$$\left(h_{\tilde{g}_t}(x) = f(x), \forall x, x_{g_t^{-1}} \in B\right) \Leftrightarrow \left(h(x) = f_{\tilde{g}_t^{-1}}(x), \forall x \in B\right).$$

Denote by

$$(G_f^+)\ |t\rangle|x\rangle|y\rangle = |t\rangle|x\rangle|y + f(x_{g_t})\rangle. \tag{5}$$

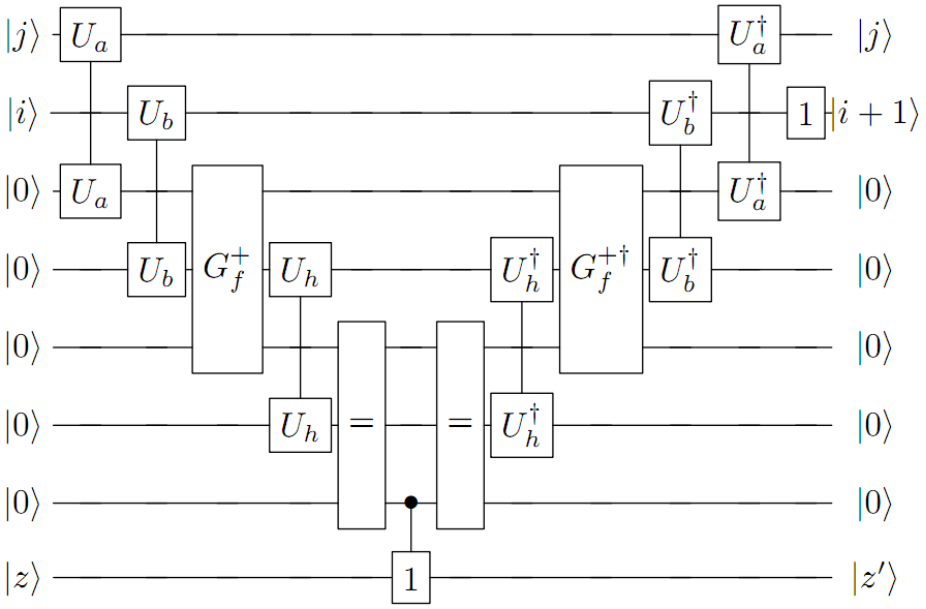
Let b be an index function of B, applying $|B|$ times the circuit below, called U_v we get U_s.



where $z' = \begin{cases} z+1 & \text{if } f_{\tilde{g}_t}(b(i)) = h(b(i)) \\ z & \text{otherwise} \end{cases}$.

2.2. The voting black-box with heuristic

According to Grover algorithm, the query complexity for searching a solution is $O(\sqrt{|G|/k})$, where k is the number of solutions. By using a proper heuristic we narrow down the searching space to a subset $H \subset G$ [7]. Denote by a an index function of H, the circuit U_v is adjusted as follows.



where $z' = \begin{cases} z+1 & \text{if } f_{\tilde{g}_{a(j)}}(b(i)) = h(b(i)) \\ z & \text{otherwise} \end{cases}$.

2.3. The problem of searching Hamiltonian cycle

Let (V,E) be an oriented graph, where $V=\{0,1,\ldots,n-1\}$ is the set of vertices and $E \subseteq X = V \times V$ the set of edges. Denote by S_n be the symmetric group of V, then S_n induces a group G acting on X defined by

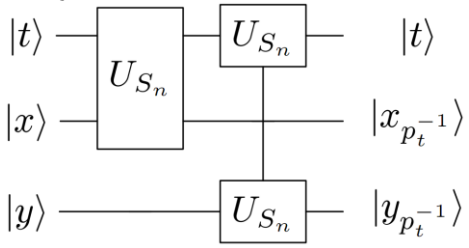
$$p \in S_n \mapsto g \in G : (a,b) \mapsto (p(a), p(b))$$

A Hamiltonian cycle is a subset $\{(i_0,i_1),(i_1,i_2),\ldots,(i_{n-1},i_0)\}$ defined by the permutation

$$\sigma = \begin{pmatrix} 0 & 1 & \ldots & n-1 \\ i_0 & i_1 & \ldots & i_{n-1} \end{pmatrix}$$

and vice-versa [6].

