Quantum Searching, Counting and Amplitude Amplification by Eigenvector Analysis

Michele Mosca

Mathematical Institute
University of Oxford
24-29 St. Giles', Oxford OX1 3LB , U.K.

Centre for Quantum Computation
Clarendon Laboratory
Parks Road, OX1 3PU, U.K.

Abstract

Grover's quantum searching algorithm uses a quantum computer to find the solution to $f(x) = 1$ for a given function f. The algorithm, which repeatedly applies a certain operator G, has led to a major family of quantum algorithms for generating and counting solutions to $f(x) = 1$ for more general f. By studying the eigenvectors and eigenvalues of G and its variations, we arrive at simple algorithms and analyses for quantum searching, approximate counting, and amplitude amplification and estimation.

1 Introduction

Grover's original quantum searching algorithm [7] showed that we could find the unique solution to $f(x) = 1$ for a binary function f on a domain of size N with only $O(\sqrt{N})$ evaluations of the function f. Tighter bounds on the number of evaluations necessary were soon found, the restriction that f has a unique solution was subsequently removed [3], and other algorithms followed that also approximately counted the number of solutions to $f(x) = 1$.

Let us define the searching and counting problems more explicitly. Consider a function f which maps each element of a set X to either 0 or 1. For example, let X represent the set of the 3^n possible 3-colourings of an n-vertex graph $\mathcal{G}$, and $f(x) = 1$ if and only if the colouring x is a proper colouring of $\mathcal{G}$ (that is, no adjacent vertices are coloured with the same colour). Define X_1 to be the subset of X for which f evaluates to 1 (that is, the set of proper 3-colourings of $\mathcal{G}$), and X_0 to be the elements for which f evaluates to 0. Let us define j to be $|X_1|$, the number of elements in X_1.

The *generation* or *search* problem associated with f is to find an element x such that $f(x) = 1$, that is, an element of X_1. The *uniform generation* problem is to generate such an element uniformly at random from the set X_1. A more general problem is to *count* either *exactly* or *approximately* the number of solutions to $f(x) = 1$. To *approximately count* X_1 *with accuracy* ϵ means to output a number $\tilde{j}$ such that

$$(1 - \epsilon)j < \tilde{j} < (1 + \epsilon)j \tag{1}$$

where j is the number of elements in X_1. A *randomised approximation scheme (RAS)* for j is a randomised algorithm that for any real parameter $\epsilon > 0$ outputs a number $\tilde{j}$ such that with probability [1] 2/3 we have

$$(1-\epsilon)j \leq \tilde{j} \leq (1+\epsilon)j. \tag{2}$$

Grover presented an algorithm for quantum searching [7] and it was subsequently generalised [3, 4, 8]. These algorithms do not run in polynomial time (that is, in time polynomial in $\log N$, where $|X| = N$), but they do run in time roughly the square root of the running time for the best classical algorithm. By *running time* we are referring to the number of calls to the *oracle* or *black-box* U_f for the function f. This black-box for evaluating f reversibly computes $f(x)$ given input $|x\rangle$, usually by mapping $|x\rangle|b\rangle$ to $|x\rangle|b \oplus f(x)\rangle$, but in this paper we will assume the value of $f(x)$ is simply encoded in the phase [2] by mapping $|x\rangle$ to $(-1)^{f(x)}|x\rangle$. In [3] the idea of using the main operator in Grover's algorithm, let us call it G, the *Grover iterate*, to approximately count is first presented. Further details and related approaches have been discussed subsequently [9, 11]. The randomised approximation schemes suggested in [3, 11, 9], and herein run in time $O((1/\epsilon + \log\log(N))\sqrt{N/a})$. By *running time* we are referring to the number of calls to the operator U_f. We just count the number of calls to U_f since the lower bounds associated with these algorithms are in terms of these calls. It turns out in fact that for all the algorithms discussed here the number of other operations is usually[3] proportional to the number of calls to U_f, so this measure of running time is indeed representative of the running time of these algorithms in terms of all the elementary operations necessary. Each G makes one call to U_f, so the number of repetitions of G corresponds to the number of calls to U_f.

Analysing the eigenvectors and eigenvalues for this operator G provides a very simple analysis of the searching (Section 5) and counting (Section 4) algorithms, and insights into how to exploit the properties of G further. Estimation of certain eigenvalues gives a good estimate of the number of elements in X_1, so in the next section we will review some basic results in the estimation of phases, which will be very useful in analysing the counting algorithm to be presented in Section 4.

