Grover's Algorithm for Multiobject Search in Quantum Computing

Goong Chen[1,2], Stephen A. Fulling[1], and Marlan O. Scully[3,4]

Abstract

L. K. Grover's search algorithm in quantum computing gives an optimal, square-root speedup in the search for a single object in a large unsorted database. In this paper, we expound Grover's algorithm in a Hilbert-space framework that isolates its geometrical essence, and we generalize it to the case where more than one object satisfies the search criterion.

In memory of Daniel Walls

1. Department of Mathematics, Texas A&M University, College Station, TX 77843-3368.
2. Supported in part by Texas A&M University Interdisciplinary Research Grant IRI 99-22.
3. Department of Physics and Institute for Quantum Studies, Texas A&M University, College Station, TX 77843-4242, and Max-Planck Institut für Quantenoptik, Munich.
4. Supported in part by ONR, NSF, and Welch Foundation.

1 Introduction

A quantum computer (QC) is envisaged as a collection of 2-state "quantum bits", or *qubits* (e.g., spin 1/2 particles). Quantum computation does calculations on data densely coded in the entangled states that are the hallmark of quantum mechanics, potentially yielding unprecedented parallelism in computation, as P. Shor's work [8, 9] proved in 1994. Two years later, L. K. Grover [4] showed that for an unsorted database with N items in storage, it takes an average number of $\mathcal{O}(\sqrt{N})$ searches to locate a single desired object by his quantum search algorithm. If N is a very large number, this is a significant square-root speedup over the exhaustive search algorithm in a classical computer, which requires an average number of $\frac{N+1}{2}$ searches. Even though Grover's algorithm is not logarithmically fast (as Shor's is), it has been argued that the wide range of its applicability compensates for this [2].

Grover's original papers [4, 5] deal with search for a single object. In practical applications, typically more than one item will satisfy the criterion used for searching. In the simplest generalization of Grover's algorithm, the number of "good" items is known in advance (and greater than 1). Here we expound this generalization, along the lines of a treatment of the single-object case by Farhi and Gutmann [3, Appendix] that makes the Hilbert-space geometry of the situation very clear.

The success of Grover's algorithm and its multiobject generalization is attributable to two main sources:

(i) the notion of amplitude amplication; and

(ii) the dramatic reduction to invariant subspaces of low dimension for the unitary operators involved.

Indeed, the second of these can be said to be responsible for the first: A proper geometrical formulation of the process shows that all the "action" takes place within a *two-dimensional, real* subspace of the Hilbert space of quantum states. Since the state vectors are normalized, the state is confined to a one-dimensional unit circle and (if moved at all) initially has nowhere to go except toward the place where the amplitude for the sought-for state is maximized. This accounts for the robustness of Grover's algorithm — that is, the fact that Grover's original choice of initial state and of the Walsh–Hadamard transformation can be replaced by (almost) any initial state and (almost) any unitary transformation [6, 7, 2].

The notion of amplitude amplification was emphasized in the original works [4, 5, 6] of Grover himself and in those of Boyer, Brassard, Høyer and Tapp [1] and Brassard, Høyer and Tapp [2]. Dimensional reduction is prominent in the papers by Farhi and Gutmann [3] and Jozsa [7]. We applied dimensional reduction to multiobject search independently of references [1] and [2] and later learned that the same conclusions about multiobject search (and more) had been obtained there in a different framework. (We modestly suggest that our framework is clearer.)

The rest of the paper is divided into two parts. In §2, we reformulate the original Grover algorithm, and in §3, a multiobject search algorithm is studied.

2 Introduction to Grover's Algorithm

In this section, we review Grover's algorithm for searching a single element in an unsorted database containing $N \gg 1$ items, following [3]. This proof is presented in a way that makes possible the generalization of the algorithm to perform multiobject search in an unstructured database.

