Optimized quantum random-walk search algorithm for multi-solution search*

Zhang Yu-Chao(张宇超)[a)b)], Bao Wan-Su(鲍皖苏)[a)b)†], Wang Xiang(汪 翔)[a)b)], and Fu Xiang-Qun(付向群)[a)b)]

[a)] Zhengzhou Information Science and Technology Institute, Zhengzhou 450004, China

[b)] Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China

(Received 11 July 2015; published online 10 October 2015)

This study investigates the multi-solution search of the optimized quantum random-walk search algorithm on the hypercube. Through generalizing the abstract search algorithm which is a general tool for analyzing the search on the graph to the multi-solution case, it can be applied to analyze the multi-solution case of quantum random-walk search on the graph directly. Thus, the computational complexity of the optimized quantum random-walk search algorithm for the multi-solution search is obtained. Through numerical simulations and analysis, we obtain a critical value of the proportion of solutions q. For a given q, we derive the relationship between the success rate of the algorithm and the number of iterations when q is no longer than the critical value.

Keywords: quantum search algorithm, quantum random walk, multi-solution, abstract search algorithm

PACS: 03.67.Lx, 03.67.Ac **DOI:** 10.1088/1674-1056/24/11/110309

1. Introduction

The concepts of quantum computation and quantum computer[1] were proposed by Feynman in 1982. In 1985, Deutsch pointed out that the parallel quantum computation could be achieved by taking advantage of the coherent superposition of quantum states.[2] However, it was not until later when Shor's algorithm[3] and Grover's algorithm[4] were proposed that extensive attention into quantum computers and quantum algorithms was aroused.[5–7] These greatly promoted the development of quantum computation and quantum communication technologies.

Essentially, Grover's algorithm is an exhaustive algorithm on the quantum computer. It solves the unsorted database search and achieves the quadratic speed-up compared with the classical algorithm. Although the Grover algorithm does not reach the obvious increase in speed compared with Shor's algorithm, the widely applicable search algorithm has also attracted people's attention. With the in-depth study, the efficiency of Grover's algorithm has been constantly improved, and it is more and more applied in practical problems. In 2001, Long proposed an improved Grover's algorithm with a success rate of 1 by replacing the phase inversion by phase rotation.[8] The Long algorithm[8] has proven to be optimal and the simplest by far.[9] In 2010, Wang *et al.* proposed a quantum algorithm for searching a target solution of fixed weight, which is more efficient to search for the NTRU private key.[10] In practice, the search space often contains a multi-solution. When Grover's algorithm is applied to the multi-solution search, the success rate of the algorithm has the potential to reduce. If the proportion of solutions is between $1/4$ and $1/2$, the success rate will reduce to $1/2$. To solve this problem, there have been many improved algorithms proposed.[11–13] Through altering the phase matching and the number of iterations, the success rate of the algorithm can be improved obviously. In Ref. [14], the multi-solution of Long's algorithm was also briefly mentioned. Moreover, the quantum deletion algorithms,[15,16] which are related to the quantum search algorithm are presented. All the above studies make Grover's algorithm be used more and more widely, and promote the development of the quantum search algorithm.

In recent years, quantum random walks have attracted much attention.[17–19] The quantum random walk is a generalization of random walk with the quantum mechanical, which can be used to design effective quantum algorithms.[20–22] In 2003, Shenvi *et al.* proposed an algorithm based on quantum random walks (SKW algorithm), which is applied to the unsorted database search as Grover's algorithm.[23] The SKW algorithm is similar in many steps to the operation of Grover's algorithm. Both algorithms make use of the Grover diffusion operator. Both algorithms use an oracle which marks the target state with a phase of -1, and both algorithms have a running time of $O(\sqrt{N})$. Because it has been proved that the quantum random walks can be physically implemented,[24,25] the proposed SKW algorithm provides a new approach to achieve the quantum search algorithm. Although the SKW algorithm is not superior to Grover's algorithm in computational complexity, it has certain advantages in physical implementation and resistance to errors. In 2006, Li studied the effects of the error in the Grover diffusion operator on the SKW algorithm and found that the resistance to errors of the SKW algorithm is

*Project supported by the National Basic Research Program of China (Grant No. 2013CB338002).

†Corresponding author. E-mail: 2010thzz@sina.com

© 2015 Chinese Physical Society and IOP Publishing Ltd

stronger than that of Grover's algorithm.[26] In 2008, Potocek put forward an optimized quantum random-walk search algorithm (optimized SKW algorithm) on the basis of the SKW algorithm, and the success rate of the algorithm and the number of iterations were further optimized.[27] In 2015, Zhang *et al.* studied the effects of the error in phase inversions on the optimized SKW algorithm and found that it is more robust against phase errors than Grover's algorithm.[28] Therefore, studying the search algorithm based on quantum random walks has certain theoretical significance and practical value.

However, the SKW algorithm was proposed only to search for one solution. Although numerical calculations suggest that it can also be used to search for a multi-solution, no related demonstrations and results have been presented. This is because when there is one solution, we use the method of geometric description to prove that the SKW algorithm is a rotation in the plane defined by the initial state and the final state, and the final state is composed primarily of the solution. When the number of solutions is larger than one, we cannot construct the final state properly to prove the algorithm by geometric description. In general, one solution is just a special case of multi-solution. Moreover, the optimized SKW algorithm can be generalized to the multi-solution case (Ref. [27]) based on the assumption that the SKW algorithm is applicable to the multi-solution case. Therefore, the research on the multi-solution case of the algorithm is meaningful and necessary whether on the algorithm itself or the follow-up research. In 2004, Ambainis *et al.* proposed an abstract search algorithm which is applied to search on the graph, and verified the correctness of the SKW algorithm with one solution.[29] In the same year, Szegedy showed how to analyze the multi-solution case for a different quantum walk algorithm, element distinctness.[30] These investigations provided ideas and possibilities for the study of the multi-solution case of the SKW algorithm and the optimized SKW algorithm.

