Quantum Information Processing, Vol. 6, No. 1, February 2007 (© 2006)
DOI: 10.1007/s11128-006-0037-y

Sure Success Partial Search

Byung-Soo Choi,[1,2] Thomas A. Walker,[1] and Samuel L. Braunstein[1]

Received March 16, 2006; accepted June 12, 2006; Published online November 28, 2006

Partial search has been proposed recently for finding the target block containing a target element with fewer queries than the full Grover search algorithm which can locate the target precisely. Since such partial searches will likely be used as subroutines for larger algorithms their success rate is important. We propose a partial search algorithm which achieves success with unit probability.

KEY WORDS: Quantum database search; Grover's algorithm; partial search; sure success.

PACS: 03.67.Lx; 03.67.-a.

1. INTRODUCTION

In 1985 Deutsch designed a quantum algorithm which evaluates whether the two outputs of a Boolean function are the same or not using only one function evaluation.(1) Deutsch and Jozsa generalized this algorithm for a more general case such as whether a given Boolean function is constant or balanced. This algorithm demonstrated an exponential speed-up on a quantum machine compared to the best performance on classical machines.(2) The most important contribution in this field was achieved when Shor discovered a polynomial-time quantum algorithm for factoring and computing discrete logarithms—yielding an exponentially faster algorithm than the best known classical ones.(3) After this breakthrough many researchers started to find various applications, especially in cryptanalysis. On the other hand, Grover discovered the quantum (virtual) database search algorithm which yields a quadratic speed-up compared to classical database searches.(4) Since the database search algorithm is one of

[1]Department of Computer Science, University of York, York, Y010 5DD, UK.
[2]To whom correspondence to be addressed. E-mail: bschoi3@gmail.com

the most widely used algorithms in computer applications, the scientific impact is huge and many researchers have been interested in various applications of the quantum database search algorithm. The work presented here is concerned with a variation of the Grover search algorithm.

Recently, several researchers have investigated a partial search where instead of seeking the exact location of a unique target solution, they are interested in finding in which 'target block' the solution sits.[5,6] Indeed, because only a partial search is being performed an improvement in speed over the full search is expected. Indeed, recently proposed algorithms achieve meaningful performance improvements over full search.[(7)]

Meanwhile, until now these works have considered only optimizing the performance at the expense of finding the target block with unit probability. One might hope that partial search could become an important component or subroutine of larger quantum algorithms if a sure success (unit probability) formulation could be found. The idea would be to perform the search on successively smaller block sizes with each partial search successively revealing more information about the location of the target. Indeed, in Ref. 6 the idea for a sure success partial search has been mentioned. In order to achieve this goal we utilized the scheme for partial search as described in Ref. 8 which reduces the problem to one essentially involving rotations in a three-dimensional Hilbert space. In this way, we find that a simple modification, involving introducing additional phases in the final step, allows us to construct a sure success partial search algorithm.

This paper is organized as follows. First, we review an optimal version of the partial search algorithm, known as the GRK algorithm.[(7)] Second, we propose a modification to the phases for the final step to guarantee sure success of the partial search algorithm. We derive a phase condition that must be satisfied for this modification to yield sure success and finally we show numerically that this condition may easily be solved. We conclude with a consideration of other problems that might be extensions suitable for further study.

2. GRK PARTIAL SEARCH ALGORITHM

The GRK partial search algorithm[(7)] is defined by the sequence of unitary operations

$$G_{\mathrm{g}} G_{\mathrm{l}}^{j_{\mathrm{l}}} G_{\mathrm{g}}^{j_{\mathrm{g}}}, \tag{1}$$

where G_{g} is a 'global' Grover operator which acts on the entire search space of size N and G_{l} is a 'local' Grover operator which acts on the local search space in each non-overlapping block B_i of size b, $i = 1, \ldots, K$. The initial state, uniformly superposed over all N input values, is

$$|\psi_{\rm init}\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \tag{2}$$

and, similarly, the target state is a uniform superposition over the single block B_t containing the unique solution state in a regular Grover search

$$|\psi_{\rm target}\rangle = \frac{1}{\sqrt{b}} \sum_{x\in B_t} |x\rangle \,. \tag{3}$$

