CHIN. PHYS. LETT. Vol. 34, No. 7 (2017) 070305

A Four-Phase Improvement of Grover's Algorithm *

Bo-Wen Ma(马博文)[1,2], Wan-Su Bao(鲍皖苏)[1,2**], Tan Li(李坦)[1,2], Feng-Guang Li(李风光)[1,2], Shuo Zhang(张硕)[1,2], Xiang-Qun Fu(付向群)[1,2]

[1]*Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou 450001*
[2]*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026*

(Received 26 April 2017)

When applying Grover's algorithm to an unordered database, the probability of obtaining correct results usually decreases as the quantity of target increases. A four-phase improvement of Grover's algorithm is proposed to fix the deficiency, and the unitary and the phase-matching condition are also proposed. With this improved scheme, when the proportion of target is over 1/3, the probability of obtaining correct results is greater than 97.82% with only one iteration using two phases. When the computational complexity is $O(\sqrt{M/N})$, the algorithm can succeed with a probability no less than 99.63%.

PACS: 03.67.Lx, 03.67.−a, 03.67.Ac DOI: 10.1088/0256-307X/34/7/070305

A quantum search algorithm is able to search a target in a parallel way. However, due to the property of quantum mechanics, it cannot yield an answer with certainty but with a probability. Therefore, how to increase the probability of a target is the key to design a quantum search algorithm. Grover's algorithm[1,2] is one of the most famous quantum search algorithms, compared with classical search algorithms, it achieves quadratic acceleration when searching a target in an unordered database. Nevertheless, there are still some imperfections with it. When the proportion of target is over 1/4, the success probability decreases rapidly, and when the proportion of target is over 1/2, the algorithm fails.

To amend these limitations, many methods have been proposed.[3–18] Grover[3] and Long *et al.*[4] extended the phases of the algorithm to be arbitrary. Younes *et al.*[9] proposed a quantum algorithm with the probability of success no less than 87.88% by using the partial diffusion operator. In 2005, Grover[10] presented a fixed point quantum algorithm with the phase $\pi/3$; when the proportion of target is more than 1/3, a target can be searched with the probability over 90% with only one iteration. Li *et al.*[11] proposed a new phase-matching condition, and they also mentioned that when the proportion of target is over 1/3, the success probability is greater than 25/27 with only one iteration. Zhong *et al.*[14] obtained a quantum search algorithm based on the phase 1.018, achieving a success probability larger than 93.43%. Li *et al.*[15] proposed a fixed-phase quantum search algorithm with more flexible behavior, yielding a success probability of 99.38% with the phase fixed at 0.1π. Younes[16] presented a fixed-phase search algorithm, yielding the minimum success probability at 99.58%, with phase fixed at 1.91684π. Li *et al.*[17] proposed his quantum search algorithm based on multi-phase, of which the success probability rises with the increase of the number of phases with just one iteration, and tends to be 100% when the proportion of target is over a limit. In 2017, Guo *et al.*[18] proposed a Q-learning-based adjustable fixed-phase quantum Grover search algorithm which avoids the optimal local situations, enabling success probabilities to approach one.

There are two phases which can be changed in Long's algorithm,[4] while three phases allowed changing in Ref. [11]. In this Letter, the number of variable phases is generated to four. In this proposed scheme, when the proportion of target is over 1/3, by using two different phases 1.3789 and 1.8025, the success probability is greater than 97.82% with only one iteration, which is relatively higher than the conclusion obtained by Zhong *et al.*[19] We also come up with an optimal phase 6.0215, of which the algorithm comes up with the probability no less than 99.63% in $O(\sqrt{M/N})$, which is relatively higher than the conclusion from Younes[16] under the same conditions.

When searching through an N-elements searching space $\{0, 1, 2 \ldots N-1\}(N = 2^n)$, these elements can be stored in n bits, and there are M targets for searching, $1 \leq M \leq N$.