In [3], [4], and [8] it is observed that the searching algorithm is really just a special case of a more general algorithm referred to as *amplitude amplification* (Section 6). Further, the counting algorithm is a special case of *amplitude estimation*, which we can translate into a phase estimation.

2 Quantum Phase Estimation

Here we will review the relationship, as pointed out in [5], between the quantum Fourier transform and the estimation of phases.

Given any real number ω satisfying $0 \leq \omega < 1$ encoded in the phases of the superposition

$$\sum_{x=0}^{M-1} e^{2\pi i \omega x} |x\rangle, \tag{3}$$

[1] The number 2/3 can be replaced by any value, say $1-\delta$, that exceeds 1/2 by a constant. Given a particular RAS, we can apply a *bootstrapping scheme* (using the Chernoff bound) that applies the given RAS a number of times polynomial in $\log(1/\delta)$ and produces an ϵ-approximation with probability $1-\delta$. See, for example, Exercise 11.2 of [10].

[2] Note that this modified U_f can be realised with an oracle which maps $|x\rangle|b\rangle$ to $|x\rangle|b \oplus f(x)\rangle$, by setting $|b\rangle$ to $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

[3] The operator A we discuss later is typically a Hadamard transform or some other transform which can be efficiently implemented.

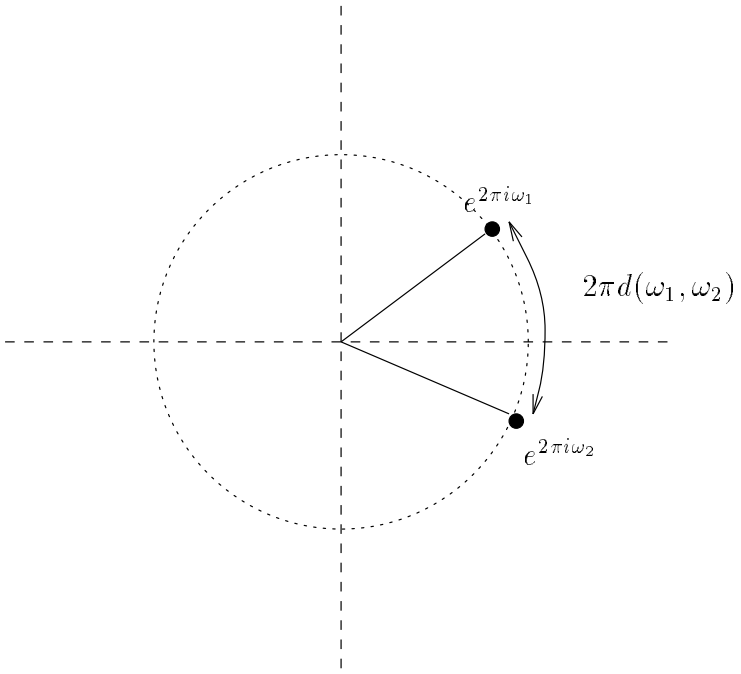

Figure 1: We define the distance between the real numbers ω_1 and ω_2, $d(\omega_1, \omega_2)$, to be the smallest real number d between 0 and 1/2 such that $e^{2\pi i(a-b)}$ equals one of $e^{2\pi id}$ or $e^{-2\pi id}$. In other words, it is length of the shortest path (scaled) along the unit circle from $e^{2\pi i\omega_1}$ to $e^{2\pi i\omega_2}$.

(we will usually ignore normalisation factors) applying the inverse quantum Fourier transform F_M^{-1} will map to a superposition

$$\sum_{x=0}^{M-1} \alpha_x \,|\, x\rangle \,, \tag{4}$$

which we will denote by $|\,\widetilde{\omega}\rangle$, where the amplitudes are concentrated near the values of x such that x/M are good estimates of ω. More precisely, we have the following lemmas (see [5]). Let $d(a, b)$ denote the distance between a and b modulo 1 (see figure 1).

Lemma 1 *The probability of observing $|\,x\rangle$ such that $d(\omega, x/M) \leq 1/2M$ is at least $4/\pi^2$. This fraction x/M corresponds to the best estimate of ω as a fraction of M.*

We can replace $4/\pi^2$ with any $1-\delta$, $0 < \delta < 1$, by increasing M by a factor of $1/2\delta + 1/2$.