This paper studies the multi-solution search of the optimized SKW algorithm. We first generalize the abstract search algorithm to the multi-solution case which is originally applied to search for one solution on the graph. Thus, it can be applied to analyze the multi-solution search of quantum random walk on the graph directly. Then, we obtain the computational complexity of the optimized SKW algorithm with multi-solution through the generalized abstract search algorithm. Using theoretical analysis and numerical simulations, we find that if the proportion of solutions q is small, the success rate of the algorithm and the number of iterations decrease with the increase of q. Finally, we obtain a critical value of q. When q is not larger than the critical value, for a given q, we derive the relationship between the success rate of the algorithm and the number of iterations.

The rest of this paper is organized as follows. In Section 2, we introduce the background. The optimized SKW algorithm with multi-solution is proposed in Section 3. In Section 4, we give the results of numerical simulations. The conclusion is given in Section 5.

2. Background

2.1. SKW algorithm

The SKW algorithm is based on a quantum random walk on a hypercube. Let $C_n = (V_n, E_n)$ denote the graph of the n-dimensional hypercube. The vertices V_n of the hypercube are labelled by binary, $\boldsymbol{x} = (x_1, x_2, \ldots, x_n), x_i = \{0,1\}$. The Hamming weight of $\boldsymbol{x}$ is $|\boldsymbol{x}|$. They are connected only if their Hamming distance is 1. The Hilbert space of the SKW algorithm is $H^{C_n} \otimes H^{V_n}$ where H^{V_n} is the 2^n-dimensional Hilbert space representing the vertices, and H^{C_n} is the n-dimensional space associated with the quantum coin.

The operator of the SKW algorithm can be written as $U' = SC'$, where S is the shift operator

$$S = \sum_{x=0}^{2^n-1} \sum_{d=1}^{n} |d, \boldsymbol{x} \oplus \boldsymbol{e}_d\rangle \langle d, \boldsymbol{x}|, \tag{1}$$

where $|\boldsymbol{e}_d\rangle = |0\cdots010\cdots0\rangle$ corresponds to the edges originating from the given vertex, S performs a control transfer depending on the state of d. If the target is $\boldsymbol{x}_{\mathrm{tg}}$, the coin operator can be written as

$$C' = C_0 \otimes I + (C_1 - C_0) \otimes \left|\boldsymbol{x}_{\mathrm{tg}}\right\rangle \left\langle \boldsymbol{x}_{\mathrm{tg}}\right|, \tag{2}$$

where C_0 is generally chosen as the Grover operator: $-I + 2\left|S^{\mathrm{C}}\right\rangle \left\langle S^{\mathrm{C}}\right|$, and $\left|S^{\mathrm{C}}\right\rangle = \sum_{d=1}^{n} |d\rangle/\sqrt{n}$, C_1 is generally chosen to be $-I$, taking on the function of an oracle. Without loss of generality, we can assume that $\boldsymbol{x}_{\mathrm{tg}} = 0$.

The initial state of the SKW algorithm is the equal superposition over all states $|\psi_0\rangle = \sum_{d=1}^{n} \sum_{\boldsymbol{x}} |d, x\rangle/\sqrt{n2^n}$. Applying the evolution operator U' to $|\psi_0\rangle$ with $\pi\sqrt{2^{n-1}}/2$ times, we will obtain the target $|0\rangle$ with a probability close to 0.5.

2.2. Optimized SKW algorithm

The optimized SKW algorithm is based on the SKW algorithm, but quantum random walks occur on an $(n+1)$-dimensional hypercube, $p(\boldsymbol{x}) = |\boldsymbol{x}| \bmod 2$ is denoted the parity bit of $\boldsymbol{x}$. Then a map from the 2^n-dimensional space to the 2^{n+1}-dimensional space can be built, $\boldsymbol{x} \to \boldsymbol{x}' = \boldsymbol{x}||p(\boldsymbol{x})$. After mapping, $\boldsymbol{x}$ corresponds to the vertices of an $(n+1)$-dimensional hypercube, and the Hamming weights of them are even. Because $\boldsymbol{x}$ is one-to-one with $\boldsymbol{x}'$, the oracle is capable of identifying the target after mapping.

The operator of the optimized SKW algorithm can be written as $U' = S(C_0 \otimes I)SC'$. Each iteration C' is only applied once, which is equivalent to calling the oracle once. The

initial state is the equal superposition over coin space and the even vertice space $\left|\psi_0^{(\mathrm{e})}\right\rangle$. Applying the evolution operator U' to $\left|\psi_0^{(\mathrm{e})}\right\rangle$ with $\pi\sqrt{2^n}/4$ times, the probability to obtain the target $|0\rangle$ is close to 1.

2.3. Abstract search algorithm

The abstract search algorithm consists of two unitary transformations U_1 and U_2 and two states $|\psi_{\mathrm{start}}\rangle$ and $\left|\psi_{\mathrm{good}}\right\rangle$. It requires the following properties.

(i) $U_1 = I - 2\left|\psi_{\mathrm{good}}\right\rangle\left\langle\psi_{\mathrm{good}}\right|$.

(ii) $U_2|\psi_{\mathrm{start}}\rangle = |\psi_{\mathrm{start}}\rangle$, the amplitude of $|\psi_{\mathrm{start}}\rangle$ is real, and there is no other eigenvector with eigenvalue 1.

(iii) U_2 is described by a real unitary matrix.

The abstract search algorithm applies the unitary transformation $(U_2U_1)^{\mathrm{T}}$ to the initial state with a proper T. The final state $(U_2U_1)^{\mathrm{T}}|\psi_{\mathrm{start}}\rangle$ has a sufficiently large inner product with $\left|\psi_{\mathrm{good}}\right\rangle$. The main properties of abstract search algorithm will be given in the following.

Since U_2 is a real unitary matrix, its non-±1 eigenvalues come in pairs of complex conjugate numbers. Denote them by $\mathrm{e}^{\pm\mathrm{i}\theta_1},\ldots,\mathrm{e}^{\pm\mathrm{i}\theta_m}$. Let $\theta_{\min} = \min(\theta_1,\ldots,\theta_{\mathrm{m}})$ and $U' = U_2U_1$.

