Post-processing can speed up general quantum search algorithms

Avatar Tulsi
Department of Physics, IIT Bombay, Mumbai-400076, India

A general quantum search algorithm aims to evolve a quantum system from a known source state $|s\rangle$ to an unknown target state $|t\rangle$. For this, it needs multiple applications of the selective phase inversion of the target state as well as a diffusion operator having source state as one of its eigenstates. The famous Grover’s algorithm is a special case of general algorithm where the diffusion operator is a selective phase inversion of the source state. The general algorithm evolves the source state to a particular state $|w\rangle$, call it w-state, in $O(B/\alpha)$ time steps where $\alpha = |\langle t|s\rangle|$ and $B$ is a characteristic of the diffusion operator. Measuring w-state gives the target state with a success probability of $O(1/B^2)$ and $O(B^2)$ runnings of algorithm can boost this success probability from $O(1/B^2)$ to $O(1)$, making the total time complexity $O(B^3/\alpha)$. A more efficient way to boost the success probability is quantum amplitude amplification but that requires efficient implementation of $I_w$, the selective phase-inversion of w-state, which is not known so far. Here, we present an efficient implementation of $I_w$ and we show that $O(1)$ runnings of general algorithm are sufficient to get the target state, reducing the time complexity to $O(B/\alpha)$. Though $O(B/\alpha)$ algorithms are known to exist, but our alternative algorithm offers implementation advantages. As a special case, we present an alternative $O(\sqrt{N} \log N)$ algorithm for two-dimensional spatial search based on quantum post-processing.

PACS numbers: 03.67.Ac

I. INTRODUCTION

Grover’s algorithm or more generally quantum amplitude amplification drives a quantum computer from a source state $|s\rangle$ to a target state $|t\rangle$, say the target state by using selective phase inversion operators, $I_s$ and $I_t$, of these two states $|s\rangle$ and $|t\rangle$. The algorithm is an $O(1/\alpha)$ times iteration of the operator $G = I_s I_t$ on $|s\rangle$ to get $|t\rangle$ where $\alpha = |\langle t|s\rangle|$. For search problem, we choose $|s\rangle$ to be the uniform superposition of all $N$ basis states to be searched i.e. $|s\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle$. In case of a unique solution, the target state $|t\rangle$ is a unique basis state and $\alpha = |\langle t|s\rangle| = 1/\sqrt{N}$. Thus Grover’s algorithm outputs a solution in just $O(\sqrt{N})$ time steps which is quadratically faster than classical search algorithms taking $O(N)$ time steps. Grover’s algorithm is proved to be strictly optimal [3].

A general framework of quantum search algorithms was presented in [4]. The general quantum search algorithm replaces $I_s$ by a more general diffusion operator $D_s$ with the only restriction of having $|s\rangle$ as one of its eigenstates. This restriction seems to be more or less justified as the diffusion operator should have some special connection with the source state. Let the normalized eigenspectrum of $D_s$ be given by $D_s |\ell\rangle = e^{i \theta _\ell} |\ell\rangle$ with $|\ell\rangle$ as the eigenstates and $e^{i \theta _\ell}$ as the corresponding eigenvalues (eigenphases). Since a global phase is irrelevant in quantum dynamics, we choose $D_s |s\rangle = |s\rangle$, i.e. $\theta _{s-s} = 0$. The general search operator is $S = D_s I_t$ and its iteration on $|s\rangle$ can be analyzed by finding its eigenspectrum. Such an analysis was done in [4] and we found that the performance of general algorithm depends upon two quantities $\Lambda_1$ and $\Lambda_2$, where

$$\Lambda_p = \sum_{\ell \neq s} |\langle \ell|t\rangle|^2 \cot p \frac{\theta _\ell}{2}$$

(1)

is the $p^{th}$ moment of $\cot \frac{\theta _\ell}{2}$ with respect to the distribution $|\langle \ell|t\rangle|^2$ over all $\ell \neq s$. For a successful quantum search, we found $\Lambda_1 \approx 0$ to be an essential condition. An algorithm was also presented in Section IV.A of [2] which uses an ancilla qubit to cleverly control the applications of $D_s$ and $D_s^\dagger$ to effectively make $\Lambda_1$ zero. In this paper, we restrict ourselves to the case $\Lambda_1 = 0$. In case, it is not so, we can always use just-mentioned algorithm to make it so.