Briefly, after $j_{\rm g}$ iterations of the global operator $G_{\rm g}$, the amplitude of the solution state increases. Next, after $j_{\rm l}$ iterations of the local operator $G_{\rm l}$, the amplitude of the solution state and the amplitudes of the remaining states in the target block have been modified, with no change to the amplitudes of all other states. Finally, one more iteration of the global search operator $G_{\rm g}$ is used. After these steps one would ideally want non-zero amplitudes only for those states within the target block. Several combinations of the sequences of global and local operators have been investigated and numerically the GRK formulation has been found to be optimal (in number of calls to the oracle).(8) For the purposes of this paper we shall assume this result correct. Hence, we shall give more details about the GRK construction.(8)

Since the number of blocks K and block size b satisfy $N = Kb$ we find it useful to define some trigonometric counterparts to them via

$$\sin^2\theta_{\rm g} = \frac{1}{N}\,, \qquad \sin^2\theta_{\rm l} = \frac{1}{b}\,, \qquad \sin^2\gamma = \frac{1}{K}\,. \tag{4}$$

To succeed perfectly in finding the target block, the following condition should be satisfied

$$|\langle\psi_{\rm rem}|G_{\rm g} G_{\rm l}^{j_{\rm l}} G_{\rm g}^{j_{\rm g}}|\psi_{\rm init}\rangle| = 0\,, \tag{5}$$

where $|\psi_{\rm rem}\rangle$ is the uniform superposition of all states outside the target block. This reduces to the number of global $j_{\rm g}$ and local $j_{\rm l}$ Grover iterations as satisfying(8)

$$\begin{aligned} \cos(2j_{\rm l}\theta_{\rm l}) &= \frac{\tan\gamma}{\tan 2\gamma} = \frac{K-2}{2(K-1)}, \\ \tan(2j_{\rm g}\theta_{\rm g}) &= \frac{\cos 2\gamma}{\sin\gamma\sqrt{3-4\sin^2\gamma}} = \frac{K-2}{\sqrt{3K-4}}\,. \end{aligned} \tag{6}$$

Unfortunately, in general $j_{\rm l}$ and $j_{\rm g}$ satisfying these equations are not integers. Hence, in the GRK algorithm in order to minimize error in the final state one instead should use $\hat{j}_l = \lfloor j_l \rceil$ and $\hat{j}_g = \lfloor j_g \rceil$ number of local and global iterations, respectively, (where $\lfloor r \rceil$ is the nearest integer to r). Naturally, this approximation causes some error in the partial search. We shall now show how to modify the GRK algorithm to guarantee sure success, thus overcoming this difficulty. For the moment, however, we shall leave the number of local and global iterations j_l and j_g as unspecified.

3. PHASE CONDITION FOR SURE SUCCESS

The special case of sure success partial search is the sure success full search—in other words, a sure success variation of the usual Grover search algorithm. Many approaches to guaranteeing the ideal behavior of full search have been proposed.[9–11] In this work, however, we shall investigate a variation of what we consider to be the simplest of these, given originally by Brassard *et al.*,[11] which only requires modifying the final global operator iteration of the entire algorithm.

First, as in Ref. 8, we note that the entire action of the partial search may be compactly described by a three-dimensional subspace spanned by the vectors: $|x_{\text{sol}}\rangle$ the unique solution to the full search; $|\psi'_{\text{target}}\rangle$ the normalized target block state *excluding* the solution state; and $|\psi_{\text{rem}}\rangle$ for other states. Using these three basis states, the initial state $|\psi_{\text{init}}\rangle$ of Eq. (2) may be written

$$\begin{aligned} |\psi_{\text{init}}\rangle = {} & \sin\gamma \sin\theta_l |x_{\text{sol}}\rangle + \sin\gamma\cos\theta_l |\psi'_{\text{target}}\rangle \\ & + \cos\gamma |\psi_{\text{rem}}\rangle . \end{aligned} \tag{7}$$