The initial state of the algorithm is the equal superposition state $|s\rangle$,

$$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \quad (1)$$

Grover's algorithm consists of repeated application of a quantum subroutine, called Grover iteration, denoted as G, which may be broken up into four steps. (1) Apply the oracle I_t. The purpose of using oracle I_t is to reverse the amplitude of the target, which is $I_t|x\rangle = (-1)^{f(x)}|x\rangle$, when $|x\rangle = |t\rangle$ and $f(x) = 1$. When $|x\rangle \neq |t\rangle$ and $f(x) = 0$, $|t\rangle$ is the target state.

Therefore, I_t can be denoted as

$$I_t = I - 2|t\rangle\langle t|. \quad (2)$$

*Supported by the National Basic Research Program of China under Grant No 2013CB338002, and the National Natural Science Foundation of China under Grant No 11504430.

**Corresponding author. Email: 2010thzz@sina.com

© 2017 Chinese Physical Society and IOP Publishing Ltd

(2) Perform the Hadamard-transform $H^{\otimes n}$.

(3) Apply a conditional phase shift, which performs a (-1) phase shift to all states except $|0\rangle$. This transform can be expressed as

$$I_0 = 2|0\rangle\langle 0| - I. \tag{3}$$

(4) Perform the Hadamard-transform $H^{\otimes n}$.

It is useful to note that the combined effect of steps (2)–(4)

$$I_s = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|s\rangle\langle s| - I. \tag{4}$$

Thus the Grover iteration may be written as

$$G = I_s I_t. \tag{5}$$

In fact, the Grover iteration can be seen as a rotation in the two-dimensional space spanned by the vectors $|\alpha\rangle$ and $|\beta\rangle$, where $|\alpha\rangle$ indicates the normalized states of the sum of all targets, and $|\beta\rangle$ indicates normalized states of the sum of non-targets. The initial state $|s\rangle$ may be rewritten as

$$|s\rangle = \sin\theta|\alpha\rangle + \cos\theta|\beta\rangle, \tag{6}$$

where $\sin\theta = \sqrt{M/N}$.

Apply G to $|s\rangle$ for k times, and use some simple algebra

$$G^k|s\rangle = \sin((2k+1)\theta)|\alpha\rangle + \cos((2k+1)\theta)|\beta\rangle. \tag{7}$$

When this occurs, a target will be searched with the success probability

$$P = \sin^2((2k+1)\theta), \tag{8}$$

set[20]

$$k = \lfloor \frac{\pi\sqrt{N/M}}{4} \rfloor. \tag{9}$$

The image of P is shown in Fig. 1.

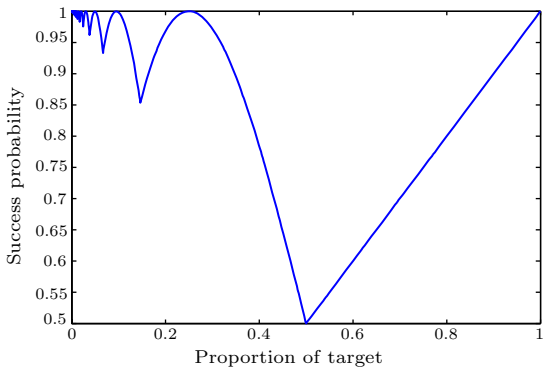

Fig. 1. The success probability as a function of the proportion of target in Grover's algorithm.

For simplicity, the proportion of target is denoted as $\lambda(\lambda = M/N)$. From Fig. 1, when $1/4 \le \lambda \le 1/2$, the success probability decreases rapidly, when $\lambda \ge 1/2$, the algorithm fails. From Eqs. (8) and (9), when $\lambda = 0.147$, $P = 0.854$, when $\lambda = 0.5$, $P = 0.5$.