Grover treated the following abstract problem: We are given a Boolean function $f(a)$, $a = 1$, $2, \ldots, N$, which is known to be zero for all a except at a single point, say at $a = w$, where $f(w) = 1$. The problem is to find the value w. (The function is an "oracle" or "black box": all we know about it is its output for any input we care to insert.) On a classical computer we have to evaluate the function $\frac{N+1}{2}$ times on average to find the answer to this problem. In contrast, Grover's quantum algorithm finds w in $\mathcal{O}(\sqrt{N})$ steps.

The quantum-mechanical statement of the problem is that given an orthonormal basis $\{\,|\,a\rangle \,:\, a = 1, 2, \ldots, N\}$ we want to single out the basis element $|\,w\rangle$ for which $f(w) = 1$. (More concretely, each $|\,a\rangle$ is to be an eigenstate of the qubits making up the QC. If $N = 2^n$, then n qubits will be needed.) At $t = 0$, we prepare the state of the system $|\,\psi\rangle$ in a superposition of the states $\{\,|\,a\rangle\}$, each with the same probability:

$$|\,\psi\rangle = \frac{1}{\sqrt{N}} \sum_{1}^{N} |\,a\rangle \equiv |\,s\rangle. \tag{2.1}$$

By the Gram–Schmidt construction we extend $|\,w\rangle$ to an orthonormal basis for the subspace spanned by $|\,w\rangle$ and $|\,s\rangle$. That is, we introduce a normalized vector $|\,r\rangle$ orthogonal to $|\,w\rangle$,

$$|\,r\rangle = \frac{1}{\sqrt{N-1}} \sum_{a \neq w} |\,a\rangle, \tag{2.2}$$

and find that the initial state has the representation

$$|\,s\rangle = \sqrt{\frac{N-1}{N}}|\,r\rangle + \frac{1}{\sqrt{N}}|\,w\rangle. \tag{2.3}$$

Following Grover, we now define the unitary operator of *inversion about average*,

$$I_s = \boldsymbol{I} - 2|s\rangle\langle s|. \tag{2.4}$$

Notice that the only action of this operator is to flip the sign of the state $|\,s\rangle$; that is, $I_s\,|\,s\rangle = -|\,s\rangle$ but $I_s|\,v\rangle = |\,v\rangle$ if $\langle s|v\rangle = 0$. Using (2.3) we write I_s as

$$I_s = -\left(1 - \frac{2}{N}\right)(\,|\,r\rangle\langle r\,| - |\,w\rangle\langle w\,|\,) - 2\frac{\sqrt{N-1}}{N}(\,|\,r\rangle\langle w\,| + |\,w\rangle\langle r\,|\,). \tag{2.5}$$

In other words, with respect to the orthonormal basis the operator I_s is represented by the orthogonal (real unitary) matrix

$$\begin{bmatrix} 1-\dfrac{2}{N} & -2\cdot\dfrac{\sqrt{N-1}}{N} \\ -2\cdot\dfrac{\sqrt{N-1}}{N} & -\left(1-\dfrac{2}{N}\right) \end{bmatrix}.$$

Similarly, the operator I_w is defined by

$$I_w = \boldsymbol{I} - 2\,|\,w\rangle\langle w\,| \tag{2.6}$$

and satisfies $I_w|\,w\rangle = -|\,w\rangle$. The crucial fact is that in terms of the oracle function f,

$$I_w\,|\,a\,\rangle = (-1)^{f(a)}\,|\,a\rangle \tag{2.7}$$

for each $|\,a\,\rangle$ in the original basis for the full state space of the QC. Therefore, to execute the operation I_w one does not need to know w; one only needs to know f. (And conversely, being able to execute I_w does not mean that one can immediately determine w; $\sqrt{N}$ steps will be needed.)