Similarly, the ideal target state $|\psi_{\text{target}}\rangle$ of Eq. (3) is

$$|\psi_{\text{target}}\rangle = \sin\theta_l |x_{\text{sol}}\rangle + \cos\theta_l |\psi'_{\text{target}}\rangle . \tag{8}$$

The $G_g^{j_g}$ operator is represented as

$$G_g^{j_g} = T M_{j_g} T, \tag{9}$$

where

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \dfrac{\cos\theta_l \sin\gamma}{\cos\theta_g} & \dfrac{\cos\gamma}{\cos\theta_g} \\ 0 & \dfrac{\cos\gamma}{\cos\theta_g} & -\dfrac{\cos\theta_l\sin\gamma}{\cos\theta_g} \end{pmatrix} \tag{10}$$

and

$$M_{j_{\rm g}} = \begin{pmatrix} \cos(2j_{\rm g}\theta_{\rm g}) & \sin(2j_{\rm g}\theta_{\rm g}) & 0 \\ -\sin(2j_{\rm g}\theta_{\rm g}) & \cos(2j_{\rm g}\theta_{\rm g}) & 0 \\ 0 & 0 & (-1)^{j_{\rm g}} \end{pmatrix}. \tag{11}$$

The $G_l^{j_l}$ operator is represented as[8]

$$G_{\rm l}^{j_{\rm l}} = \begin{pmatrix} \cos(2j_{\rm l}\theta_{\rm l}) & \sin(2j_{\rm l}\theta_{\rm l}) & 0 \\ -\sin(2j_{\rm l}\theta_{\rm l}) & \cos(2j_{\rm l}\theta_{\rm l}) & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{12}$$

The intermediate state after $j_{\rm g}$ global Grover iterations is given by Korepin and Liao[8]

$$G_{\rm g}^{j_{\rm g}}|\psi_{\rm init}\rangle = \frac{1}{\cos^2\theta_{\rm g}} \begin{pmatrix} \cos\theta_{\rm g}\left(s_{\rm g}m + c_{\rm g}\cos\theta_{\rm g}\sin\theta_{\rm g}\right) \\ \cos\theta_{\rm l}\sin\gamma\left(c_{\rm g}m - s_{\rm g}\cos\theta_{\rm g}\sin\theta_{\rm g}\right) \\ \cos\gamma\left(c_{\rm g}m - s_{\rm g}\cos\theta_{\rm g}\sin\theta_{\rm g}\right) \end{pmatrix}, \tag{13}$$

where $c_{\rm g} = \cos(2j_{\rm g}\theta_{\rm g})$, $s_{\rm g} = \sin(2j_{\rm g}\theta_{\rm g})$, and $m = \cos^2\theta_{\rm l}\sin^2\gamma + \cos^2\gamma$.

The next intermediate state after j_g global and j_l local Grover iterations is given by Korepin and Liao[8]

$$\begin{aligned} G_l^{j_l} G_g^{j_g}|\psi_{\rm init}\rangle &= \frac{1}{\cos^2\theta_g} \\ &\times \begin{pmatrix} c_l\cos\theta_g\left(s_g m + c_g\cos\theta_g\sin\theta_g\right) + s_l\cos\theta_l\sin\gamma\left(c_g m - s_g\cos\theta_g\sin\theta_g\right) \\ -s_l\cos\theta_g\left(s_g m + c_g\cos\theta_g\sin\theta_g\right) + c_l\cos\theta_l\sin\gamma\left(c_g m - s_g\cos\theta_g\sin\theta_g\right) \\ \cos\gamma\left(c_g m - s_g\cos\theta_g\sin\theta_g\right) \end{pmatrix} \\ &= \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \end{aligned} \tag{14}$$

where $c_{\rm l} = \cos(2j_{\rm l}\theta_{\rm l})$ and $s_{\rm l} = \sin(2j_{\rm l}\theta_{\rm l})$.