Lemma 1 Define the arc A as the set of $\mathrm{e}^{\mathrm{i}\theta}$ for all real θ satisfying $-\theta_{\min} < \theta < \theta_{\min}$. Then U' has at most two eigenvalues in A.

Let $|\Phi_j^+\rangle$ and $|\Phi_j^-\rangle$ be the eigenvectors with eigenvalues $\mathrm{e}^{\mathrm{i}\theta_j}$ and $\mathrm{e}^{-\mathrm{i}\theta_j}$, respectively. We express $\left|\psi_{\mathrm{good}}\right\rangle$ as a superposition of the eigenvectors of U_2 as

$$\left|\psi_{\mathrm{good}}\right\rangle = a_0|\psi_{\mathrm{start}}\rangle + \sum_{j=1}^{m}(a_j^+|\Phi_j^+\rangle + a_j^-|\Phi_j^-\rangle). \tag{3}$$

Lemma 2 It is possible to select $|\Phi_j^+\rangle$ and $|\Phi_j^-\rangle$ so that $a_j^+ = a_j^-$ and a_j^+ is a real number.

Lemma 3 The eigenvalues of U' in A are $\mathrm{e}^{\pm\mathrm{i}\alpha}$ where

$$\alpha = O\left(\frac{1}{\sqrt{\sum_j \dfrac{a_j^2}{a_0^2}\dfrac{1}{1-\cos\theta_j}}}\right). \tag{4}$$

Let $|\omega_\alpha\rangle$ and $|\omega_{-\alpha}\rangle$ be the two eigenvectors with eigenvalues $\mathrm{e}^{\mathrm{i}\alpha}$ and $\mathrm{e}^{-\mathrm{i}\alpha}$, respectively. Define

$$\left|\omega'_{\mathrm{start}}\right\rangle = \frac{1}{\sqrt{2}}|\omega_\alpha\rangle - \frac{1}{\sqrt{2}}|\omega_{-\alpha}\rangle,$$
$$|\omega_{\mathrm{start}}\rangle = \frac{1}{||\,|\omega'_{\mathrm{start}}\rangle\,||}\left|\omega'_{\mathrm{start}}\right\rangle,$$

and then, $|\omega_{\mathrm{start}}\rangle$ is close to the starting state $|\psi_{\mathrm{start}}\rangle$.

Lemma 4 Assume that $\alpha < \theta_{\min}/2$, and then

$$\langle\psi_{\mathrm{start}}|\omega_{\mathrm{start}}\rangle \geq 1 - O\left(\alpha^4\sum_j \frac{a_j^2}{a_0^2}\frac{1}{1-\cos\theta_j}\right). \tag{5}$$

Lemma 5 Assume that $\alpha < \theta_{\min}/2$. Let $\left|\omega_{\mathrm{good}}\right\rangle = |\omega_\alpha\rangle/\sqrt{2} + |\omega_{-\alpha}\rangle/\sqrt{2}$, and then

$$|\left\langle\psi_{\mathrm{good}}|\omega_{\mathrm{good}}\right\rangle| = O\left(\min\left(\frac{1}{\sum_j a_j^2\cot^2\dfrac{\theta_j}{4}}, 1\right)\right). \tag{6}$$

According to the Lemmas of the abstract search algorithm, we can regard the algorithm being studied as an instance of the abstract search algorithm and then obtain the computational complexity of it.

3. Optimized SKW algorithm with multi-solution

3.1. Generalization of the abstract search algorithm

The abstract search algorithm is proposed for the search of quantum random walks on the graph, but it applies to one solution. In Theorem 5 of Ref. [29], it is generalized to the case of two solutions. In this section, we will generalize the abstract search algorithm to the multi-solution case.

Lemma 6 The abstract search algorithm searching for four solutions v_1, v_2, v_3, v_4 is reduced to search for s'_1, s'_2, where

$$\left|s'_1\right\rangle = \frac{|s,v_1\rangle + |s,v_2\rangle}{\sqrt{2}}, \quad \left|s'_2\right\rangle = \frac{|s,v_3\rangle + |s,v_4\rangle}{\sqrt{2}},$$

and s is the equal superposition over coin space.

Proof Assume v_1 and v_2 are two solutions and $|\psi\rangle$ is the initial state, and U' is the operator of the algorithm. Then we can obtain the following relationship according to Claim 12 in Ref. [29]:

$$\begin{aligned}&(I - 2|s,v_1\rangle\langle s,v_1| - 2|s,v_2\rangle\langle s,v_2|)(U')^t|\psi\rangle\\ =\ &(I - 2\left|s'_1\right\rangle\left\langle s'_1\right|)(U')^t|\psi\rangle,\end{aligned} \tag{7}$$

where $|s'_1\rangle = |s,v_1\rangle + |s,v_2\rangle/\sqrt{2}$. The above relationship regards the case of searching for v_1 and v_2 as the case of searching for s'_1. Similarly, if v_3 and v_4 are two solutions, we have

$$\begin{aligned}&(I - 2|s,v_3\rangle\langle s,v_3| - 2|s,v_4\rangle\langle s,v_4|)(U')^t|\psi\rangle\\ =\ &(I - 2\left|s'_2\right\rangle\left\langle s'_2\right|)(U')^t|\psi\rangle,\end{aligned} \tag{8}$$

where $|s'_2\rangle = |s,v_3\rangle + |s,v_4\rangle/\sqrt{2}$. Then we add up Eqs. (7) and (8) by the left and right respectively, having the following relationship:

$$\begin{aligned}&(I - 2|s,v_1\rangle\langle s,v_1| - 2|s,v_2\rangle\langle s,v_2| - 2|s,v_3\rangle\\ &\langle s,v_3| - 2|s,v_4\rangle\langle s,v_4|)(U')^t|\psi\rangle\\ =\ &(I - 2\left|s'_1\right\rangle\left\langle s'_1\right| - 2\left|s'_2\right\rangle\left\langle s'_2\right|)(U')^t|\psi\rangle.\end{aligned} \tag{9}$$

Thus, the abstract search algorithm searching for four solutions reduces to searching for two superposition states. Lemma 6 is proved.