A "Grover iteration" is the unitary operator $U \equiv -I_sI_w$. This product can be calculated easily in either the bra-ket or the matrix formalism. In particular, for the transition element $\langle w\,|\,U\,|\,s\rangle$ we obtain

$$\begin{aligned} \langle w\,|\,U\,|\,s\rangle &= \langle w\,|\left[\left(1-\frac{2}{N}\right)\boldsymbol{I} + \frac{2\sqrt{N-1}}{N}(\,|\,w\rangle\langle r\,| - |\,r\rangle\langle w\,|\,)\right]|\,s\rangle \\ &= \left(1-\frac{2}{N}\right)\frac{1}{\sqrt{N}} + 2\left(1-\frac{1}{N}\right)\frac{1}{\sqrt{N}} \\ &= \frac{1}{\sqrt{N}} + \frac{2}{\sqrt{N}} + \mathcal{O}(N^{-3/2}). \end{aligned} \tag{2.8}$$

The fact that the matrix element $\langle w\,|\,U\,|\,s\rangle$ is nonzero can be used to reinforce the probability amplitude of the unknown state $|\,w\rangle$. If we use U as our unitary search operation, then after $m \gg 1$ trials the value $\langle w\,|\,U^m\,|\,s\rangle$ can be evaluated as follows:

$$\begin{aligned} \langle w|U^m|s\rangle &= [1 \quad 0]\begin{bmatrix} 1-\dfrac{2}{N} & 2\cdot\dfrac{\sqrt{N-1}}{N} \\ -2\cdot\dfrac{\sqrt{N-1}}{N} & 1-\dfrac{2}{N} \end{bmatrix}^m \begin{bmatrix} \dfrac{1}{\sqrt{N}} \\ \sqrt{\dfrac{N-1}{N}} \end{bmatrix} \\ &= [1 \quad 0]\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}^m \begin{bmatrix} \dfrac{1}{\sqrt{N}} \\ \sqrt{\dfrac{N-1}{N}} \end{bmatrix} \qquad \left(\theta \equiv \sin^{-1}\frac{2\sqrt{N-1}}{N}\right) \\ &= [1 \quad 0]\begin{bmatrix} \cos m\theta & \sin m\theta \\ -\sin m\theta & \cos m\theta \end{bmatrix} \begin{bmatrix} \dfrac{1}{\sqrt{N}} \\ \sqrt{\dfrac{N-1}{N}} \end{bmatrix} \\ &= \frac{1}{\sqrt{N}}\cos m\theta + \sqrt{\frac{N-1}{N}}\sin m\theta, \end{aligned}$$

or

$$\langle w|U^m|s\rangle = \cos(m\theta - \alpha), \qquad \alpha \equiv \cos^{-1}\frac{1}{\sqrt{N}}\,. \tag{2.9}$$

Setting $\cos^2(m\theta - \alpha) = 1$, we can maximize the amplitude of $U^m|s\rangle$ in $|w\rangle$; thus

$$\begin{aligned} m\theta - \alpha &= 0, \\ m &= \frac{\alpha}{\theta}\,. \end{aligned} \tag{2.10}$$

(If no integer satisfies this equation exactly, take the closest one.) When N is large, $\theta \approx \frac{2}{\sqrt{N}}$, $\alpha \approx \frac{\pi}{2}$, from (2.10) we obtain

$$m \approx \frac{\pi}{2}\Big/\left(\frac{2}{\sqrt{N}}\right) = \frac{\pi}{4}\sqrt{N}. \tag{2.11}$$

Therefore, after $m = \mathcal{O}(\sqrt{N})$ trials the state $|\,w\rangle$ will be projected out, which is precisely Grover's result. By observing the qubits, we will learn w. *By constructive interference, we have constructed* $|\,w\rangle$! (Since m only approximately satisfies (2.10), there is a small chance of getting a "bad" w. But because evaluating $f(w)$ is easy, in that case one will recognize the mistake and start over.)

3 Generalization of Grover's Algorithm to Multiobject Search

Here we generalize Grover's search algorithm in its original form [4, 5] to the situation where the number of objects satisfying the search criterion is greater than 1.