The final global Grover operator iteration is modified with two phases as in the exact Grover search[11]

$$\begin{aligned} G_{\rm g}^{\rm final} \equiv &-\left[\mathbb{1} - (\mathbb{1} - {\rm e}^{2i\theta})|\psi_{\rm init}\rangle\langle\psi_{\rm init}|\right] \\ &\times\left[\mathbb{1} - (\mathbb{1} - {\rm e}^{i(\phi-\theta)})|x_{\rm sol}\rangle\langle x_{\rm sol}|\right]. \end{aligned} \tag{15}$$

Translating this into the three basis states supporting the entire computation we obtain

$$G_{\rm g}^{\rm final}=\begin{pmatrix} -e^{i(\phi-\theta)}[1-(1-e^{2i\theta})\sin^2\gamma\sin^2\theta_1] & (1-e^{2i\theta})\sin^2\gamma\sin\theta_1\cos\theta_1 & (1-e^{2i\theta})\cos\gamma\sin\gamma\sin\theta_1 \\ e^{i(\phi-\theta)}(1-e^{2i\theta})\sin^2\gamma\sin\theta_1\cos\theta_1 & (1-e^{2i\theta})\sin^2\gamma\cos^2\theta_1-1 & (1-e^{2i\theta})\cos\gamma\sin\gamma\cos\theta_1 \\ e^{i(\phi-\theta)}(1-e^{2i\theta})\sin\gamma\sin\theta_1\cos\gamma & (1-e^{2i\theta})\sin\gamma\cos\gamma\cos\theta_1 & (1-e^{2i\theta})\cos^2\gamma-1 \end{pmatrix}. \tag{16}$$

Finally then, our aim of a sure success partial search will be achieved if we can find two phases, θ and ϕ, for the above final global Grover operator which satisfy the condition

$$|\langle\psi_{\rm rem}|G_{\rm g}^{\rm final}G_1^{j_1}G_{\rm g}^{j_{\rm g}}|\psi_{\rm init}\rangle|=0\,. \tag{17}$$

The relevant phase condition then reduces to

$$\begin{aligned} &a e^{i(\phi-\theta)}(1-e^{2i\theta})\sin\gamma\sin\theta_1\cos\gamma \\ &\quad+b(1-e^{2i\theta})\sin\gamma\cos\gamma\cos\theta_1 \\ &\quad+c[(1-e^{2i\theta})\cos^2\gamma-1]=0\,, \end{aligned} \tag{18}$$

where a, b, and c are defined in Eq. (14).

The phase condition may then be rewritten as

$$e^{i(\phi-\theta)}(1-e^{2i\theta})x+(1-e^{2i\theta})y+2z=0\,, \tag{19}$$

where

$$\begin{aligned} x &\equiv a\sin\gamma\sin\theta_1\cos\gamma, \\ y &\equiv b\sin\gamma\cos\gamma\cos\theta_1+c\cos^2\gamma, \\ z &\equiv -\frac{c}{2}\,. \end{aligned} \tag{20}$$

The real and imaginary parts of Eq. (19) may be simplified to give

$$\begin{aligned} \sin\phi &= -\frac{y}{x}\sin\theta-\frac{z}{x\sin\theta}, \\ \cos\phi &= -\frac{y}{x}\cos\theta\,. \end{aligned} \tag{21}$$

Finally, combining these two equations together, we may eliminate ϕ to yield

$$\sin^2\theta=\frac{z^2}{x^2-y^2-2yz}\,, \tag{22}$$

which to have a solution must satisfy

$$x^2\geq(y+z)^2\,. \tag{23}$$

There will then be a solution for ϕ provided the right-hand-sides of Eq. (21) are bounded in absolute value by unity.