Lemma 7 The abstract search algorithm searching for four solutions v_1, v_2, v_3, v_4 is reduced to searching for s''_1, where $s''_1 = (s'_1 + s'_2)/\sqrt{2}$.

Proof According to Eq. (7), the abstract search algorithm searching for two solutions v_1 and v_2 in space $\{v_1, v_2, \ldots, v_N\}$ is reduced to searching for s'_1 with the initial state

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |s, v_i\rangle.$$

Similarly, searching for two solutions s'_1 and s'_2 in space $\{s'_1, s'_2, \ldots, s'_M\}$ is reduced to searching for s''_1 with the initial state $|\psi_1\rangle = \sum_{i=1}^{M} |s_i'\rangle/\sqrt{M}$. Therefore

$$\begin{aligned} &(I - 2|s'_1\rangle\langle s'_1| - 2|s'_2\rangle\langle s'_2|)(U')^t |\psi_1\rangle \\ &= (I - 2|s''_1\rangle\langle s''_1|)(U')^t |\psi_1\rangle . \end{aligned} \tag{10}$$

If $|s'_i\rangle$ is composed of elements in $\{v_1, v_2, \ldots, v_N\}$ with the form of $|s, v_i\rangle + |s, v_j\rangle/\sqrt{2}$ $(i \neq j)$, the scale of $\{s'_i\}$ is $M = [N(N-1)]/2$, and there is

$$|\psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{i=1}^{M} |s_i'\rangle = \sqrt{\frac{N-1}{N}} \sum_{i=1}^{N} |s, v_i\rangle = \sqrt{N-1}\,|\psi\rangle .$$

With Eq. (10), we have

$$\begin{aligned} &(I - 2|s'_1\rangle\langle s'_1| - 2|s'_2\rangle\langle s'_2|)(U')^t |\psi\rangle \\ &= (I - 2|s''_1\rangle\langle s''_1|)(U')^t |\psi\rangle . \end{aligned} \tag{11}$$

Combining Eqs. (9) and (11), we obtain the following relationship:

$$\begin{aligned} &(I - 2|s, v_1\rangle\langle s, v_1| - 2|s, v_2\rangle\langle s, v_2| - 2|s, v_3\rangle \\ &\langle s, v_3| - 2|s, v_4\rangle\langle s, v_4|)(U')^t |\psi\rangle \\ &= (I - 2|s''_1\rangle\langle s''_1|)(U')^t |\psi\rangle , \end{aligned} \tag{12}$$

where

$$s''_1 = \frac{s'_1 + s'_2}{\sqrt{2}} = \frac{|s, v_1\rangle + |s, v_2\rangle + |s, v_3\rangle + |s, v_4\rangle}{2}.$$

Lemma 7 is proved.

Theorem 1 The abstract search algorithm searching for 2^m solutions $(2 < m < \log_2 N)$ is reduced to searching for $\tilde{s}_1$, where $\tilde{s}_1 = \sum_{i=1}^{2^m} |s, v_i\rangle \Big/ \sqrt{2^m}$.

Proof By induction, we proved the case of four solutions. If the inductive assumption case of 2^{m-1} solutions is true, then we have

$$\begin{aligned} &(I - 2\sum_{i=1}^{2^{m-1}} |s, v_i\rangle\langle s, v_i|)(U')^t |\psi\rangle \\ &= (I - 2|\bar{s}_1\rangle\langle \bar{s}_1|)(U')^t |\psi\rangle , \end{aligned} \tag{13}$$

where $\bar{s}_1 = \sum_{i=1}^{2^{m-1}} |s, v_i\rangle \Big/ \sqrt{2^{m-1}}$. Similarly, according to the derivation of Eq. (9) from Eqs. (7) and (8), we can obtain

$$\begin{aligned} &\left(I - 2\sum_{i=1}^{2^{m-1}} |s, v_i\rangle\langle s, v_i| - 2\sum_{i=2^{m-1}+1}^{2^m} |s, v_i\rangle\langle s, v_i|\right)(U')^t |\psi\rangle \\ &= (I - 2|\bar{s}_1\rangle\langle \bar{s}_1| - 2|\bar{s}_2\rangle\langle \bar{s}_2|)(U')^t |\psi\rangle , \end{aligned} \tag{14}$$

which shows that the abstract search algorithm searching for 2^m solutions is reduced to searching for $\bar{s}_1$ and $\bar{s}_2$.

On the other hand, the abstract search algorithm searching for two solutions $\bar{s}_1$ and $\bar{s}_2$ in space $\{\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_M\}$ is reduced to searching for $\tilde{s}_1 = (\bar{s}_1 + \bar{s}_2)/\sqrt{2}$ with the initial state

$$|\psi_1\rangle = \frac{1}{\sqrt{M}} \sum_{i=1}^{M} |\bar{s}_i\rangle,$$

thus

$$\begin{aligned} &(I - 2|\bar{s}_1\rangle\langle \bar{s}_1| - 2|\bar{s}_2\rangle\langle \bar{s}_2|)(U')^t |\psi_1\rangle \\ &= (I - 2|\tilde{s}_1\rangle\langle \tilde{s}_1|)(U')^t |\psi_1\rangle . \end{aligned} \tag{15}$$

When $|\bar{s}_i\rangle$ is composed of elements in $\{v_1, v_2, \ldots, v_N\}$ with the form of $\sum_{i=1}^{2^{m-1}} |s, v_i\rangle \Big/ \sqrt{2^{m-1}}$, the scale of $\{\bar{s}_i\}$ is $M = C_N^{2^{m-1}}$, and there is

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{M}} \sum_{i=1}^{M} |\bar{s}_i\rangle = \frac{1}{\sqrt{C_N^{2^{m-1}}}} \frac{C_N^{2^{m-1}} 2^{m-1}}{N} \frac{\sum_{i=1}^{N} |s, v_i\rangle}{\sqrt{2^{m-1}}} \\ &= \sqrt{C_{N-1}^{2^{m-1}-1}}\,|\psi\rangle . \end{aligned}$$

With Eq. (15), we have

$$\begin{aligned} &(I - 2|\bar{s}_1\rangle\langle \bar{s}_1| - 2|\bar{s}_2\rangle\langle \bar{s}_2|)(U')^t |\psi\rangle \\ &= (I - 2|\tilde{s}_1\rangle\langle \tilde{s}_1|)(U')^t |\psi\rangle . \end{aligned} \tag{16}$$

Combining Eqs. (14) and (16), we obtain

$$\begin{aligned} &(I - 2\sum_{i=1}^{2^m} |s, v_i\rangle\langle s, v_i|)(U')^t |\psi\rangle \\ &= (I - 2|\tilde{s}_1\rangle\langle \tilde{s}_1|)(U')^t |\psi\rangle , \end{aligned} \tag{17}$$

where $\tilde{s}_1 = \sum_{i=1}^{2^m} |s, v_i\rangle \Big/ \sqrt{2^m}$. Theorem 1 is hence proved.