Unlike Grover’s algorithm, the general algorithm does not rotate the quantum state in a plane spanned by $|s\rangle$ and $|t\rangle$. Rather, it induces rotation in a different plane spanned by $|s\rangle$ and a particular state $|w\rangle$, which we also refer as w-state here. The rotation angle is $2\alpha/B$ and w-state has an overlap of $O(1/B)$ with the desired final state $|t\rangle$. Thus, we get w-state after one round of algorithm which takes $O(B/\alpha)$ time steps and we perform $O(B^2)$ rounds to get $|t\rangle$ with high probability. That makes the total time complexity to be $O(B/\alpha) \times O(B^3) = O(B^3/\alpha)$.

We know that performing $O(B^2)$ rounds of algorithm to boost the success probability from $O(1/B^2)$ to $O(1)$ is a classical process. Quantum mechanically, it can be done more efficiently using quantum amplitude amplification (QAA). But to drive $|w\rangle$ towards $|t\rangle$, we need to implement $I_w$, the selective phase-inversion of w-state, which is not so easy. By definition $I_w = S^q |s\rangle$ for some $q$ so $I_w = S^q I_s S^{-q}$. So we can implement $I_w$ if we can implement $I_s$ but the whole purpose of studying general quantum search algorithm was to discuss the cases when
$I_s$ is not efficiently implementable. Rather, what is available to us is a general diffusion operator $D_s$ of which $I_s$ is just a special case. We point out that $I_s$ is not easily implementable in cases of physical interest [5,9].

Thus, we are in some sense forced to use the classical process of running $O(B^2)$ rounds of search algorithm to get the target state. However, in this paper, we show that $I_w$ is not at all hard to implement and $O(1)$ rounds of search algorithm and hence $O(B/\alpha)$ time steps are enough to get the target state. We use quantum fourier transform to implement $I_w$. We point out that $O(B/\alpha)$ algorithms are known to exist [5,10] but our alternative approach offers implementation advantages as in general, it uses significantly lesser number of controlled transformations which are physically harder to implement. In next section, we present the algorithm. We conclude in Section III.

II. ALGORITHM

First, we briefly review the general quantum search algorithm [3]. It iterates the operator $D_s I_s^p$ on $|s\rangle$. Here $D_s$ is as defined earlier and $I_s^p$ is the selective phase rotation of target state by angle of $\phi$. We choose $\phi = \pi$ so that $I_s^p$ is the selective phase inversion $I_t$ of the target state. We assume $|s\rangle$ to be a non-degenerate eigenstate for simplicity. The normalized eigenspectrum of $D_s$ is given by $D_s |\ell\rangle = e^{i\theta_\ell}|\ell\rangle$. By convention, $\theta_{t=s} = 0$. Let other eigenvalues satisfy

$$|\theta_{\ell\neq s}| \geq \theta_{\text{min}} > 0, \quad \theta_\ell \in [-\pi, \pi]$$

The iteration of $S = D_s I_s$ on $|s\rangle$ can be analysed by finding its eigenspectrum. The secular equation was found in [5] to be

$$\sum_\ell |\langle \ell | t \rangle|^2 \cot \frac{\lambda_\ell - \theta_\ell}{2} = 0.$$  (3)

Any eigenvalue $e^{i\lambda_\ell}$ of $S$ has to satisfy above equation.

Since $\cot x$ varies monotonically with $x$ except for the jump from $-\infty$ to $\infty$ when $x$ crosses zero, there is a unique solution $\lambda_\ell$ between each pair of consecutive $\theta_\ell$'s. Then with $\theta_{t=s} = 0$, there can be at most two solutions $\lambda_\ell$ in the interval $[-\theta_{\text{min}}, \theta_{\text{min}}]$. Only two eigenstates $|\lambda_\pm\rangle$ with the corresponding eigenvalues $e^{i\lambda_\pm}$ of $S$ are relevant. Under the assumption, $|\lambda_\pm| \ll \theta_{\text{min}}$, the initial state $|s\rangle$ is almost completely spanned by two eigenstates $|\lambda_\pm\rangle$. We point out that $\lambda_\pm$ are the only two solutions of eq. (3) in the interval $[-\theta_{\text{min}}, \theta_{\text{min}}]$. They are given by

$$\lambda_\pm = \pm \frac{2\alpha}{B} (\tan \eta)^{\pm 1}; \quad \cot 2\eta = \frac{\Lambda_1}{2\alpha B}.$$  (4)

where

$$B = \sqrt{1 + \Lambda_2}, \quad \Lambda_p = \sum_{\ell \neq s} |\langle \ell | t \rangle|^2 \cot^p \frac{\theta_\ell}{2}.$$  (5)

We consider the case when $\Lambda_1 = 0$. Then eq. (4) indicates that

$$\Lambda_1 = 0 \implies \eta = \frac{\pi}{4}, \quad \lambda_\pm = \pm \frac{2\alpha}{B}.$$  (6)

With $\eta = \pi/4$ and $\phi = \pi$, Eq. (23) and (24) of [3] gives us the initial state $|s\rangle$ and the effect of iterating $S$ on $|s\rangle$ in terms of two relevant eigenstates $|\lambda_\pm\rangle$. We have

$$|s\rangle = -i/\sqrt{2} [e^{i\lambda_+}/2 |\lambda_+\rangle - e^{i\lambda_-}/2 |\lambda_-\rangle],$$  (7)

and

$$S^t |s\rangle = -i/\sqrt{2} [e^{iq\lambda_+} |\lambda_+\rangle - e^{iq\lambda_-} |\lambda_-\rangle],$$  (8)

where $q' = q + \frac{\pi}{4}$.