Let a database $\{w_i \mid i = 1, 2, \ldots, N\}$, with corresponding orthonormal eigenstates $\{|w_i\rangle : i = 1, 2, \ldots, N\}$ in the QC, be given. Let f be an oracle function such that

$$f(w_j) = \begin{cases} 1, & j = 1, 2, \ldots, \ell, \\ 0 & j = \ell + 1, \ell + 2, \ldots, N. \end{cases}$$

Here the ℓ elements $\{w_j \mid 1 \leq j \leq \ell\}$ are the desired objects of search. (To avoid introducing another layer of subscripts, we pretend in this theoretical discussion that these good objects are the first ℓ items in the list. In a real search application they would appear in the list in random order; in other words, all N items w_i are subjected to some unknown permutation, which we do not indicate explicitly.) Let $\mathcal{H}$ be the Hilbert space generated by the orthonormal basis $\mathcal{B} = \{|w_j\rangle \mid j = 1, \ldots, N\}$. Let $L = \mathrm{span}\{|w_j\rangle \mid 1 \leq j \leq \ell\}$ be the subspace of $\mathcal{H}$ spanned by the vectors of the good objects.

Define a linear operation in terms of the oracle function f as follows:

$$I_L|w_j\rangle = (-1)^{f(w_j)}|w_j\rangle, \qquad j = 1, 2, \ldots, N. \tag{3.1}$$

Then since I_L is linear, the extension of I_L to the entire space $\mathcal{H}$ is unique, with an "explicit" representation

$$I_L = \boldsymbol{I} - 2\sum_{j=1}^{\ell} |w_j\rangle\langle w_j|, \tag{3.2}$$

where $\boldsymbol{I}$ is the identity operator on $\mathcal{H}$. I_L is the operator of *rotation (by π) of the phase* of the subspace L. Note again that the explicitness of (3.2) is misleading because explicit knowledge of $\{|w_j\rangle \mid 1 \le j \le \ell\}$ in (3.2) is not available. Nevertheless, (3.2) is a well-defined (and unitary) operator on $\mathcal{H}$ because of (3.1). (Unitarity is a requirement for all operations in a QC.)

We now again define $|s\rangle$ as

$$|s\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N} |w_i\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{\ell} |w_i\rangle + \sqrt{\frac{N-\ell}{N}}|r\rangle, \tag{3.3}$$

where now

$$|r\rangle = \frac{1}{\sqrt{1-(\ell/N)}}\left(|s\rangle - \frac{1}{\sqrt{N}}\sum_{i=1}^{\ell}|w_i\rangle\right).$$

As before, we use

$$I_s = \boldsymbol{I} - 2|s\rangle\langle s|. \tag{3.4}$$

Note that I_s in (3.4) is unitary and hence quantum-mechanically admissible. I_s is explicitly known, constructible with the so-called Walsh–Hadamard transformation.

Lemma 3.1. *Let $\widetilde{L} = \mathrm{span}(L \cup \{|r\rangle\})$. Then $\{|w_i\rangle, |r\rangle \mid i = 1, 2, \ldots, \ell\}$ forms an orthonormal basis of $\widetilde{L}$. The orthogonal direct sum $\mathcal{H} = \widetilde{L} \oplus \widetilde{L}^{\perp}$ is an orthogonal invariant decomposition for both operators $I_{\widetilde{L}}$ and I_s. Furthermore,*

(i) The restriction of I_s to $\widetilde{L}$ admits this real unitary matrix representation with respect to the orthonormal basis $\{|w_1\rangle, |w_2\rangle, \ldots, |w_\ell\rangle, |r\rangle\}$:

$$A = [a_{ij}]_{(\ell+1)\times(\ell+1)},$$

$$a_{ij} = \begin{cases} \delta_{ij} - \dfrac{2}{N}, & 1 \le i, j \le \ell, \\ -\dfrac{2\sqrt{N-\ell}}{N}(\delta_{i,\ell+1} + \delta_{j,\ell+1}), & i = \ell+1 \text{ or } j = \ell+1, i \ne j, \\ \dfrac{2\ell}{N} - 1, & i = j = \ell+1. \end{cases} \tag{3.5}$$

(ii) The restriction of I_s of $\widetilde{L}^{\perp}$ is $\mathbb{P}_{\widetilde{L}^{\perp}}$, the orthogonal projection operator onto $\widetilde{L}^{\perp}$. Consequently, $I_s|_{\widetilde{L}^{\perp}} = \boldsymbol{I}_{\widetilde{L}^{\perp}}$, where $\boldsymbol{I}_{\widetilde{L}^{\perp}}$ is the identity operator on $\widetilde{L}^{\perp}$.