To fix these limitations mentioned above, Long *et al.*[4] extended the phases of the algorithm from π to arbitrary. In the algorithm

$$\begin{aligned} I_0 &= (1 - e^{i\alpha})|0\rangle\langle 0| - I, \\ I_t &= I - (1 - e^{i\beta})|t\rangle\langle t|, \end{aligned} \tag{10}$$

which obtain two changeable phases, Long *et al.*[4] also found a phase-matching condition, that is, when $\alpha = \beta$, the success probability is much higher.

Li *et al.*[11] proposed a different improved scheme from phases and a different phase-matching condition. In the algorithm,

$$\begin{aligned} I_0 &= (1 - e^{i\alpha})|0\rangle\langle 0| + e^{i\alpha} I, \\ I_t &= I - (1 - e^{i\beta})|t\rangle\langle t|, \end{aligned} \tag{11}$$

which obtains three changeable phases, and the phase-matching condition is $\alpha = -\beta$. Li *et al.*[11] also mentioned that when $\lambda \ge 1/3$, setting $\alpha = -\beta = -\pi/2$, the success probability $P \ge 25/27$ can be obtained after only one Grover iteration.

In this four-phase improved scheme, two operators are generally expressed as follows:

$$\begin{aligned} I_0 &= (1 - e^{i\beta})|0\rangle\langle 0| + e^{i\alpha} I, \\ I_t &= -e^{i\varphi} I - (1 - e^{i\phi})|t\rangle\langle t|. \end{aligned} \tag{12}$$

The four changeable phases α, β, φ and ϕ must keep $\alpha = \beta$ or $\alpha = \pi$ and $\varphi = \phi$ or $\varphi = \pi$.

The unitary of the operator described by Eq. (12) is proved in the following. Since

$$I_0 = (1 - e^{i\beta})|0\rangle\langle 0| + e^{i\alpha} I, \tag{13}$$

then

$$I_0^\dagger = (1 - e^{-i\beta})|0\rangle\langle 0| + e^{-i\alpha} I, \tag{14}$$

$$\begin{aligned} I_0 I_0^\dagger &= \begin{pmatrix} 1 - e^{i\beta} + e^{i\alpha} & 0 & \cdots & 0 \\ 0 & e^{i\alpha} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{i\alpha} \end{pmatrix} \\ &\quad \times \begin{pmatrix} 1 - e^{-i\beta} + e^{-i\alpha} & 0 & \cdots & 0 \\ 0 & e^{-i\alpha} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{-i\alpha} \end{pmatrix} \\ &= \begin{pmatrix} A_{11} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, \end{aligned} \tag{15}$$

where $A_{11} = (1 - e^{i\beta} + e^{i\alpha})(1 - e^{-i\beta} + e^{-i\alpha})$. If I_0 is unitary,

$$(1 - e^{i\beta} + e^{i\alpha})(1 - e^{-i\beta} + e^{-i\alpha}) = 1, \tag{16}$$

must be satisfied. From Eq. (16), $\alpha = \pi$ or $\alpha = \beta$ is obtained,

$$I_t = -e^{i\varphi} I - (1 - e^{i\phi})|t\rangle\langle t|, \tag{17}$$

$$I_t^\dagger = -e^{-i\varphi} I - (1 - e^{-i\phi})|t\rangle\langle t|, \tag{18}$$

$$\begin{aligned} I_t I_t^\dagger = &-[e^{i\varphi}(1 - e^{-i\phi}) + e^{-i\varphi}(1 - e^{i\phi})]|t\rangle\langle t| \\ &+ 1 + (1 - e^{i\phi})(1 - e^{-i\phi})(|t\rangle\langle t|)^2. \end{aligned} \tag{19}$$

Since $(|t\rangle\langle t|)^2 = |t\rangle\langle t|$, then

$$I_t I_t^\dagger = [(1-e^{i\phi})(1-e^{-i\phi}) - e^{i\varphi}(1-e^{-i\phi}) + e^{-i\varphi}(1-e^{i\phi})]|t\rangle\langle t| + 1. \quad (20)$$

If I_t is unitary,

$$(1-e^{i\phi})(1-e^{-i\phi}) - e^{i\varphi}(1-e^{-i\phi}) + e^{-i\varphi}(1-e^{i\phi}) = 0 \quad (21)$$

must be satisfied. From Eq. (21), $\varphi = \pi$ or $\varphi = \phi$ is obtained.