The transform (2) is precisely built as follows



Denote by $C=\{(0,1),(1,2),\ldots,(n-2,n-1),(n-1,0)\}$, called the *canonical Hamiltonian cycle*, we solve the problem (1) with $h=\chi_C$, $f=\chi_E$ and determine the Hamiltonian cycle for each solution t found.

3. THE NEW ALGORITHM FOR TSP

The TSP is the problem for searching the shortest Hamiltonian cycle of a graph. In order to solve the problem we consider G is the symmetric group acting on the set of vertices of the graph. In this section we produce a type of numbering permutations based on Lehmer code. Depending on the specific problem we choose a proper way of numbering allows to search for a solution in a set of small indexes.

3.1. Numbering permutations

Let $G = S_n$ be the symmetric group of $X = \{0,1,...,n-1\}$ and $\pi \in G$. Denote by $L(\pi) = (l_i)_{i=0,...,n-2}$ the Lehmer code of π, then

$$l_i = |\{j > i \,|\, \pi(j) < \pi(i)\}|.$$

It is not difficult to see how π can be reconstructed from the code $L(\pi)$ [15]:

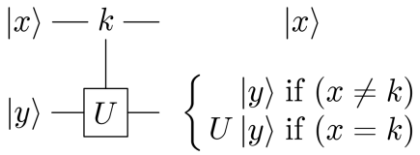
$$\pi(k) = N_k[l_k]; N_0 = X, N_k = X - \{\pi(0),...,\pi(k-1)\}$$

3.2. An implementation of the symmetric group

Using the cyclic permutation transformation

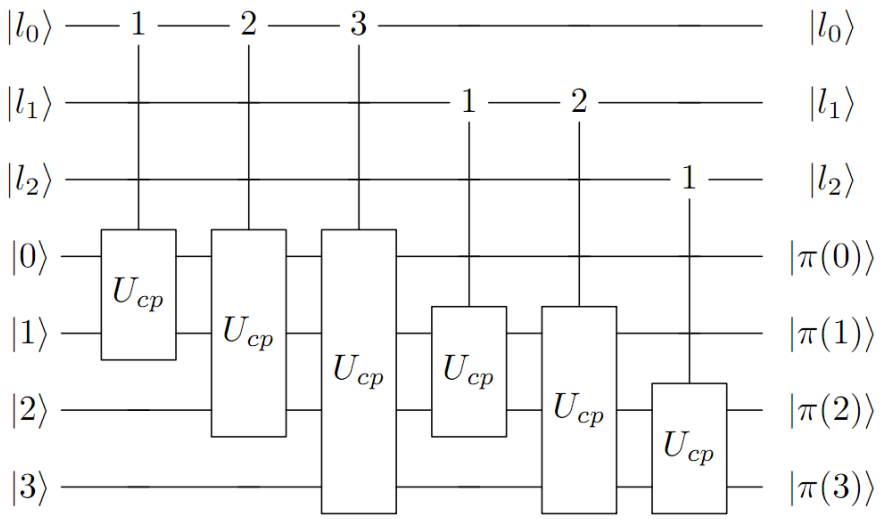
$$U_{cp} : |x_0\rangle|x_1\rangle...|x_{k-1}\rangle|x_k\rangle \mapsto |x_1\rangle|x_2\rangle...|x_k\rangle|x_0\rangle,$$

and the extended control gates have form



we easily construct the decode circuit for $L(\pi)$. The following example illustrates the case $n = 4$.