Proof. We have, from (3.3) and (3.4),

$$
\begin{aligned}
I_s &= \boldsymbol{I} - 2\left[\frac{1}{\sqrt{N}}\sum_{i=1}^{\ell}|w_i\rangle + \sqrt{\frac{N-\ell}{N}}|r\rangle\right]\left[\frac{1}{\sqrt{N}}\sum_{j=1}^{\ell}\langle w_j| + \sqrt{\frac{N-\ell}{N}}\langle r|\right]\\
&= \left[\sum_{i=1}^{\ell}|w_i\rangle\langle w_i\rangle + |r\rangle\langle r| + \mathbb{P}_{\widetilde{L}^\perp}\right] - \left\{\frac{2}{N}\sum_{i=1}^{\ell}\sum_{j=1}^{\ell}|w_i\rangle\langle w_j|\right.\\
&\quad \left. + \frac{2\sqrt{N-\ell}}{N}\left[\sum_{i=1}^{\ell}(|w_i\rangle\langle r| + |r\rangle\langle w_i|)\right] + 2\left(\frac{N-\ell}{N}\right)|r\rangle\langle r|\right\}\\
&= \sum_{i=1}^{\ell}\sum_{j=1}^{\ell}\left(\delta_{ij} - \frac{2}{N}\right)|w_i\rangle\langle w_j| - \frac{2\sqrt{N-\ell}}{N}\left[\sum_{i=1}^{\ell}(|w_i\rangle\langle r| + |r\rangle\langle w_i|)\right]\\
&\quad + \left(\frac{2\ell}{N} - 1\right)|r\rangle\langle r| + \mathbb{P}_{\widetilde{L}^\perp}.
\end{aligned} \tag{3.6}
$$

The conclusion follows. ◻

The generalized "Grover search engine" for multiobject search is now constructed as

$$
U = -I_s I_L\,. \tag{3.7}
$$

Lemma 3.2. *The orthogonal direct sum $\mathcal{H} = \widetilde{L} \oplus \widetilde{L}^\perp$ is an invariant decomposition for the unitary operator U, such that the following holds:*

(1) With respect to the orthonormal basis $\{|w_1\rangle, \dots, |w_\ell\rangle, |r\rangle\}$ of $\widetilde{L}$, U admits the real unitary matrix representation

$$
\begin{aligned}
&U|_{\widetilde{L}} = [u_{ij}]_{(\ell+1)\times(\ell+1)},\\
&u_{ij} = \begin{cases} \delta_{ij} - \dfrac{2}{N}, & 1 \le i, j \le \ell,\\[2mm] \dfrac{2\sqrt{N-\ell}}{N}(\delta_{j,\ell+1} - \delta_{i,\ell+1}), & i = \ell+1 \text{ or } j = \ell+1, i \ne j,\\[2mm] 1 - \dfrac{2\ell}{N}, & i = j = \ell+1. \end{cases}
\end{aligned} \tag{3.8}
$$

(2) The restriction of U to $\widetilde{L}^\perp$ is $-\mathbb{P}_{\widetilde{L}^\perp} = -\boldsymbol{I}_{\widetilde{L}^\perp}$.

Proof. Substituting (3.2) and (3.6) into (3.7) and simplifying, we obtain

$$
\begin{aligned}
U &= -I_s I_L = \cdots \text{(simplification)}\\
&= \sum_{i=1}^{\ell}\sum_{j=1}^{\ell}\left(\delta_{ij} - \frac{2}{N}\right)|w_i\rangle\langle w_j| + \frac{2\sqrt{N-\ell}}{N}\sum_{i=1}^{\ell}(|w_i\rangle\langle r| - |r\rangle\langle w_i|)\\
&\quad + \left(1 - \frac{2\ell}{N}\right)|r\rangle\langle r| - \mathbb{P}_{\widetilde{L}^\perp}\,.
\end{aligned}
$$

The lemma follows. ◻

Lemmas 3.1 and 3.2 above effect a reduction of the problem to an invariant subspace $\widetilde{L}$. However, $\widetilde{L}$ is an $(\ell+1)$-dimensional subspace where ℓ may also be fairly large. Another reduction of dimensionality is needed to further simplify the operator U.

