CHIN.PHYS.LETT. Vol. 25, No. 8 (2008) 2774

Research on Quantum Searching Algorithms Based on Phase Shifts *

ZHONG Pu-Cha(钟普查)**, BAO Wan-Su(鲍皖苏)

Institute of Electronic Technology, The PLA Information Engineering University, Zhengzhou 450004

(Received 22 April 2008)

One iterative in Grover's original quantum search algorithm consists of two Hadamard–Walsh transformations, a selective amplitude inversion and a diffusion amplitude inversion. We concentrate on the relation among the probability of success of the algorithm, the phase shifts, the number of target items and the number of iterations via replacing the two amplitude inversions by phase shifts of an arbitrary $\phi = \varphi (0 \leq \phi, \varphi \leq 2\pi)$. Then, according to the relation we find out the optimal phase shifts when the number of iterations is given. We present a new quantum search algorithm based on the optimal phase shifts of 1.018 after $0.5\pi/\sqrt{M/N}$ iterations. The new algorithm can obtain either a single target item or multiple target items in the search space with the probability of success at least 93.43%.

PACS: 03.67.Lx, 03.67.−a, 89.20.Ff

A quantum computer can perform computation in a parallel way, but it outputs an answer with a certain probability. Recently many quantum algorithms have been presented to improve the probability of achieving the answer.

In 1996, Grover[1] presented a quantum search algorithm, which reduces the computational complexity of the classical search algorithms $O(N/M)$ to $O(\sqrt{N/M})$, where M is the number of target items, and $N = 2^n$ is the number of items in the search space. Subsequently, a lot of pursuers analysed some aspects of Grover's original algorithm, such as initial state,[2] the Walsh–Hadamard transition,[3] and phase shifts.[4−6] In 1999, Zalka[7] proved that Grover's algorithm is the most efficient algorithm when there was only one target item in the search space. In 2000, Nielson and Chuang[8] indicated that the probability of success of Grover's algorithm is too low when the target items exceeded half of the search space. To overcome this disadvantage, Younes[9] proposed a quantum algorithm with probability of success not less than 87.88% for any $M(1 \leq M \leq N)$ using the partial diffusion operator. In 2005, Grover[10] presented a fixed point quantum algorithm with phase shifts of $\pi/3$, which could obtain a target item after a single iteration with probability over 90% when the number of matches is more than one third of the search space. In 2007, Younes[11] designed a fixed phase quantum algorithm, of which the probability of success is at least 99.58% after $k = 1.91684\pi/\sqrt{M/N}$ iterations.

In this Letter, we research the relation among the probability of success, the phase shifts, the number of target items and the number of iterations by replacing the two amplitude inversions with arbitrary phase shifts in quantum search algorithm. We give the optimal phase shifts according to the relation for some special number of iterations. We present a new quantum search algorithm with the phase shifts of 1.018, of which the probability of success is at least 93.43% for all the $M(M \in [1, N])$.

Grover proposed a quantum search algorithm that could search faster than any other known classical algorithms. One iterative in Grover's original quantum search algorithm is expressed as

$$G = G(H, f, \pi, \pi) = -HS_{0,\pi}H^{\dagger}S_{f,\pi}, \tag{1}$$

where

$$S_{0,\pi} = I - (1 - e^{i\pi})|0\rangle\langle 0| = I - 2|0\rangle\langle 0|, \tag{2}$$

which is called the selective amplitude inversion, and

$$S_{f,\pi} = I - (1 - e^{i\pi})|t\rangle\langle t| = I - 2|t\rangle\langle t|, \tag{3}$$

which is called the diffusion amplitude inversion, and $|0\rangle$ denotes the n qubits with zero, $|t\rangle$ is the target item, $i = \sqrt{-1}$, H is the Hadamard–Walsh transformation, $I$is the identity operator.

Brassard[5] generalized Grover's original algorithm, and obtained the Grover operator of an arbitrary phase shifts G', which is expressed as

$$G' = G'(H, f, \phi, \varphi) = -HS_{0,\phi}H^{\dagger}S_{f,\varphi}, \tag{4}$$

where ϕ and φ are the arbitrary phases, and

$$\begin{aligned} S_{0,\phi} &= I - (1 - e^{i\phi})|0\rangle\langle 0|, \\ S_{f,\varphi} &= I - (1 - e^{i\varphi})|t\rangle\langle t|. \end{aligned} \tag{5}$$

From the above description, we can obtain that the phase-π Grover operator is a special case of G'.

The operation of G' can be seen as a circumgyration of the initial vector $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$ in a

*Supported by the National Natural Science Foundation of China under Grant No 10501053.