In this subsection, we generalize the abstract search algorithm to the case of multi-solution. Based on the above conclusion, we can use the abstract search algorithm to analyze the quantum random-walk search on the various graphs directly.

3.2. Computational complexity of the algorithm

The relation between the optimized SKW algorithm and the SKW algorithm was given in Ref. [27]. Therefore, we only need to research the computational complexity of the SKW algorithm with multi-solution. The proof for one solution case is presented in Section 8 of Ref. [29]. The operation of the SKW algorithm can be written as $U' = U(I - 2|s, x_{\rm tg}\rangle\langle s, x_{\rm tg}|)$ by the previous conclusion. We assume 2^m solutions with $2 < m < \log_2 N$. According to the Theorem 5 in Ref. [29], we only need to replace $|x_{\rm tg}\rangle$ by $\sum_{i=1}^{2^m} |x_{\rm tg}^{(i)}\rangle \Big/ \sqrt{2^m}$ in the process of proof, and then we will use the method presented in Theorem

1 of Ref. [29] to obtain the computational complexity of the SKW algorithm with multi-solution.

The eigenvalues and eigenvectors of U are already given in Ref. [31]. The quantum walk of the SKW algorithm stays in an 2^n-dimensional subspace spanned by 2^n eigenvectors $|v_k^{\pm}\rangle$ of U with eigenvalues $e^{i\theta_k}$, where $\cos\theta_k = 1-2k/n$ for $k=0,\ldots,n$, each with degeneracy $\binom{n}{k}$.[29] When $k=0$, $|v_0^{\pm}\rangle = |v_0\rangle = |\psi\rangle$ is the initial state which is the only eigenvector of eigenvalue 1. Let H_0' be the space spanned by $|v_k^{\pm}\rangle$. According to Section 8 in Ref. [29], $|s,\boldsymbol{x}_{\rm tg}\rangle$ is also in H_0'.

Theorem 2 $U'(H_0') = H_0'$. Furthermore, U' has no eigenvector of eigenvalue 1 in H_0'.

Proof For the first part, because $U' = U(I - 2|s,\boldsymbol{x}_{\rm tg}\rangle\langle s,\boldsymbol{x}_{\rm tg}|)$, we only show $U(H_0') = H_0'$ and $(I - 2|s,\boldsymbol{x}_{\rm tg}\rangle\langle s,\boldsymbol{x}_{\rm tg}|)(H_0') = H_0'$ with $|\boldsymbol{x}_{\rm tg}\rangle = \sum_{i=1}^{2^m}|\boldsymbol{x}_{\rm tg}^{(i)}\rangle/\sqrt{2^m}$. The first equality is true because H_0' is spanned by eigenvectors of U. Therefore, $U(H_0') = H_0'$. Assuming $|\varphi\rangle \in H_0'$, we have $(I - 2|s,\boldsymbol{x}_{\rm tg}\rangle\langle s,\boldsymbol{x}_{\rm tg}|)(|\varphi\rangle) = |\varphi\rangle - 2\langle s,\boldsymbol{x}_{\rm tg}|\varphi\rangle|s,\boldsymbol{x}_{\rm tg}\rangle$. This is a linear combination of $|\varphi\rangle$ and $|s,\boldsymbol{x}_{\rm tg}\rangle$. Because $|s,\boldsymbol{x}_{\rm tg}\rangle \in H_0'$, $(I - 2|s,\boldsymbol{x}_{\rm tg}\rangle\langle s,\boldsymbol{x}_{\rm tg}|)(|\varphi\rangle) \in H_0'$. Similarly, if $|s,\boldsymbol{x}_{\rm tg}\rangle$ is replaced by $\sum_{i=1}^{2^m}|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle/\sqrt{2^m}$, it is a linear combination of $|\varphi\rangle$ and $|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle$. Therefore, $U'(H_0') = H_0'$.

For the second part, assume $|\omega_0\rangle$ is an eigenvector of eigenvalue 1 of U' in H_0', and then

$$\begin{aligned} &0 \neq \langle\psi|\omega_0\rangle \\ &= \langle\psi|U'|\omega_0\rangle = \langle\psi|U(I-2|s,\boldsymbol{x}_{\rm tg}\rangle\langle s,\boldsymbol{x}_{\rm tg}|)|\omega_0\rangle \\ &= \langle\psi|\omega_0\rangle - 2\frac{\sum_{i,j=1}^{2^m}\langle\psi|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle\langle s,\boldsymbol{x}_{\rm tg}^{(j)}|\omega_0\rangle}{2^m}. \end{aligned} \tag{18}$$

This implies $\sum_{i,j=1}^{2^m}\langle\psi|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle\langle s,\boldsymbol{x}_{\rm tg}^{(j)}|\omega_0\rangle = 0$. Because $\langle\psi|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle = 1/\sqrt{N} \neq 0$, we obtain $\sum_{j=1}^{2^m}\langle s,\boldsymbol{x}_{\rm tg}^{(j)}|\omega_0\rangle = 0$,

$$\begin{aligned} |\omega_0\rangle &= U'|\omega_0\rangle \\ &= U|\omega_0\rangle - 2\frac{\sum_{i,j=1}^{2^m}|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle\langle s,\boldsymbol{x}_{\rm tg}^{(j)}|\omega_0\rangle}{2^m} = U|\omega_0\rangle, \end{aligned}$$

which in turn implies that $|\omega_0\rangle$ is an eigenvector of eigenvalue 1 of U. Because $\sum_{j=1}^{2^m}\langle s,\boldsymbol{x}_{\rm tg}^{(j)}|\omega_0\rangle = 0$ and $\langle\psi|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle \neq 0$, if the eigenvector of eigenvalue 1 of U is orthogonal to $|\psi\rangle$, it is orthogonal to $\sum_{i=1}^{2^m}|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle$. It follows that $\langle\psi|\omega_0\rangle = 0$ which contradicts that $|\omega_0\rangle \in H_0'$.