Example 1. The circuit



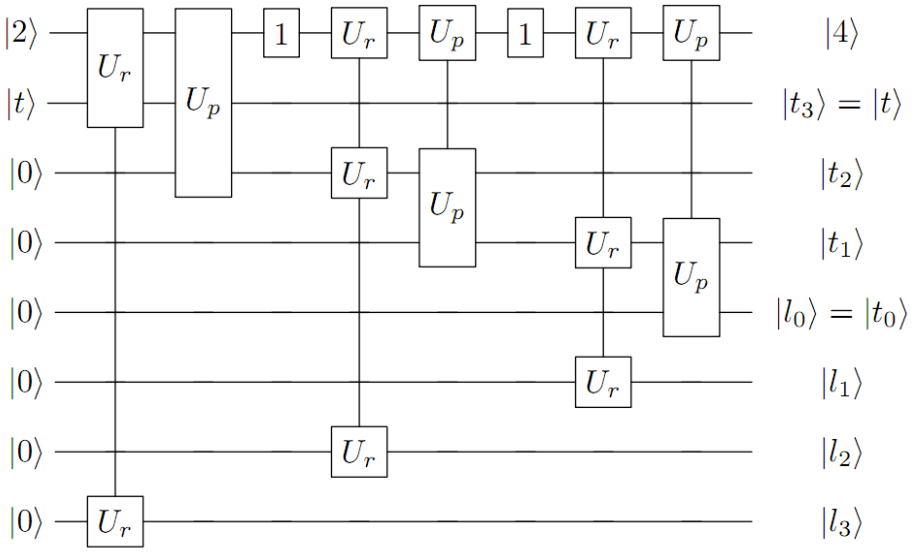
decodes $l=(0,2,1)$ to return $\pi=(0,3,2,1)$.

We number each permutation π by $t(\pi)=\sum_{i=0}^{n-2} l_i \times (n-i-1)!$. It is easy to recall $L(\pi)$ by using the integer division. In order to build the circuit recall $L(\pi)$ we use the black-boxes to evaluate integer division

$$U_p \ : \ |m\rangle|n\rangle|x\rangle \mapsto \ |m\rangle|n\rangle|x+n/m\rangle \ ,$$
$$U_r \ : \ |m\rangle|n\rangle|x\rangle \mapsto \ |m\rangle|n\rangle|x+n\%m\rangle \ .$$

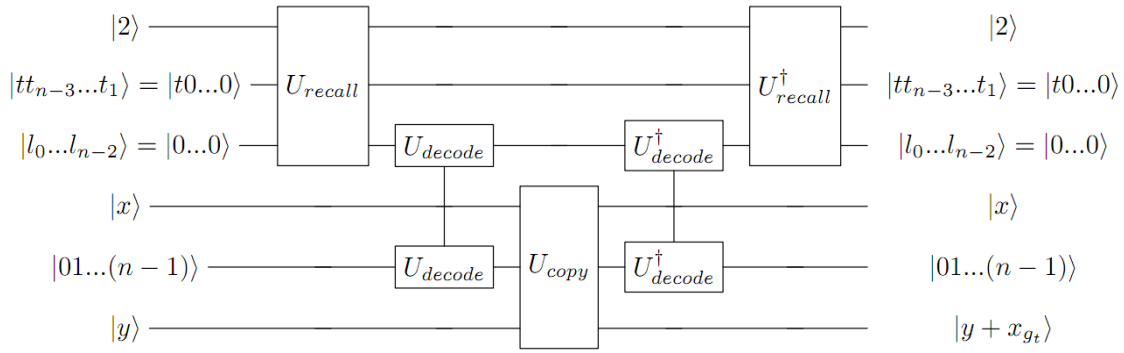
The following example illustrates the case *n* = 5.