**Email: zhongpucha@163.com

© 2008 Chinese Physical Society and IOP Publishing Ltd

two-dimensional space. The orthonormal basis is formed by the sum of target items $|\alpha\rangle$ and the sum of non-target items $|\beta\rangle$, where

$$|\alpha\rangle = \frac{1}{\sqrt{M}}\sum_x{}''|x\rangle, \quad |\beta\rangle = \frac{1}{\sqrt{N-M}}\sum_x{}'|x\rangle, \quad (6)$$

and $\sum_x{}''$ denotes a sum over i which represents target items in the search space, and $\sum_x{}'$ denotes a sum over i which represents non-target items in the search space.

Every pure state $|u\rangle$ involved in the quantum search space has a unique decomposition $|u\rangle = a|\alpha\rangle + b|\beta\rangle$, where $|a|^2+|b|^2 = 1$, and all the state vectors can be written in this basis as $|u\rangle = (a, b)^T$. Then the initial state of searching is given by $|\psi\rangle = (\sin\theta, \cos\theta)^T$, where $\sin^2\theta = M/N$. We set the phases $\phi = \varphi$ according to the phase matching proposed by Long.[12] The operator G' can be expressed as matrices in the linear space, i.e.

$$G' = \begin{bmatrix} \mathcal{A}_1 & \mathcal{A}_2 \\ \mathcal{B}_1 & \mathcal{B}_2 \end{bmatrix}, \quad (7)$$

$$\begin{aligned} \mathcal{A}_1 &= -\exp(i\phi)[\sin^2\theta\exp(i\phi) + \cos^2\theta], \\ \mathcal{A}_2 &= \sin\theta\cos\theta[1-\exp(i\phi)], \\ \mathcal{B}_1 &= \sin\theta\cos\theta\exp(i\phi)[1-\exp(i\phi)], \\ \mathcal{B}_2 &= -[\cos^2\theta\exp(i\phi) + \sin^2\theta]. \end{aligned}$$

Then we can obtain that the characteristic equation of the matrix

$$\lambda^2 + [\sin^2\theta(1-\exp(i\phi))^2 + 2\exp(i\phi)]\lambda + \exp(2i\phi) = 0. \quad (8)$$

Let $\cos(\delta) = 2\sin^2\theta\sin^2(\phi/2) - 1$, we can obtain the eigenvalues

$$\lambda_\pm = \exp(i\phi)\exp(\pm i\delta), \quad (9)$$

and the eigenvectors of G' as follows:

$$|\psi^+\rangle = \left(\frac{\sin^2\theta\sin\phi - \sin\delta}{(\sin(2\theta)\sin(\phi/2)\exp(i\phi/2))}, 1\right)^T, \quad (10)$$

$$|\psi^-\rangle = \left(\frac{\sin^2\theta\sin\phi + \sin\delta}{(\sin(2\theta)\sin(\phi/2)\exp(i\phi/2))}, 1\right)^T, \quad (11)$$

where $G'|\psi^\pm\rangle = \lambda_\pm|\psi^\pm\rangle$. Using the eigenvalues the amplitude of the quantum state after k iterations of $G'2$ will be obtained easily.

Assuming that the initial state is $|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$, phase shifts is equal, after applying k iterations of G' on the initial state, we obtain

$$|\psi^{(k)}\rangle = G'^k(\sin\theta, \cos\theta)^T = (a_k, b_k)^T. \quad (12)$$

Since the initial state can be expressed by the eigenvectors, i.e.

$$|\psi\rangle = v_1'|\psi^+\rangle + v_2'|\psi^-\rangle, \quad (13)$$

then we have

$$\begin{aligned} |\psi^{(k)}\rangle &= G'^k|\psi\rangle = G'^k(v_1'|\psi^+\rangle + v_2'|\psi^-\rangle) \\ &= (\lambda_+)^k v_1'|\psi^+\rangle + (\lambda_-)^k v_2'|\psi^-\rangle = (a_k, b_k)^T. \end{aligned} \quad (14)$$

Thus we obtain

$$a_k = (\lambda_+)^k v_1 + (\lambda_-)^k v_2, \quad (15)$$

where

$$v_1 = v_1'\frac{\sin^2\theta\sin\phi - \sin\delta}{\sin(2\theta)\sin(\phi/2)\exp(i\phi/2)}, \quad (16)$$

$$v_2 = v_2'\frac{\sin^2\theta\sin\phi + \sin\delta}{\sin(2\theta)\sin(\phi/2)\exp(i\phi/2)}. \quad (17)$$