Since the Hadamard-transform $H^{\otimes n}$ is unitary, the unitary of this proposed scheme is proved. When $\alpha = \pi$, $\varphi = \phi$, it degenerates to Li's scheme.[11] When $\alpha = \pi$, $\varphi = \pi$, it becomes Long's algorithm.[4] When $\alpha = \beta = \phi = \varphi = \pi$, it becomes the original Grover's algorithm.[1]

In this study, set $\alpha = \beta$ and $\varphi = \phi$, then operators I_s and I_t can be written as

$$I_s = (1-e^{i\alpha})|s\rangle\langle s| + e^{i\alpha} I,$$
$$I_t = -e^{i\phi} I - (1-e^{i\phi})|t\rangle\langle t|. \quad (22)$$

Next, the performance of this four-phase scheme with one iteration is studied.

Applying this four-phase Grover iteration to the initial state $|s\rangle$ described by Eq. (1),

$$|\psi_1\rangle = G|s\rangle = I_s I_t |s\rangle, \quad (23)$$
$$I_t|s\rangle = [-e^{i\phi} I - (1-e^{i\phi})|t\rangle\langle t|][\sin\theta|\alpha\rangle + \cos\theta|\beta\rangle] = -e^{i\phi}|s\rangle - (1-e^{i\phi})\sin\theta|\alpha\rangle, \quad (24)$$

then

$$\begin{aligned}|\psi_1\rangle &= I_s I_t |s\rangle \\ &= [(1-e^{i\alpha})|s\rangle\langle s| + e^{i\alpha} I][-e^{i\phi}|s\rangle \\ &\quad - (1-e^{i\phi})\sin\theta|\alpha\rangle] \\ &= -\sin\theta[e^{i\phi} + \sin^2\theta(1-e^{i\alpha})(1-e^{i\phi}) \\ &\quad + e^{i\alpha}(1-e^{i\phi})]|\alpha\rangle - \cos\theta[e^{i\phi} + \sin^2\theta \\ &\quad \cdot (1-e^{i\alpha})(1-e^{i\phi})]|\beta\rangle. \end{aligned} \quad (25)$$

Letting

$$\delta = -\sin\theta[e^{i\phi} + \sin^2\theta(1-e^{i\alpha})(1-e^{i\phi}) + e^{i\alpha}(1-e^{i\phi})], \quad (26)$$

the success probability $P = |\delta|^2$. The control variant method is used to analyze P, setting $\sin\theta = 0.1$ and $\sin\theta = 0.5$, respectively, namely, the proportions of target are 0.01 and 0.25, the surface charts of P are shown in Figs. 2 and 3.

Figures 4 and 5 are the top views of Figs. 2 and 3, respectively.

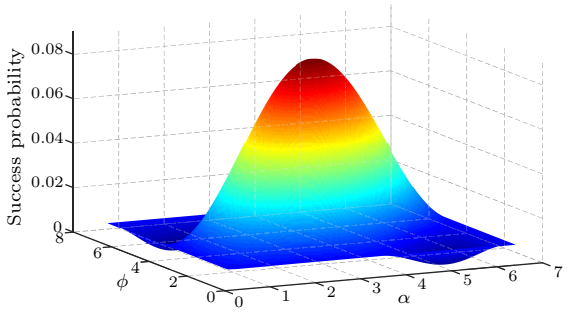

Fig. 2. The relationship between the success probability P, phases α and ϕ, when $\lambda = 0.01$.