Example 2. The circuit

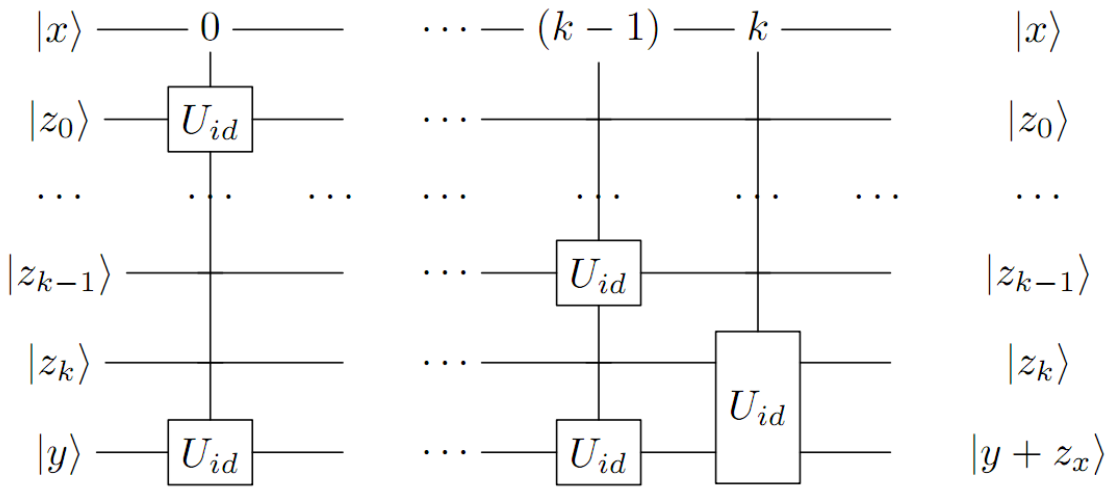


recalls $t=94=0+2\times 2!+3\times 3!+3\times 4!$ to return $L=(3,3,2,0)$ is Lehmer code of permutation $\pi=(3,4,2,0,1)$.

Denote by U_{decode} the decoded circuit and by U_{recall} the recalled circuit. The circuit for (5) is built as follows.



where U_{copy} is



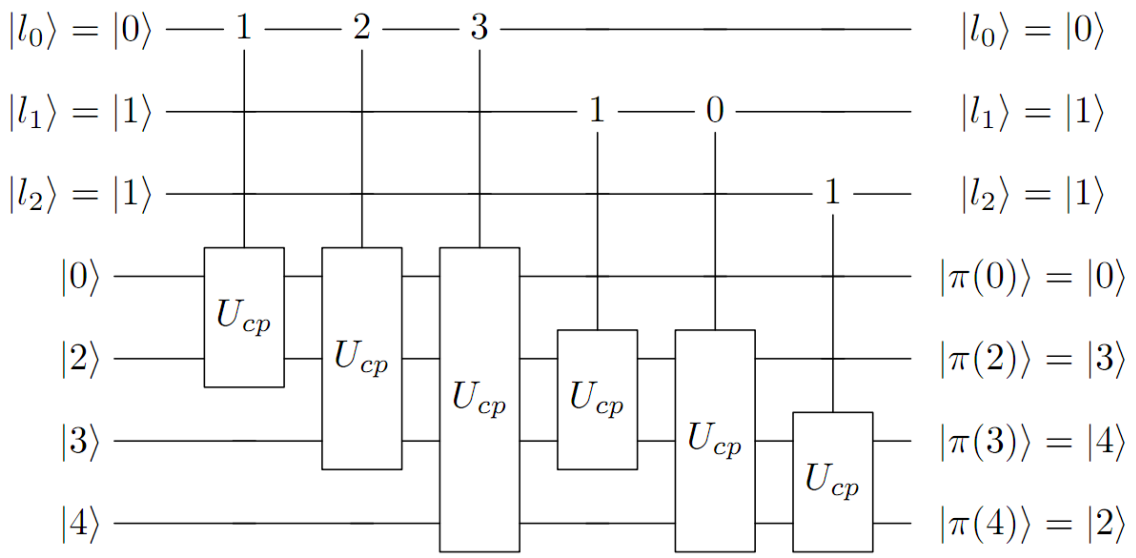
3.3. Renumber S_n for the TSP

Adjusting the control values in the decode transformation U_{decode} we renumber the symmetric group of X so that some solution g_t can be found at small indexes. In following example we use the greedy heuristic to adjust the control values.