Theorem 2 shows that the SKW algorithm with multi-solution starting in $|\psi\rangle$ is restricted to a subspace H_0' of the Hilbert space. Since $|\psi\rangle$ is the only 1-eigenvector of U in H_0', we can regard the SKW algorithm with multi-solution as an instance of the abstract search algorithm on the space H_0', with $U_1 = (I - 2|\psi_{\rm good}\rangle\langle\psi_{\rm good}|)$, $U_2 = U$, $|\psi_{\rm start}\rangle = |\psi\rangle$, and $|\psi_{\rm good}\rangle = \sum_{i=1}^{2^m}|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle/\sqrt{2^m}$.

Then, according to Lemma 3, we evaluate

$$\alpha = O\left[\left(\sqrt{\sum_k \frac{a_k^2}{a_0^2}\frac{1}{1-\cos\theta_k}}\right)^{-1/2}\right],$$

which determines the computational complexity of the algorithm. Assuming $|s,\boldsymbol{x}_{\rm tg}\rangle = a_0|\psi\rangle + \sum_k a_k(|v_k^-\rangle + |v_k^+\rangle)$ when there is only one solution. Thus we have $a_0 = \langle\psi|s,\boldsymbol{x}_{\rm tg}\rangle = 1/\sqrt{N}$ and $a_k = \langle v_k^+|s,\boldsymbol{x}_{\rm tg}\rangle = 1/\sqrt{2N}$ according to Ref. [31]. Therefore, when $|s,\boldsymbol{x}_{\rm tg}\rangle$ is replaced by $\sum_{i=1}^{2^m}|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle/\sqrt{2^m}$, we have

$$a_0' = \frac{\sum_{i=1}^{2^m}\langle\psi|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle}{\sqrt{2^m}}, \quad a_k' = \frac{\sum_{i=1}^{2^m}\langle v_k^+|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle}{\sqrt{2^m}}.$$

Because $\langle\psi|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle = \langle\psi|s,\boldsymbol{x}_{\rm tg}\rangle$ and $\langle v_k^+|s,\boldsymbol{x}_{\rm tg}^{(i)}\rangle = \langle v_k^+|s,\boldsymbol{x}_{\rm tg}\rangle$, we obtain

$$a_0' = \sqrt{\frac{2^m}{N}}, \quad a_k' = \sqrt{\frac{2^{m-1}}{N}}, \quad \frac{a_k}{a_0} = \frac{a_k'}{a_0'}.$$

Therefore, we only need to evaluate

$$\sum_{k=1}^{n}\binom{n}{k}\frac{1}{1-\cos\theta_k} = O(N),$$

which is the same as that in Section 8 of Ref. [29]. Therefore, $\alpha = O(1/\sqrt{N})$ and the computational complexity of the algorithm is $T = O(\sqrt{N})$.

Let $|w_\alpha\rangle$ and $|w_{-\alpha}\rangle$ be the two eigenvectors with eigenvalues $e^{i\alpha}$ and $e^{-i\alpha}$, respectively, and define $|w_{\rm start}\rangle = [|w_\alpha\rangle - |w_{-\alpha}\rangle]/\sqrt{2}$. According to Lemma 4, $\langle\psi|w_{\rm start}\rangle$ is determined by α, a_k^2/a_0^2, $1/(1-\cos\theta_k)$. The previous evaluations show that their values are the same as the case of one solution. Therefore, $\langle\psi|w_{\rm start}\rangle$ is also the same as that when there is one solution, and the starting state $|\psi\rangle$ is close to $|w_{\rm start}\rangle$.

Finally, we show that measuring the final state $|w_{\rm good}\rangle = [|w_\alpha\rangle + |w_{-\alpha}\rangle]/\sqrt{2}$ can obtain the target with constant probability. For one solution case, there are

$$\frac{1}{\sqrt{\sum_k a_k^2\cot^2\frac{\theta_k}{4}}} \geq \frac{1}{\sqrt{\frac{1}{2N}\sum_k\frac{4}{\theta_k^2}}},$$

$$\sum_k\frac{1}{\theta_k^2} = O\left(\sum_k\frac{1}{1-\cos\theta_k}\right),$$

according to Claim 10 in Ref. [29]. Furthermore,

$$O\left(\sum_k\frac{1}{1-\cos\theta_k}\right) = O(N),$$

according to Section 8 in Ref. [29], and $\langle s,\boldsymbol{x}_{\rm tg}|w_{\rm good}\rangle = 1\Big/\sqrt{\sum_k a_k^2\cot^2(\theta_k/4)} = O(1)$ according to Lemma 5.

Because $a_k'^2 = 2^m a_k^2$, we have $\langle \psi_{\text{good}} | w_{\text{good}} \rangle = 1 \Big/ \sqrt{\sum_k a_k'^2 \cot^2(\theta_k/4)} = O(1/\sqrt{2^m})$ for the multi-solution case. Therefore, we can obtain the target with constant probability as long as m is a constant.

Through the above proofs, we obtain the computational complexity of the SKW algorithm with multi-solution. According to Ref. [27], the computational complexity of the optimized SKW algorithm with multi-solution is also $O(\sqrt{N})$.

4. Numerical simulations and results

Through the abstract search algorithm, we can only obtain the computational complexity of the algorithm with multi-solution, but it does not involve the number of iterations. Therefore, we will further research the relationship between the success of the algorithm, the number of iterations, and the proportion of solutions by numerical simulations.