Lemma 2 *For any positive integer $k < M$, the probability of observing an $|\,x\rangle$ such that $d(\omega, x/M) \leq k/2M$ is at least $1 - 1/(2k-1)$.*

Thus given an operator G with eigenvector $|\,\Psi\rangle$ and eigenvalue ω, we can estimate ω as follows. Prepare the state

$$\sum_{x=0}^{M-1} |\,x\rangle \,|\,\Psi\rangle \tag{5}$$

and apply G to $|\,\Psi\rangle$ x times when the first register is in state $|\,x\rangle$. This creates the state

$$\sum_{x=0}^{M-1} e^{2\pi i\omega x} \,|\,x\rangle \,|\,\Psi\rangle \,. \tag{6}$$

Applying F_M^{-1} to the first register gives the state $|\,\widetilde{\omega}\rangle \,|\,\Psi\rangle$, and has the property that when we observe the first register we get an estimate $\tilde{\omega}$ of ω.

Suppose we are just given G and $|\Psi\rangle$ such that $G|\Psi\rangle = e^{2\pi i\omega}|\Psi\rangle$. We have the following two lemmas.

Lemma 3 *For any $\epsilon > 0$, we can obtain an estimate $\tilde{\omega}$ of ω so that $d(\omega, \tilde{\omega}) < \epsilon$ with probability $\geq 2/3$, with $O(1/\epsilon)$ applications of G.*

Proof: The sufficiency of $\lceil 1/\epsilon \rceil$ applications [4] follows from the above analysis of the quantum Fourier transform. □

Lemma 4 *For ϵ between $1/N$ and $1/\sqrt{N}$, to obtain an estimate $\tilde{\omega}$ of ω so that $d(\omega, \tilde{\omega}) < \epsilon$ with probability $\geq 2/3$, requires $\Omega(1/\epsilon)$ applications of G.*

Proof: From Theorem 3.3 of [1] it follows that to decide, with error probability at most $1/3$, if f has fewer than M solutions to $f(x) = 1$, for $0 < M \leq N/2$, requires $\Omega(\sqrt{NM})$ calls to U_f. Lemma 5 tells us that by estimating ω_j, where j is the number of solutions to $f(x) = 1$, within $1/2\sqrt{M(N-M)}$ with error at most $1/3$ will solve this problem for us. The lower bound now follows by letting $M = \lceil \frac{1}{2N\epsilon^2} \rceil$. □

3 The Grover iterate and its properties

The quantum searching algorithm [7, 3] prepares the state

$$\sum_{x=0}^{N-1} |x\rangle$$

and then iterates the operator

$$G = -AU_0A^{-1}U_f$$

where A is any operator which maps $|0\rangle$ to $\sum_{x=0}^{M-1}|x\rangle$, U_0 maps $|0\rangle$ to $-|0\rangle$ and leaves the remaining $|x\rangle$ alone, and U_f maps $|x\rangle$ to $(-1)^{f(x)}|x\rangle$.
Recall that $j = |X_1|$, the number of solution to $f(x) = 1$, and $|X_0| = N - j$, and define

$$|X_1\rangle = \frac{1}{\sqrt{j}} \sum_{x \in X_1} |x\rangle, \text{ if } 0 < j \leq N \tag{7}$$

$$|X_0\rangle = \frac{1}{\sqrt{N-j}} \sum_{x \in X_0} |x\rangle, \text{ if } 0 \leq j < N \tag{8}$$

$$|\Psi_+\rangle = |X_1\rangle + i|X_0\rangle, \text{ and} \tag{9}$$

$$|\Psi_-\rangle = |X_1\rangle - i|X_0\rangle. \tag{10}$$

For $j = 0$ or N, define $|\Psi_+\rangle = |\Psi_-\rangle = \sum_{x \in X}|x\rangle$. Note that $|\Psi_+\rangle$ and $|\Psi_-\rangle$ are eigenvectors of G with respective eigenvalues

$$e^{2\pi i\omega_j} = 1 - \frac{2j}{N} + \frac{2i\sqrt{j(N-j)}}{N} \text{ and } e^{-2\pi i\omega_j} = 1 - \frac{2j}{N} - \frac{2i\sqrt{j(N-j)}}{N}.$$

Also note that

$$|\Psi_+\rangle + |\Psi_-\rangle = |X_1\rangle$$

[4] With $\lceil \frac{3}{2\epsilon} \rceil$ applications, we could boost the probability 2/3 to 4/5.