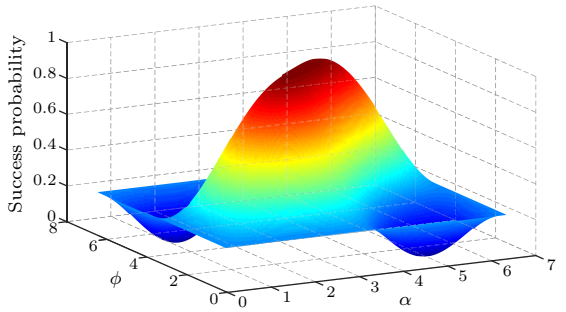

Fig. 3. The relationship between the success probability P, phases α and ϕ, when $\lambda = 0.25$.

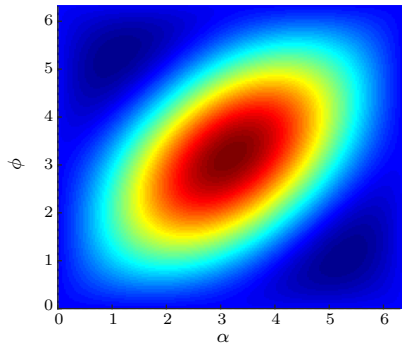

Fig. 4. The top view of Fig. 2.

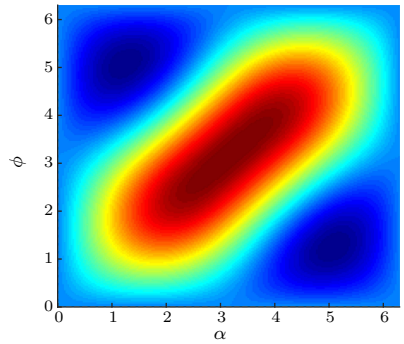

Fig. 5. The top view of Fig. 3.

From these figures, when $\alpha = \phi$, the success probability is obviously higher, therefore, $\alpha = \phi$ is taken as the phase-matching condition. Under this condition, P can be simplified to

$$P = (4\cos^2\alpha - 8\cos\alpha + 4)\lambda^3 + (-4\cos^2\alpha + 12\cos\alpha - 8)\lambda^2 + (5 - 4\cos\alpha)\lambda. \quad (27)$$

When $\alpha = 1.3789$ and $\alpha = 1.8025$, the curves

of P are shown in Fig. 6 ($\alpha = 1.3789$) and Fig. 7 ($\alpha = 1.8025$), respectively.

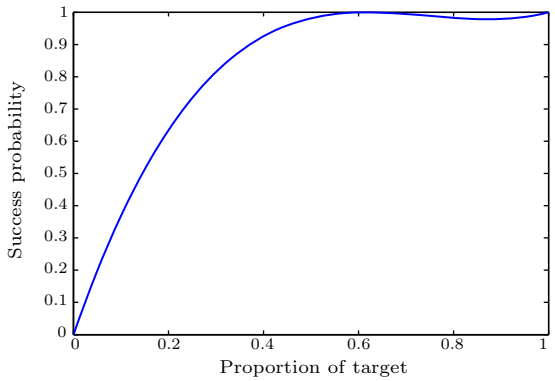

Fig. 6. The success probability as a function of the proportion of target in our scheme when the phase $\alpha = 1.3789$.

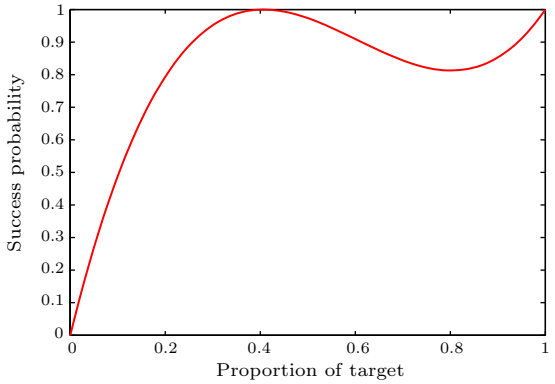

Fig. 7. The success probability as a function of the proportion of target in our scheme when the phase $\alpha = 1.8025$.