From $|\psi^{(1)}\rangle = G'^1(\sin\theta, \cos\theta)^T = (a_1, b_1)^T$, it is easy to obtain

$$a_1 = \sin\theta\big(2\cos\delta\exp(i\phi) + 1\big). \quad (18)$$

If we also have $|\psi\rangle = (\sin\theta, \cos\theta)^T = (a_0, b_0)^T$, then we obtain

$$a_0 = \sin\theta. \quad (19)$$

By using Eqs. (15), (18) and (19), we have

$$\begin{aligned} v_1 &= \frac{\sin\theta(2\cos\delta\exp(i\phi) + 1 - \lambda_-)}{\lambda_+ - \lambda_-}, \\ v_2 &= \frac{\sin\theta(\lambda_+ - 2\cos\delta\exp(i\phi) - 1)}{\lambda_+ - \lambda_-}. \end{aligned} \quad (20)$$

Hence

$$\begin{aligned} a_k = \frac{\sin\theta}{\sin\delta}\big(&\exp(i\phi k)\sin((k+1)\delta) \\ &+ \exp(i\phi(k-1))\sin(k\delta)\big). \end{aligned} \quad (21)$$

Similarly, we can obtain b_k in the form

$$b_k = \frac{\sin\theta}{\sin\delta}\exp\big(i\phi(k-1)\big)\big(\sin((k+1)\delta) + \sin(k\delta)\big). \quad (22)$$

Measuring the quantum state, we can obtain the target item with the probability of success p, which is

$$\begin{aligned} p = |a_k|^2 = \sin^2\theta\big\{&[\cos(k\phi)\sin((k+1)\delta) \\ &+ \cos((k-1)\phi)\sin(k\delta)]^2 + [\sin(k\phi)\sin((k+1)\delta) \\ &+ \sin((k-1)\phi)\sin(k\delta)]^2\big\}/\sin^2\delta. \end{aligned} \quad (23)$$

From the equality (23) we can obtain the relation among the probability of success p, the phase shifts ϕ, the number of iterations k and the number of target items M. If k is fixed, the relation of the others can be confirmed. It is the same as phase shifts.

In this study, we assume that the number of iterations k is specified in advance and to ensure that the

probability of success of getting the target items is not less than some value we define the optimal phase shift as follows.

Definition 1. Letting p_{ij} be the probability of success of obtaining the target items with phase shifts of ϕ_i when the number of target items is j and $p_i = \min\{p_{ij}\}$, $1 \le j \le N$, then we define the optimal phase shifts

$$\phi_{opt} = \phi_{\{j:p_j = \max\limits_{0\le i\le 2\pi}\{p_i\}\}}.$$

Taking several given numbers of iterations as an example, we can give the optimal phase shifts and the corresponding probability of success according to the experimental simulations.

Let the number of iterations k is $\pi/(2\sin\theta)$. The relation among p, $\phi = \varphi$ and M/N is shown in Fig. 1. From Fig. 1, we know that the optimal phase shift is 1.018, and the algorithm using phase shift of 1.018 can reach a probability of success not less than 93.43% for an arbitrary M.

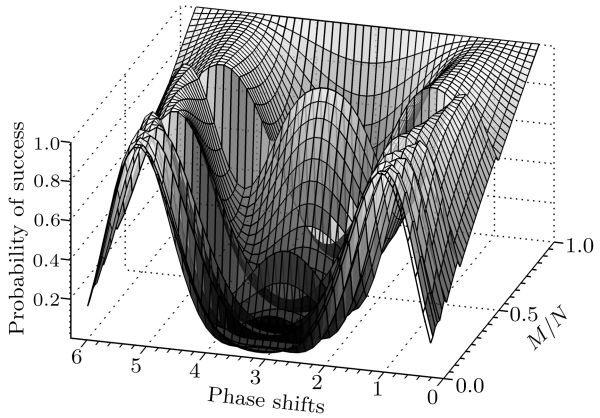

Fig. 1. Relation between p, ϕ and M/N when k is $\pi/(2\sin\theta)$.

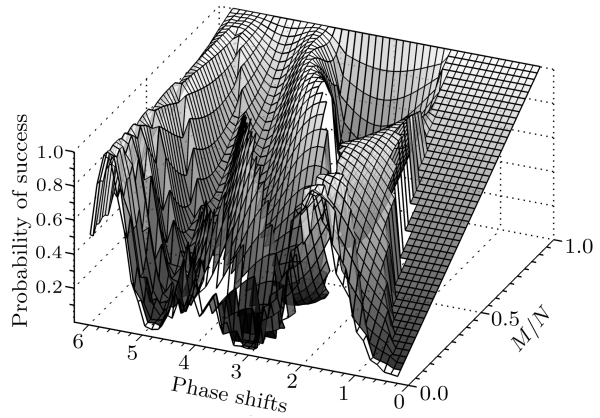

Fig. 2. Relation between p, ϕ and M/N when k is $\phi/(2\sin\theta)$.