Proposition 3.3. *Define $\mathcal{V}$ by*

$$\mathcal{V} = \left\{ |v\rangle \in \widetilde{L} \,:\, |v\rangle = a\sum_{i=1}^{\ell} |w_i\rangle + b|r\rangle;\ a,b \in \mathbb{C} \right\}.$$

Then $\mathcal{V}$ is an invariant two-dimensional subspace of U such that

(1) $r, s \in \mathcal{V}$;

(2) $U(\mathcal{V}) = \mathcal{V}$.

Proof. Straightforward verification. □

Let $|\widetilde{w}\rangle = \frac{1}{\sqrt{\ell}} \sum\limits_{i=1}^{\ell} |w_i\rangle$. Then $\{|\widetilde{w}\rangle, |r\rangle\}$ forms an orthonormal basis of $\mathcal{V}$. We have the second reduction, to dimensionality 2.

Theorem 3.4. *With respect to the orthonormal basis $\{|\widetilde{w}\rangle, |r\rangle\}$ in the invariant subspace $\mathcal{V}$, U admits the real unitary matrix representation*

$$U = \begin{bmatrix} \frac{N-2\ell}{N} & \frac{2\sqrt{\ell(N-\ell)}}{N} \\ \frac{-2\sqrt{\ell(N-\ell)}}{N} & \frac{N-2\ell}{N} \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}, \quad \theta \equiv \sin^{-1}\left(\frac{2\sqrt{\ell(N-\ell)}}{N}\right). \tag{3.9}$$

Proof. Use the matrix representation (3.8) and the definition of $|\widetilde{w}\rangle$. □

Since $|s\rangle \in \mathcal{V}$, we can calculate $U^m|s\rangle$ efficiently using (3.9):

$$\begin{aligned} U^m|s\rangle &= U^m\left(\frac{1}{\sqrt{N}}\sum_{i=1}^{\ell}|w_i\rangle + \sqrt{\frac{N-\ell}{N}}|r\rangle\right) \qquad \text{(by (3.3))} \\ &= U^m\left(\frac{\ell}{\sqrt{N}}|\widetilde{w}\rangle + \sqrt{\frac{N-\ell}{N}}|r\rangle\right) \\ &= \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}^m \begin{bmatrix} \frac{\ell}{\sqrt{N}} \\ \sqrt{\frac{N-\ell}{N}} \end{bmatrix} \\ &= \begin{bmatrix} \cos(m\theta-\alpha) \\ -\sin(m\theta-\alpha)] \end{bmatrix} \quad \left(\alpha \equiv \cos^{-1}\frac{\ell}{\sqrt{N}}\right), \\ &= \cos(m\theta-\alpha)\cdot|\widetilde{w}\rangle - \sin(m\theta-\alpha)\cdot|r\rangle. \end{aligned} \tag{3.10}$$

Thus, the probability of reaching the state $|\widetilde{w}\rangle$ after m iterations is

$$P_m = \cos^2(m\theta - \alpha). \tag{3.11}$$

If $\ell \ll N$, then α is close to $\pi/2$ and, therefore, (3.11) is an increasing function of m initially. This again manifests the notion of amplitude amplification. This probability P_m is maximized if $m\theta - \alpha = 0$, implying

$$m = \left[\frac{\alpha}{\theta}\right] = \text{the integral part of } \frac{\alpha}{\theta}.$$