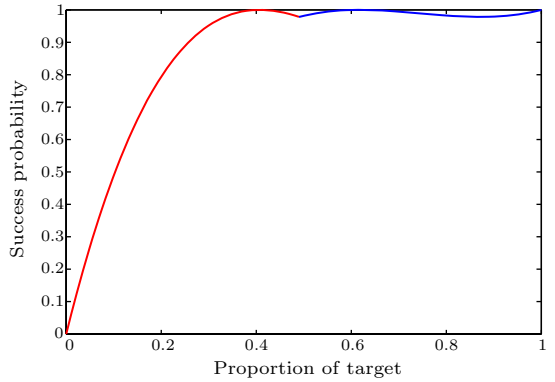

Fig. 8. The success probability as a function of the proportion of target. When the proportion of target $0 \leq \lambda \leq 0.490$, setting the phase $\alpha = 1.8025$, and when the proportion of target $\lambda \geq 0.490$, setting the phase $\alpha = 1.3789$.

From Figs. 6 and 7, when the proportion of target $1/3 \leq \lambda \leq 0.490$, by setting the phase $\alpha = 1.8025$, the minimum of P is 97.83%. When the proportion of target $\lambda \geq 0.490$, by setting the phase $\alpha = 1.3789$, the minimum of P is 97.82%. As a result, when $\lambda \geq 1/3$, the minimum of P is 97.82% with just one iteration, which is relatively higher than the conclusion obtained by Zhong *et al.*[19] The curve of P is shown in Fig. 8.

Then the performance of this four-phase scheme is researched with arbitrary iteration.

With the basis vectors $|\alpha\rangle$ and $|\beta\rangle$, the four-phase Grover iteration can be expressed as

$$G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix}, \tag{28}$$

where $G_{11} = -[e^{i\alpha} + (1 - e^{i\alpha})\sin^2\theta]$, $G_{12} = -e^{i\alpha}(1 - e^{i\alpha})\sin\theta\cos\theta$, $G_{21} = -(1 - e^{i\alpha})\sin\theta\cos\theta$, and $G_{22} = -[e^{2i\alpha} + e^{i\alpha}(1 - e^{i\alpha})\cos^2\theta]$. The phase-matching condition $\alpha = \phi$ is still used. Here $|s\rangle$ can be re-expressed as $(\sin\theta, \cos\theta)^{\mathrm{T}}$ with the basis vectors $|\alpha\rangle$ and $|\beta\rangle$. Using $|s\rangle$ as the initial state, and applying the four-phase Grover iteration to $|s\rangle$ for k times

$$|\psi^{(k)}\rangle = G^k(\sin\theta, \cos\theta)^{\mathrm{T}} = (a_k, b_k)^{\mathrm{T}}. \tag{29}$$

A target will be searched with the probability $P = |a_k|^2$ after measuring $|\psi^{(k)}\rangle$. Here P is functions of α, θ and k. Set $k = \lfloor \pi/\sin\theta \rfloor$, the relationship between the probability P, phase α and the proportion of target λ is shown in Fig. 9.

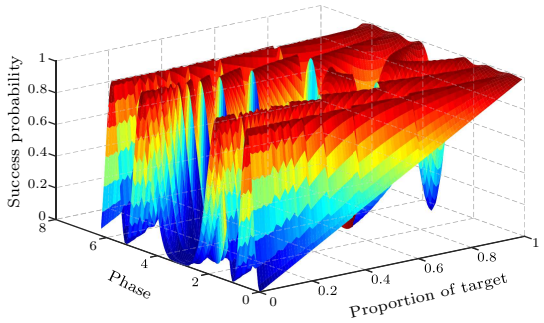

Fig. 9. The relationship between probability, phase, and proportion of target.