Let the number of iterations k is $\phi/(2\sin\theta)$. The relation among p, $\phi = \varphi$ and M/N is shown in Fig. 2. From Fig. 2, the optimal phase shift is 5.734. The algorithm with phase shift of 5.734 can achieve the probability of success not less than 98.03% for an arbitrary M.

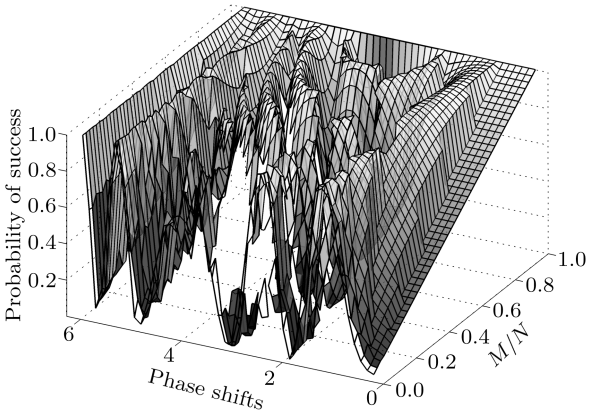

Fig. 3. Relation among p, ϕ and M/N when k is $\phi/\sin\theta$.

Let the number of iterations k is $\phi/\sin\theta$. The relation among p, $\phi = \varphi$ and M/N is shown in Fig. 3. From Fig. 3, the optimal phase shift is 6.019, of which the algorithm can succeed with probability not less than 99.58%. The same result was also obtained by Younes.[11]

The relation obtained here can help us to design the new algorithms using different phase shifts according to the success probability we desired and the number of iterations the computational ability can achieve, which is important to exhaust attack in cryptography. Selecting the optimal phase shift of 1.018 under the number of iterations $k = \pi/(2\sin\theta)$, we propose a new algorithm in the following.

Assuming the number of target items in the search space is M, we give the algorithm as follows.

Step 1. Setting the n qubits to be zero, then $|s\rangle^{\otimes n} = |0\rangle^{\otimes n}$ is the initial state. Applying $U = H^{\otimes n}$ on the $|s\rangle^{\otimes n}$, we can obtain

$$|\psi\rangle = U|s\rangle^{\otimes n} = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle = \sqrt{M/N}|\alpha\rangle + \sqrt{(N-M)/N}|\beta\rangle = (\sin(\theta),\cos(\theta))^T, \tag{24}$$

where $0 < \theta < \pi/2$.

Step 2. Letting the phase shift 1.018, $k = \pi/(2\sin(\theta))$ and applying the k iterations of G' on $|\psi\rangle$, we can obtain

$$|\psi^{(k)}\rangle = G^k(\sin(\theta),\cos(\theta))^T = (a_k, b_k)^T, \tag{25}$$

$$a_k = \frac{\sin(\theta)}{\sin(\delta)}\big(\exp(i\phi k)\sin((k+1)\delta) + \exp(i\phi(k-1))\sin(k\delta)\big), \tag{26}$$

$$b_k = \frac{\sin(\theta)}{\sin(\delta)} \exp\big(i\phi(k-1)\big)(\sin((k+1)\delta) + \sin(k\delta)). \quad (27)$$

Step 3. Testing the last state of the system, we obtain the probability of p,

$$p = |a_k|^2 = \sin^2\theta\big\{[\cos(k\phi)\sin((k+1)\delta) + \cos((k-1)\phi)\sin(k\delta)]^2 + [\sin(k\phi)\sin((k+1)\delta) + \sin((k-1)\phi)\sin(k\delta)]^2\big\}/\sin^2\delta. \quad (28)$$

Firstly, we summarize the probabilities of success and the number of iterations required in the proposed algorithm, and compare the proposed scheme with the algorithms presented in Refs. [1,9,11].

In our proposed algorithm, the probability of success, p, is

$$p = |a_k|^2 = \sin^2\theta\big\{[\cos(k\phi)\sin((k+1)\delta) + \cos((k-1)\phi)\sin(k\delta)]^2 + [\sin(k\phi)\sin((k+1)\delta) + \sin((k-1)\phi)\sin(k\delta)]^2\big\}/\sin^2\delta, \quad (29)$$

where the number of iterations is $\pi/[2\sin(\theta)] = \pi/(2\sqrt{M/N})$. Figure 3 shows the change of the probability of success with the increasing ratio of the target items in search space. We can find the plot that the minimum probability is 93.43% when $M/N = 0.6143$.