For $q = q_m \approx \pi/2|\lambda_\pm| = \pi B/4\alpha$, the state $S^{q_m} |s\rangle$ is almost the w-state $|w\rangle$ given by

$$S^{q_m} |s\rangle = |w\rangle = 1/\sqrt{2} (|\lambda_+\rangle + |\lambda_-\rangle).$$  (9)

As shown in [3], we have $|\langle t | w \rangle| = 1/B$. More explicitly,

$$|\langle t | \lambda_\pm \rangle| = \frac{1}{\sqrt{2}B}.$$  (10)

If we can efficiently implement $I_w$ then $O(B)$ iterations of quantum amplitude amplification operator $A = I_w I_t$ on $|w\rangle$ will bring us close to the target state $|t\rangle$.

We make a simple but useful observation that for our purpose $I_w$ is equivalent to $I_{\lambda_\pm}$, the selective phase inversion of both states $|\lambda_\pm\rangle$. In place of iterating $A = I_w I_t$ on $|w\rangle$ let us consider what happens if we iterate $A' = I_{\lambda_\pm} I_t$ on $|w\rangle$. This is the case of multiple (two) source states $|\lambda_\pm\rangle$ and has been analysed well in literature (for example, see the discussion before eq. (1) of [5]). Upto a global phase, the operator $I_{\lambda_\pm}$ is a special case of the general diffusion operator having a 2-dimensional degenerate eigenspace with eigenvalue 1 and as eq. (1) of [3] suggests that a successful quantum amplitude amplification is obtained provided the initial state is chosen to be

$$\sum_{\pm} \sqrt{\lambda_{\pm}} |\langle \lambda_{\pm} | t \rangle|^2.$$  (11)

Using eq. (10), we find that above equation is nothing but w-state $|w\rangle$ which is available to us after performing one round of general quantum search algorithm. Thus $O(1/|\langle t | w \rangle|) = O(B)$ iterations of $I_{\lambda_\pm} I_t$ on $|w\rangle$ will bring us very close to the target state $|t\rangle$.

To implement $I_{\lambda_\pm}$, we use quantum fourier transform for phase estimation algorithm (PEA) to reliably distinguish the $|\lambda_\pm\rangle$ from other eigenstates of $S$ (see Chapter 5 of [11] for a detailed discussion on PEA). As pointed out after eq. (3), non-$\lambda_\pm$ eigenphases of $S$ are outside the interval $[-\theta_{\text{min}}, \theta_{\text{min}}]$. Hence we can use PEA to distinguish $|\lambda_\pm\rangle$ from other eigenstates of $S$. To estimate the eigenphases of a unitary operator $S$ to an accuracy of $\theta_{\text{min}}$, PEA uses $O(1/\theta_{\text{min}})$ applications of $S$. 


and $O(\log(1/\theta_{\min}))$ ancilla qubits. However, using phase estimation algorithm to implement a selective transformation on $|\lambda_{\pm}\rangle$ states is a slightly tricky issue. We refer our readers to the section II of [12] for a detailed discussion on approximating selective transformations using PEA. There, such an approximation was achieved to distinguish the ground state of Hamiltonian from excited states. For our algorithm, we know that $|\lambda_{\pm}| \leq \theta_{\min}$ and we can safely assume that $|\lambda_{\pm}| \leq \theta_{\min}/2$. Thus we know the limits of eigenvalues corresponding to $|\lambda_{\pm}\rangle$ states which need to be distinguished.