When ℓ/N is small, we have

$$\begin{aligned}\theta &= \sin^{-1}\left(\frac{2\sqrt{\ell(N-\ell)}}{N}\right)\\ &= \sin^{-1}\left(2\sqrt{\frac{\ell}{N}}\left[1-\frac{1}{2}\frac{\ell}{N}-\frac{1}{8}\left(\frac{\ell}{N}\right)^2\pm\cdots\right]\right)\\ &= 2\sqrt{\frac{\ell}{N}}+\mathcal{O}((\ell/N)^{3/2}),\\ \alpha &= \cos^{-1}\frac{\ell}{\sqrt{N}}=\frac{\pi}{2}-\left[\frac{\ell}{\sqrt{N}}+\mathcal{O}((\ell/N^{1/2})^3)\right].\end{aligned}$$

Therefore

$$\begin{aligned}m &\approx \frac{\frac{\pi}{2}-\left[\frac{\ell}{\sqrt{N}}+\mathcal{O}((\ell/N^{1/2})^3)\right]}{2\sqrt{\frac{\ell}{N}}+\mathcal{O}((\ell/N)^{3/2})}\\ &= \frac{\pi}{4}\sqrt{\frac{N}{\ell}}\left[1+\mathcal{O}\left(\frac{\ell}{N}\right)\right].\end{aligned}\tag{3.12}$$

Corollary 3.5. *The generalized Grover algorithm for multiobject search with operator U given by (3.7) has success probability $P_m = \cos^2(m\theta-\alpha)$ of reaching the state $|\widetilde{w}\rangle \in L$ after m iterations. For ℓ/N small, after $m=\frac{\pi}{4}\sqrt{N/\ell}$ iterations, the probability of reaching $|\widetilde{w}\rangle$ is close to 1.* □

The result (3.12) is consistent with Grover's original algorithm for single object search with $\ell = 1$, which has $m \approx \frac{\pi}{4}\sqrt{N}$; cf. (2.11).

Theorem 3.6. (Boyer, Brassard, Høyer and Tapp [1]). *Assume that ℓ/N is small. Then any search algorithm for ℓ objects, in the form of*

$$U_pU_{p-1}\dots U_1|w_I\rangle,$$

where each U_j, $j=1,2,\dots,p$, is a unitary operator and $|w_I\rangle$ is an arbitrary superposition state, takes in average $p=\mathcal{O}(\sqrt{N/\ell})$ iterations in order to reach the subspace L with a positive probability $P>\frac{1}{2}$ independent of N and ℓ. Therefore, the generalized Grover algorithm in Corollary 3.5 is of optimal order.

Proof. This is the major theorem in [1]; see Section 7 and particularly Theorem 8 therein. Note also the work of Zalka [10]. □

Unfortunately, if the number ℓ of good items is not known in advance, Corollary 3.5 does not tell us when to stop the iteration. This problem was addressed in [1], and in another way in [2]. In a related context an equation arose that was not fully solved in [1]. We consider it in the final segment of this paper. As in [1, §3], consider stopping the Grover process after j iterations, and, if a good object is not obtained, starting it over again from the beginning.

From Corollary 3.5, the probability of success after j iterations is $\cos^2(j\theta-\alpha)$. By a well-known theorem of probability theory, if the probability of success in k "trials" is p, then the expected number of trials before success is achieved will be $1/p$. In our case, each trial consists of j Grover iterations, so the expected number of iterations before success is

$$E(j) = j \cdot \sec^2(j\theta - \alpha).$$

The optimal number of iterations j is obtained by setting the derivative $E'(j)$ equal to zero:

$$\begin{aligned} 0 = E'(j) &= \sec^2(j\theta-\alpha) + 2j\theta \sec^2(j\theta-\alpha)\tan(j\theta-\alpha), \\ 2j\theta &= -\cot((j\theta-\alpha)). \end{aligned} \tag{3.13}$$