Example 3. Let G be an oriented graph defined by the edge set E

E	0	1	2	3	4
0	0	0	0	3	2
1	5	0	0	0	0
2	2	6	0	5	0
3	0	0	0	0	4
4	0	4	7	0	0

Fix a vertex $v \in V$ and consider group S_4 acts on $V - \{v\}$. In the case $v = 4$, we substitute the set of control values $\{1,2,3;1,2;1\}$ by $\{0,1,3;1,2;0\}$, then the first solution is at $t = 1$ and the respective Hamiltonian cycle is $\{4,1,0,2,3,4\}$ with distance $d = 22$. Also with $v = 1$ and select new set of control values is $\{1,2,3;1,0;1\}$, we get the first solution at $t = 3$ and the respective Hamiltonian cycle is $\{1,0,3,4,2,1\}$ with the distance $d = 25$. The circuit below is for the case $v = 1$.



4. CONCLUSION

In this paper we continue to study the problem 1 started in [6, 7]. Based on Lehmer code we build a circuit for (5), where G is the symmetric group. Adjusting the set of control values of the circuit, we renumber elements of S_n. In order to solve the TSP, we select a proper set of control values depend on an individual problem. By the way we apply the pattern seach algorithm for a subset $H \subset G$.

REFERENCES

1. Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John Smolin, Harald Weinfurter - Elementary gates for quantum computation, arXiv:quant-ph/9503016 v1 23 Mar 95, 1995.
2. Artur Ekert, P.Hayden, H.Inamori - Basis concepts in quantum computation, Centre for Quantum Computation, University of Oxford, 16-Jan-2000, 2000.
3. Alberto S. Aguado, Eugenia Montiel and Mark S. Nixon - Invariant Characterization of the Hough Transform for Pose Estimation of Arbitrary Shapes, Pattern Recognition, **35** (5) (2002) 1083-1097.
4. Clark F. Olson - Constrained Hough Transforms for Curve Detection, Computer Vision and Image Understanding **73** (3) (1999) 329-345.
5. D. H. Ballard - Generalizating the Hough Transform to Detect Arbitrary Shapes, Pattern Recognition **13** (2) (1981) 111-122.
6. Duc V. Huynh, Khanh D. Bui, Diep N. Do - Pattern Search Quantum Algorithms, IEEE International Conference on Research, Innovation and Vision for the Future, HCMC, Vietnam, Addendum Contributions, 2008, pp. 36-40.
7. Duc V. Huynh, Khanh D. Bui, Diep N. Do - A Quantum Algorithm for Searching Pat-

terns, Journal of Science and Technology **46** (5A) (2009) 67-78.

8. Gilles Brassard, Peter Hyer, and Alain Tapp - Quantum Counting, arXiv:quant-ph/9805082v1 27 May 1998, 1998.
9. J. F. Cornwell - Group Theorem in Physics: An Introduction, Elsevire (Singapore) Pte Ltd, ISBN 981-259-825-1, 2006.
10. Michel Boyer, Gilles Brassard, Peter Hye, Alain Tapp - Tight bounds on quantum searching, PhysComp96, arXiv:quant-ph/9605034v1, 23 May 1996, 1996."
11. Phillip Kaye, Raymond Laflamme, Michele Mosca - An Introduction to Quantum, Computing, Oxford University Press, 2007.
12. Philipp Robbel - Pose estimation using the Hough Transform,2007.
13. Peter W. Shor - Introduction to Quantum Algorithms, arXiv:quant-ph/0005003 v2 6 Jul 2001, 2001.
14. Samuel J. Lomonaco - Shors Quantum Factoring Algorithm, A Lecture Version 1.1, arXiv:quant-ph/0010034 v1 9 Oct 2000, 2000.
15. tefan Peko - Differential Evolution for Small TSPs with Constraints, 4th International Scientific Conference, Challenges in Transport and Communication, Pardubice, September 14th -15th, 2006.
16. Tetsuo Asano - Algorithmic Evaluation of Line Detection Problem, Interdisciplinary Information Sciences **8** (2) (2002) 137-145.

Corresponding author:

Huynh Van Duc

University of Economics HCMC, Viet Nam

University of Science HCMC, Vietnam National University - HCMC, Viet Nam

Email: *hvduc0703@gmail.com*