According to the conclusion of Subsection 3.2, if the proportion of solutions is small, the target will be obtained with a constant probability. Therefore, we first study the relationship between the success rate of the algorithm and the number of iterations with a small proportion of solutions. Figure 1 shows the relationship between the success rate of the algorithm and the number of iterations when the database size is $N = 2^8$. The proportions of solutions $q = M/N$ are $1/256$, $2/256$, $3/256$ respectively.

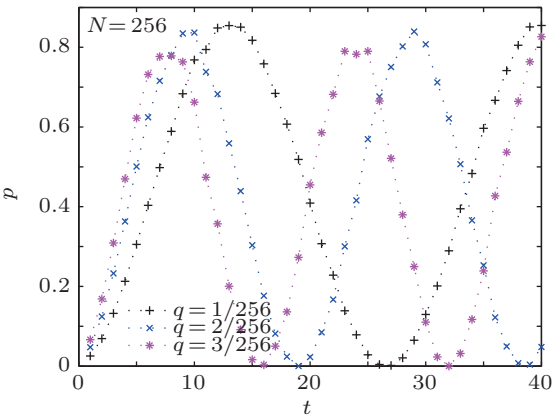


Fig. 1. (color online) Relationship between the success rate of the algorithm and the number of iterations for $N = 2^8$. The different lines show results for different values of q.

It is known from Fig. 1 that the success rate of the algorithm changes periodically along with the number of iterations, and their relationship satisfies a trigonometric function approximately. If q is larger, the maximum success rate is smaller. This is consistent with the theoretical analysis. For one solution, the expression relating the success rate of the algorithm p and the number of iterations t is

$$p = \frac{1}{c^2} \sin^2\left(\frac{2}{\sqrt{2^n}} t\right),$$

where c is determined by n, and $1/c^2$ increases toward 1 with the increase of n. For multi-solution, considering the success rate of the algorithm p is equivalent to the proportion of solutions q when $t = 0$, we assume that the relationship satisfies

$$p = \frac{q}{\sin^2 a} \sin^2(\omega t + a). \tag{19}$$

By using curve fitting, ω and a are obtained. With n increasing, $\omega \to 2\sqrt{q}$ and $a \to 1.2\sqrt{q}$. Therefore, when $\omega t + a = \pi/2$, $t = [\pi\sqrt{N/M}]/4 - 0.6$.

Then, we study the relationship between the success rate of the algorithm and the number of iterations when q is big enough.

Figure 2 shows the success rate of the algorithm and the number of iterations for different databases with $q = 1/2$. Their relationship is no longer satisfying the previous function. Before the search, the success rate of the algorithm is $1/2$ which is equivalent to the proportion of solutions q, and then it changes sharply along with the number of iterations. In practice, if $q \geq 1/2$, we can directly obtain the target with a considerable probability without iterating the algorithm.

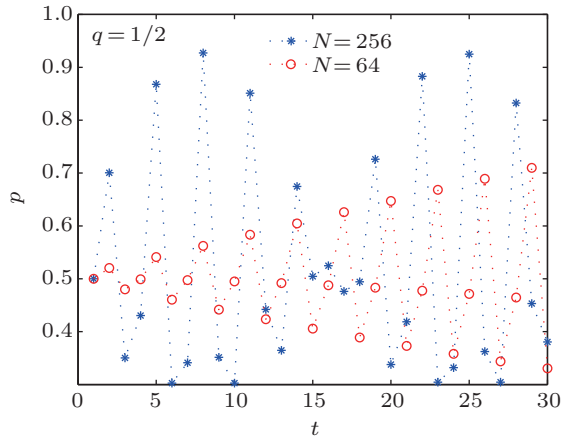


Fig. 2. (color online) Relationship between the success rate of the algorithm and the number of iterations when $q = 0.5$. The circles line represents $N = 64$ and the asterisks line represents $N = 256$.

We obtain an approximate critical value of q by numerical simulations. Only if $q \leq 5/64$, the success rate of the algorithm can reduce to 0 every time, as shown in Figs. 3 and 4. Therefore, we assume that the relationship curve still satisfies the form of Eq. (19).

Finally, we study the relationship between the success rate of the algorithm and the proportion of solutions according to Eq. (19), as shown in Fig. 5. The solid line indicates the relationship for the optimized SKW algorithm when the number of iterations $t = [\pi\sqrt{N/M}]/4 - 0.6$ with the scale of database n being large enough and $q \leq 5/64$. The dotted line indicates the relationship for Grover's algorithm. Because the success rate of the optimized SKW algorithm tends to 1 but not equal to 1, for the same proportion of solutions, the corresponding success rate is a little smaller than that of Grover's algorithm.

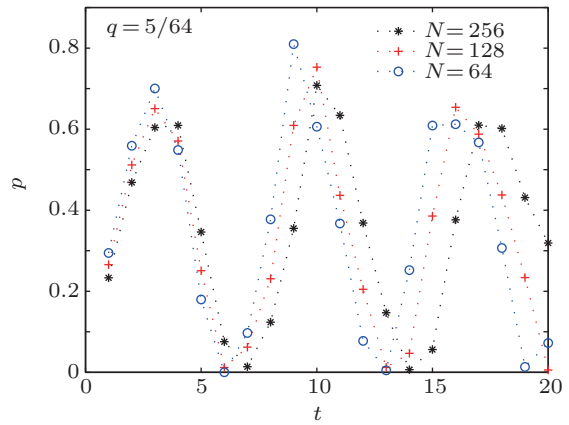


Fig. 3. (color online) Relationship between the success rate of the algorithm and the number of iterations when $q = 5/64$. The different lines show results for different values of N.