(In [1, §3], this equation is derived in the form $4\vartheta j = \tan((2j+1)\vartheta)$, which is seen to be equivalent to (3.13) by noting that $\vartheta = \frac{\theta}{2} = \frac{\pi}{2} - \alpha$. Those authors then note that they have not solved the equation $4\vartheta j = \tan((2j+1)\vartheta)$ but proceed to use an ad hoc equation $z = \tan(z/2)$ with $z = 4\vartheta j$ instead.) Let us now approximate the solution j of (3.13) iteratively as follows. From (3.13),

$$\begin{aligned} 2j\theta \sin(j\theta-\alpha) + \cos(j\theta-\alpha) &= 0, \\ e^{2i(\theta j-\alpha)} &= (i2\theta j+1)/(i2\theta j-1), \end{aligned} \tag{3.14}$$

and by taking the logarithm of both sides, we obtain

$$2i(\theta j - \alpha) = 2i\pi n + i \arg\left(\frac{i2\theta j+1}{i2\theta j-1}\right) + \ln\left|\frac{i2\theta j+1}{i2\theta j-1}\right|, \tag{3.15}$$

for any integer n. Assume that ℓ/N is small so that j is large, but we are looking for the smallest such positive j. Note that the logarithmic term in (3.15) vanishes, and

$$\begin{aligned} \arg\left(\frac{i2\theta j+1}{i2\theta j-1}\right) &= -2\tan^{-1}\frac{1}{2\theta j} \\ &= 2\left[\sum_{q=0}^{\infty} \frac{(-1)^{q+1}}{2q+1}\left(\frac{1}{2\theta j}\right)^{2q+1}\right] \\ &= -\frac{1}{\theta j} + \mathcal{O}((\theta j)^{-3}); \end{aligned}$$

by taking $n = 0$ in (3.15), we obtain

$$\begin{aligned} j &= \frac{1}{2i\theta}\left[2i\alpha - i\cdot\frac{1}{\theta j} + \mathcal{O}((\theta j)^{-3})\right] \\ &= \frac{1}{\theta}\left[\alpha - \frac{1}{2\theta j} + \mathcal{O}((\theta j)^{-3})\right]. \end{aligned} \tag{3.16}$$

The first order approximation j_1 for j is obtained by solving

$$\begin{aligned} j_1 &= \frac{1}{\theta}\left(\alpha - \frac{1}{2\theta j_1}\right), \\ j_1^2 - \frac{1}{\theta}\alpha j_1 + \frac{1}{2\theta^2} &= 0, \\ j_1 &= \frac{1}{2\theta}(\alpha + \sqrt{\alpha^2 - 2}). \end{aligned} \tag{3.17}$$

Higher order approximations j_{n+1} for $n = 1, 2, \ldots$, may be obtained by successive iterations

$$j_{n+1} = \frac{1}{\theta}\left(\alpha - \tan^{-1}\frac{1}{2\theta j_n}\right)$$

based on (3.13). This process will yield a convergent solution j to (3.13).

Acknowledgments: We thank B.-G. Englert and M. Hillery for acquainting us with some of the literature of quantum computation, and M. M. Kash for a technical discussion.

References

[1] M. Boyer, G. Brassard, P. Høyer and A. Tapp, Tight bounds on quantum searching, Fortsch. Phys. **46** (1998), 493–506.

[2] G. Brassard, P. Høyer and A. Tapp, Quantum counting, `quant-ph/9805082`, May 1998.

[3] E. Farhi and S. Gutmann, Analog analogue of a digital quantum computation, Phys. Rev. **A 57** (1998), 2403–2405.

[4] L.K. Grover, A fast quantum mechanical algorithm for database search, Proc. 28th Annual Symposium on the Theory of Computing, 212–218, ACM Press, New York, 1996.

[5] L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Phys. Rev. Letters **78** (1997), 325–328.

[6] L.K. Grover, Quantum computers can search rapidly by using almost any transformation, Phys. Rev. Letters **80** (1998), 4329–4332.

[7] R. Jozsa, Searching in Grover's algorithm, `quant-ph/9901021`, Jan. 1999.

[8] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proc. 35th IEEE Symposium on the Foundations of Computer Sci., 124–134, 1994.

[9] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comp. **26** (1997), 1484–1510.

[10] C. Zalka, Grover's quantum searching algorithm is optimal, `quant-ph/9711070`, Nov. 1997.