The discussion presented in [12] allows us to infer that a naive use of PEA will need $O(c/\theta_{\min})$ applications of $S$ and $O(\log(c/\theta_{\min}))$ ancilla qubits to approximate $I_{\lambda_{\pm}}$ to an accuracy of $O(1/\sqrt{\epsilon})$. For $c \gg 1$, this is a good approximation, but for our algorithm, we need $O(B)$ applications of $I_{\lambda_{\pm}}$ and hence $c$ has to be $O(1/B^2)$ for an approximation sufficient for the success of our algorithm. In [12], we had presented a more efficient way to improve the approximation using the well-known concept of majority voting. It was shown there that as long as $c \geq 1$, using $O(\mu c/\theta_{\min})$ applications of $S$ and $O(\mu + c/\theta_{\min})$ ancilla qubits, we can approximate $I_{\lambda_{\pm}}$ to an accuracy of $e^{-O(\mu)}$. By choosing $\mu = O(\log B)$, we get an approximation sufficient for the success of our algorithm. As we need $O(B)$ applications of $I_{\lambda_{\pm}}$, the total number of applications of $S$ required by post-processing part of our algorithm is $O\left(\frac{B}{\theta_{\min}} \log B \right)$. We add $O(B/\alpha)$ applications of $S$ to get the w-state $|w\rangle$ to above equation to get the total time complexity of our algorithm as

$$O\left(\frac{B}{\alpha} + \frac{B \log B}{\theta_{\min}}\right).$$ (12)

III. DISCUSSION AND CONCLUSION

Our algorithm is not the first $O(B/\alpha)$ algorithm for general quantum searching but it offers implementation advantages over the earlier algorithms. To understand it, we consider the controlled quantum search algorithm presented in [3], having a time complexity of $O(B/\alpha)$. But that algorithm succeeds by using $O(B/\alpha)$ controlled applications of the operators $D_s$ and $I_1$. Similarly, recently a different $O(B/\alpha)$ algorithm was presented in [13] but that also uses $O(B/\alpha)$ controlled applications of $D_s$ to implement phase estimation algorithm as well as $O(1/\alpha)$ controlled applications of $I_1$. In comparison to these two algorithm, the alternative presented here uses only $O(B \log B/\theta_{\min})$ controlled applications of $S = D_s I_1$. These controlled applications are required for the Phase Estimation algorithm. For the typical cases, $\theta_{\min}/\log B \gg \alpha$ and hence the present algorithm uses significantly lesser number of controlled operations compared to earlier algorithms. As controlled operations are harder to implement physically, our algorithm offers implementation advantages.

For the example of two-dimensional spatial search $\alpha = \theta_{\min} = 1/\sqrt{N}$ and $B = O(\log N)$ and hence our algorithm is just another alternative algorithm with a slightly increased time complexity by a factor of $O(\log \log N)$. We point out that Ambainis et.al. presented an $O(\sqrt{N \log N})$ algorithm for two-dimensional spatial search based on classical post-processing [14]. Basically they had shown that in case of $2d$ spatial search, w-state $|w\rangle$ is such that with high probability, measuring it gives a basis state $|w'\rangle$ within the distance of $O(N^{1/4} \times N^{1/4})$ local steps from the target state $|t\rangle$. Hence, $|t\rangle$ can be found by classically searching a $O(N^{1/4} \times N^{1/4})$ lattice centred at $|w'\rangle$ which takes $O(N)$ time steps. Our algorithm offers an alternative based on quantum post-processing and may be more suitable if two-dimensional spatial search is used as a quantum subroutine for other algorithms.

However, we point out that our algorithm mainly offers advantages only for general quantum search algorithms where $\theta_{\min}/\log B \gg \alpha$. We believe that our algorithm can find important applications in search problems.

[1] L.K. Grover, Phys. Rev. Lett. 79, 325 (1997).
[2] L.K. Grover, Phys. Rev. Lett. 80, 4329 (1998).
[3] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, Contemporary Mathematics (American Mathematical Society, Providence), 305, 53 (2002) [arXiv.org:quant-ph/0005055].
[4] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Computing 26, 1510 (1997) [arXiv.org:quant-ph/9701001].
[5] A. Tulsi, Phys. Rev. A 86, 042331 (2012).
[6] A. Ambainis, J. Kempe, and A. Rivosh, Proc. 16th ACM-SIAM SODA, p. 1099 (2005) [arXiv.org:quant-ph/0402107].
[7] G. Kato, Phys. Rev. A 72, 032319 (2005).
[8] N. Shenvi, J. Kempe, and K. B. Whaley, Phys. Rev. A 67, 052307 (2003).
[9] A. Ambainis, SIAM J. Computing, 37, 210 (2007) [arXiv.org:quant-ph/0311001].
[10] A. Tulsi, Phys. Rev. A 78, 012310 (2008).
[11] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, England, 2000).
[12] A. Tulsi, arxiv.org:1210.4647
[13] A. Tulsi, arxiv.org:1503.05712, Accepted for publication in PRA.
[14] Ambainis et. al., arxiv.org:1112.3337, Theory of Quantum Computation, Communication, and Cryptography, 7th conference, TQC 2012, Tokyo, LNCS 7582, Springer.