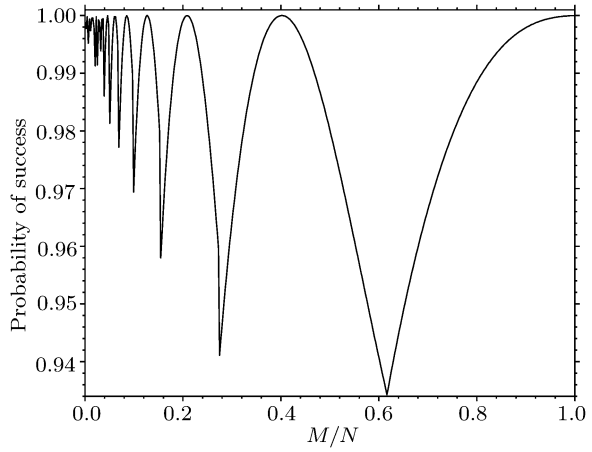

Fig. 4. Probability of success after $k = \pi/(2\sin\theta)$ iterations using the phase shift of 1.018.

The number of iterations in the initial Grover's algorithm is $k^G = \pi/(4\sin\theta) = \pi/(4\sqrt{M/N})$, and the probability of success is $p^G = \sin^2\big((2k^G+1)\theta\big)$. The relation among p^G and M/N using the number of iterations required is shown in Fig. 5. The minimum p^G in initial Grover's algorithm may reach 50% when $M/N = 0.5$.

It can be seen that the probability of success of the proposed algorithm is greatly improved, as compared with the minimum probability of success 50% of Grover's algorithm and 88.78% of the algorithm in Ref. [9]. Although the probability of success is slightly lower than that of the fixed phase algorithm proposed by Younes,[11] our algorithm just uses a quarter of the iterations of the fixed phase algorithm.

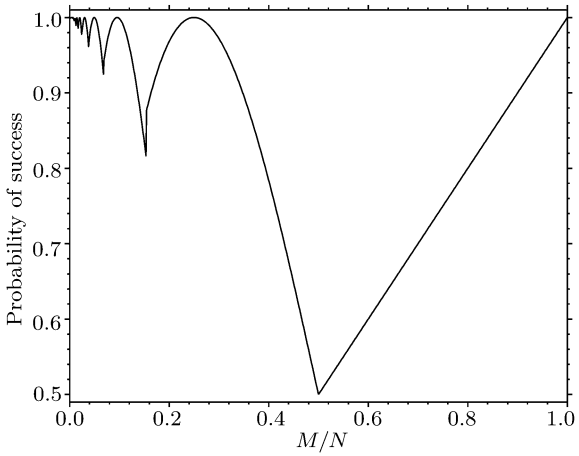

Fig. 5. Probability of success after the required iterations in Grover's algorithm.

In summary, we have investigated the relation among the probability of success, the phase shifts, the number of target items and the number of iterations, and obtain some optimal phase shifts under the condition that the numbers of iterations are given. According to the number of iterations we can accept and the probability of success we require, we can design a new algorithms using some of the optimal phase shifts. Finally, we use the phase shift of 1.018 to present a new quantum algorithm, of which the probability of success is not less than 93.43% for the target items of arbitrary number.

References

[1] Grover L K 1996 *The 28th Annual Symposium on the Theory of Computing* (New York 22–24 May 1996)
[2] Biham E and Kenigsberg D *Phys. Rev.* A **66** 062301
[3] Grover L K 1998 *Phys. Rev. Lett.* **80** 4329
[4] Boyer M, Brassard G, Høyer P and Tapp A 1996 *Proceedings of the 4th Workshop Physics and Computation* (Boston 22–24 November 1996)
[5] Brassard G, Høyer P, Mosca M and Tapp A 2000 *quantum-ph*/0005055
[6] Galindo A and Martin-Delgado M A 2000 *Phys. Rev.* A **62** 062303
[7] Zalka C 1999 *Phys. Rev.* A **60** 2746
[8] Nielson M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) chap 6 p 254
[9] Younes A, Rowe J and Miller J 2004 *Proceedings of the 7th International Conference on Quantum Communication, Measurement and Computing* (UK, 25–29 July 2004)
[10] Grover L K 2005 *Phys. Rev. Lett.* **95** 150501
[11] Younes A 2007 *quant-ph*/0704.1585v2
[12] Long G L, Li Y S, Zhang W L and Niu L 1999 *Phys. Lett.* A **262** 27