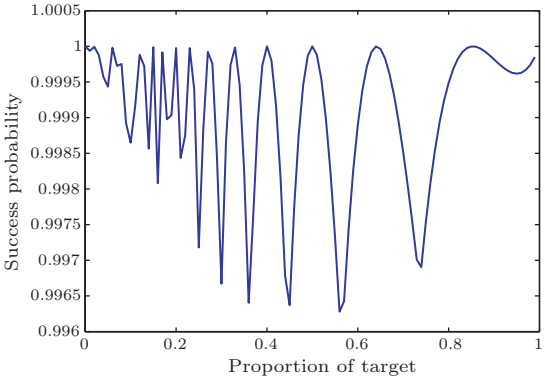

Fig. 10. The success probability as a function of the proportion of target in our scheme when the number of iterations $k = \lfloor \pi/\sin\theta \rfloor$ and the phase $\alpha = 6.0215$.

The definition of optimal phase from Zhong and Bao[14] is used for further research.

Definition 1: Let p_{ij} be the probability of success of obtaining the targets with phase shifts of α_i, when the number of targets is j and $p_i = \min\{p_{ij}\}, 1 \leq j \leq N$, then the optimal phase shifts can be defined as

$$\phi_{\mathrm{opt}} = \phi_{\{\mathrm{opt}:P_{\mathrm{opt}} = \max\limits_{0 \leq i \leq 2\pi}\{P_i\}\}}. \tag{30}$$

From Fig. 9, the optimal phase of this four-phase scheme $\alpha = 6.0215$ can be obtained, of which the algorithm can succeed with a probability no less than

99.63%, which is relatively better than the conclusion from Younes.[16] This outcome is shown clearly in Fig. 10.

In conclusion, a four-phase improved scheme of Grover's algorithm has been proposed, and the unitary and phase-matching condition have also been proposed. With this scheme, the probability of obtaining correct results is improved. When the proportion of target $\lambda \geq 1/3$, using two different phases 1.3789 and 1.8025, the minimum of success probability is 97.82% with just one iteration. When the computational complexity is $O(\sqrt{M/N})$, the algorithm can succeed with a probability no less than 99.63% with the phase 6.0215.

References

[1] Grover L K 1996 *Proceedings of the 28th Annual Symposium on Theory of Computing* (New York: ACM Press)
[2] Grover L K 1997 *Phys. Rev. Lett.* **79** 325
[3] Grover L K 1998 *Phys. Rev. Lett.* **80** 4329
[4] Long G L, Li Y S, Zhang W L and Niu L 1999 *Phys. Lett.* A **262** 27
[5] Biham E, Biham O, Biron D, Grassl M and Lidar D A 1999 *Phys. Rev.* A **60** 2742
[6] Hoyer P 2000 *Phys. Rev.* A **62** 052304
[7] Long G L 2001 *Phys. Rev.* A **64** 022307
[8] Long G L, Li X and Sun Y 2002 *Phys. Lett.* A **294** 143
[9] Younes A, Rowe J and Miller J 2004 *Proc. 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] Li P C and Li S Y 2007 *Phys. Lett.* A **366** 42
[12] Toyama F M, Van Dijk W, Nogami Y, Tabuchi M and Kimura Y 2008 *Phys. Rev.* A **77** 042324
[13] Tulsi A 2008 *Phys. Rev.* A **78** 022332
[14] Zhong P C and Bao W S 2008 *Chin. Phys. Lett.* **25** 2774
[15] Li X and Li P C 2012 *J. Quantum Inf. Sci.* **2** 28
[16] Younes A 2013 *Appl. Math. Inf. Sci.* **7** 93
[17] Li T, Bao W S, Lin W Q, Zhang H and Fu X Q 2013 *Chin. Phys. Lett.* **30** 050301
[18] Guo Y, Shi W S et al 2017 *J. Phys. Soc. Jpn.* **86** 024006
[19] Zhong P C and Bao W S 2008 *Proc. ICCSE 3rd International Conference on Computer Science & Education* (Kaifeng, China, 25–27 July 2008)
[20] Nielson M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) chap 6 p 253