4. NUMERICAL ANALYSIS

In this section, we explain our numerical results showing that the phase condition (18) may be easily solved numerically. Now the number of local and global search steps must be integers so in the GRK algorithm[7] their values are chosen to be $\hat{j}_{\rm l} = \lfloor j_{\rm l} \rceil$ and $\hat{j}_{\rm g} = \lfloor j_{\rm g} \rceil$. This works fine for GRK under the assumption that both b and K are large. However, we have sought a more general solution. Using a numerical search, we found that θ and ϕ could always be found to satisfy the phase condition (18) provided we chose

$$\begin{aligned} \hat{j}_{\rm l} &= \lfloor j_{\rm l} \rfloor, \\ \hat{j}_{\rm g} &= \lfloor j_{\rm g} \rfloor + \{0, 1, 2\}, \end{aligned} \tag{24}$$

where the floor of both $j_{\rm l}$ and $j_{\rm g}$ are chosen, however, the latter may require one or possibly two extra steps (which we denote by $\{0, 1, 2\}$). This strategy was found to work numerically for $N = Kb \le 10^6$ in all cases except for the case $K = 2$ and $b = 2$. In practice, finding the parameters to work with would be straight-forward to implement since for these three options for j_g we may determine the auxiliary quantities x, y, and z immediately with Eq. (20) after which θ and ϕ are determined separately through Eqs. (21) and (22).

5. CONCLUSION

In this work, we have investigated the necessary phase conditions to guarantee sure success of the partial search algorithm. All the search action goes on within a three-dimensional Hilbert space and solutions to the phase conditions may be found very easily.

In principle, since there are many potential generalizations of the full Grover search algorithm, partial search can also be extended for more general cases. For example, one could consider extending the partial search algorithm to the more general case involving, say, multiple target blocks. Other algorithms based on the Grover search algorithm such as the algorithm associated with the Boolean weight decision problem[12] could be converted into a, so called, block weight decision problem.

ACKNOWLEDGMENTS

BSC was partly supported by the Ministry of Information and Communication of South Korea (IT Overseas National Scholarship Program). SLB currently holds a Royal Society—Wolfson Research Merit Award. This research is part of the QIP IRC (www.qipirc.org) supported by EPSRC (GR/S82176/01).

REFERENCES

1. D. Deutsch, *Proc. Roy. Soc. Lond. Ser. A* **400**(1818), 97–117 (1985).
2. D. Deutsch and R. Jozsa, *Proc. Roy. Soc. Lond. Ser. A* **439**(1907), 553–558 (1992).
3. P. W. Shor, *SIAM J. on Comput.* **26**(5), 1484–1509 (1997).
4. L. Grover, in *Proceedings of 28th Annual Symposium on the Theory of Computing (STOC)*, (Philadelphia, Pennsylvania, USA, 1996), pp. 212–219, quant-ph/9605043.
5. V. E. Korepin and L. K. Grover, *Quantum Inform. Process.* **5**(1), 3 (2006), quant-ph/0504157.
6. L. K. Grover and J. Radhakrishnan, in *Proceedings of the 17th annual ACM Symposium on Parallelism in Algorithms and Architectures, (SPAA)*, (Las Vegas, Nevada, USA, 2005), pp. 186–194, quant-ph/0407122.
7. V. E. Korepin, *J. Phys. A. Math. Gen.* **38**, L731–758 (2005).
8. V. E. Korepin and J. Liao, *Quantum Inform. Process.* **5**(3), 209 (2006), quant-ph/0510179.
9. P. Høyer, *Phys. Rev. A* **62**, 052304 (2000).
10. Y. Sun, G.-L. Long and X. Li, *Phys. Let. A* **294**, 143 (2002).
11. G. Brassard, P. Høyer, M. Mosca, and A. Tapp, quant-ph/0005055, May 2000. in *Quantum Computation and Information, Contemporary Mathematics Series Millenium Volume,* ed. S. J. Lomonaco (AMS, providence, RI, 2002), Vol. 305, pp. 53–74 (2002).
12. S. L. Braunstein, B.-S. Choi, S. Maitra, D. Chakrabarti, S. Ghosh, and P. Mukhopadhyay, quant-ph/0410043.