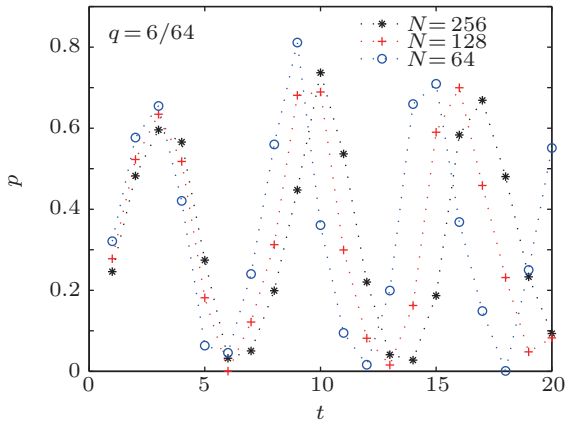


Fig. 4. (color online) Relationship between the success rate of the algorithm and the number of iterations when $q = 6/64$. The different lines show results for different values of N.

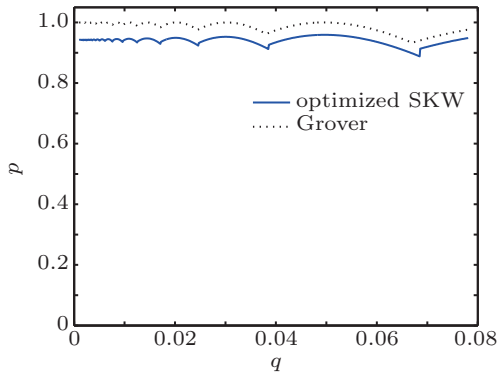


Fig. 5. (color online) Relationship between the success rate of the algorithm and the proportion of solutions for different algorithms.

In this section, we simulate the relationship between the success rate of the optimized SKW algorithm and the number of iterations. We obtain a critical valve of the proportion of solutions. When $q \leq 5/64$, the success rate of the algorithm, the number of iterations, and the proportion of solutions satisfy a quantitative relationship approximatively. When $q > 5/64$, the computational complexity of algorithm is still $O(\sqrt{N})$, but the success rate of the algorithm is no longer periodically changing along with iterations.

5. Conclusion

This paper investigates the multi-solution search of the optimized SKW algorithm. For the problem that the geometric description method cannot be applied to the multi-solution case directly, we first give the generalization of the abstract search algorithm for the multi-solution case. Then, we demonstrate that the computational complexity of the optimized SKW algorithm with multi-solution is $O(\sqrt{N})$. For the small proportion of solutions q, we find that the success rate of the algorithm and the required number of iterations will decrease with the increase of q. Finally, a critical value of q is obtained. When $q \leq 5/64$, the relationship between the success rate, the number of iterations, and the proportion of solutions satisfies a function as

$$p = \frac{q}{\sin^2 1.2\sqrt{q}} \sin^2(2\sqrt{q}t + 1.2\sqrt{q}).$$

When $q > 5/64$, the success rate is no longer periodically changing along with iterations, and the computational complexity of the algorithm is $O(\sqrt{N})$.

References

[1] Feynman R 1982 *Int. J. Theor. Phys.* **21** 467
[2] Deutsch D 1985 *Proeeeding of the Royal Soeiety of London A: Mathematical, Physical and Engineering Sciences* **400** 97
[3] Shor P W 1997 *SIAM J. Comput.* **26** 1484
[4] Grover L K 1996 *Proceeding of the* 28*th ACM Symposium on Theory of Computation* (New York: ACM Press) pp. 212–219
[5] Kane B E 1998 *Nature* **393** 133
[6] Zhang Y Y, Hu H P and Lu S F 2011 *Chin. Phys. B* **20** 040309
[7] Fu X Q, Bao W S, Li F D and Zhang Y C 2014 *Chin. Phys. B* **23** 020306
[8] Long G L 2001 *Phys. Rev. A* **64** 022307
[9] Toyama F M, van Dijk W and Nogami Y 2013 *Quantum Inf. Process.* **12** 1897
[10] Wang X, Bao W S and Fu X Q 2011 *Chin. Sci. Bull.* **56** 484
[11] Long G L, Li Y S, Zhang W L and Niu L 1999 *Phys. Lett. A* **262** 27
[12] Long G L, Xiao L and Sun Y 2002 *Phys. Lett. A* **294** 143
[13] Li T, Bao W S, Lin W Q and Fu X Q 2014 *Chin. Phys. Lett.* **31** 050301
[14] Long G L and Liu Y 2007 *Front. Comput. Sci. China* **1** 247
[15] Liu Y 2013 *Chin. Sci. Bull.* **58** 2927
[16] Liu Y and Ou-Yang X P 2013 *Chin. Sci. Bull.* **58** 2329
[17] Ampadu C 2014 *Chin. Phys. B* **23** 030302
[18] Xue P, Qin H, Tang B, Zhan X, Bian Z H and Li J 2014 *Chin. Phys. B* **23** 110307
[19] Wu J J, Zhang B D, Tang Y H, Qiang X G and Wang H Q 2013 *Chin. Phys. B* **22** 050304
[20] Ambainis A 2007 *SIAM J. Comput.* **37** 210
[21] Tulsi A 2008 *Phys. Rev. A* **78** 012310
[22] Magniez F, Nayak A, Roland J and Santha M 2011 *SIAM J. Comput.* **40** 142
[23] Shenvi N, Kempe J and Whaley K B 2003 *Phys. Rev. A* **67** 052307
[24] Travaglione B C and Milburn G J 2002 *Phys. Rev. A* **65** 032310
[25] Dür W, Raussendorf R, Kendon V M and Briegel H J 2002 *Phys. Rev. A* **66** 052319
[26] Li Y 2006 *Investigations on Quantum Random-Walk Search Algorithm* (Dissertation) (Shanghai: East China Normal University) (in Chinese)
[27] Potocek V, Gábris A, Kiss T and Jex I 2009 *Phys. Rev. A* **79** 012325
[28] Zhang Y C, Bao W S, Wang X and Fu X Q 2015 *Chin. Phys. B* **24** 060304
[29] Ambainis A, Kempe J and Rivosh A 2005 *Proceedings of the* 16*th Annual ACM-SIAM Symposium on Discrete Algorithms*, Society for Industrial and Applied Mathematics, pp. 1099–1108
[30] Szegedy M 2004 arXiv: quant-ph/0401053
[31] Moore C and Russell A 2002 *Randomization and Approximation Techniques in Computer Science* (Berlin, Heidelberg: Springer) pp. 164–178