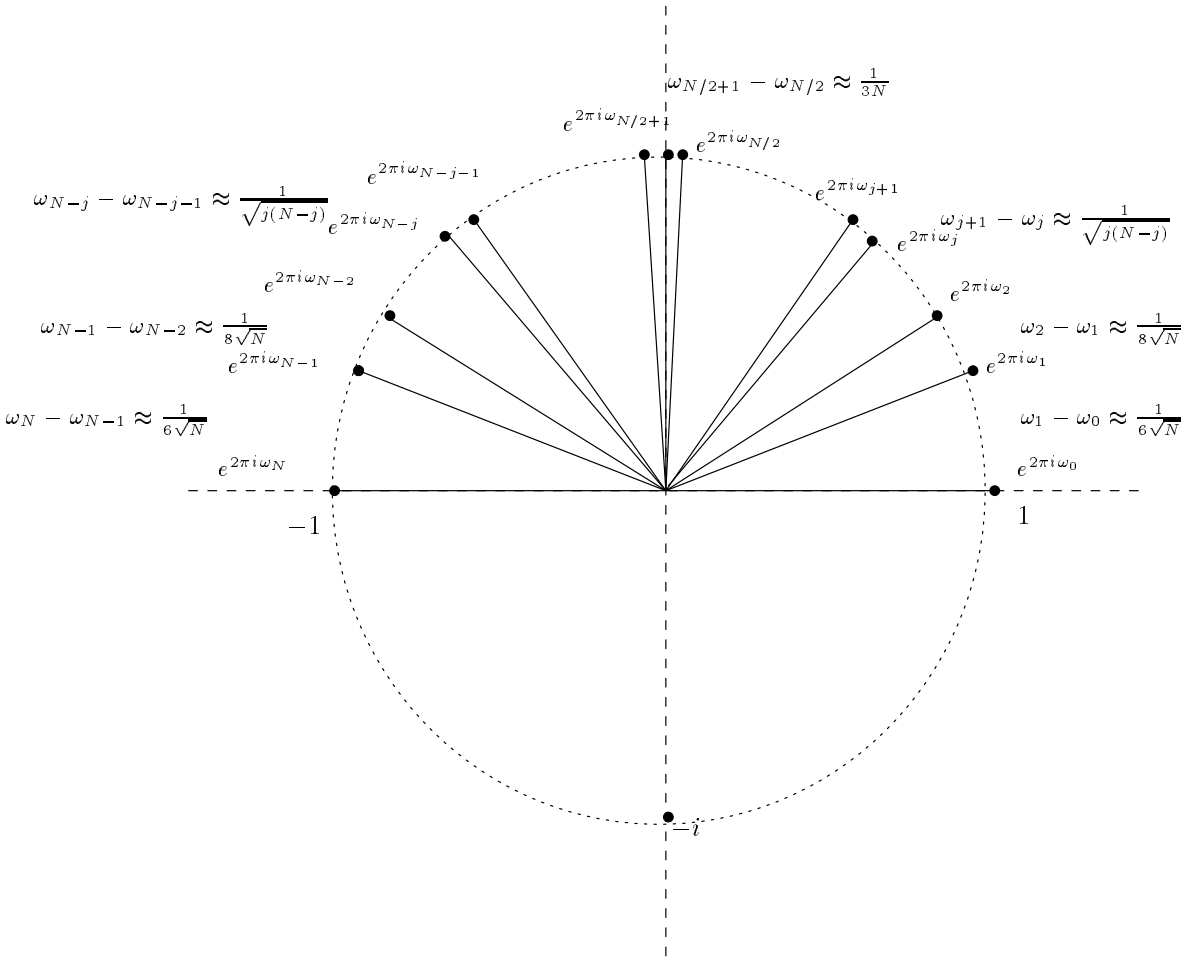

Figure 2: The eigenvalue of G on $|\Psi_+\rangle$ when there are j solutions is ω_j. Distinguishing a function f with j solutions requires a more precise estimate of ω_j as j gets closer to $N/2$.

which we seek since observing $|X_1\rangle$ solves the uniform generation problem for f. We start with the state $A|0\rangle$, which expressed in the eigenvector basis equals

$$e^{-2\pi i\theta_j}|\Psi_+\rangle + e^{2\pi i\theta_j}|\Psi_-\rangle\,.$$

where

$$e^{2\pi i\theta_j} = \left(\sqrt{\frac{j}{N}} + i\sqrt{\frac{N-j}{N}}\right).$$

Definition 1 *Define ω_j so that the eigenvalue of the eigenvector $|\Psi_+\rangle$ of $G = -AU_0A^{-1}U_f$ is $e^{2\pi i\omega_j} = (N-2j)/N + 2i\sqrt{j/N - (j/N)^2}$ (see figure 2.)*

Consequently,

$$2\pi\omega_j = \arccos(1-2j/N) = 2\sqrt{j/N} + O((j/N)^{3/2}). \tag{11}$$

It follows that $\theta_k = 1/4 - \omega_j/2$. To determine or estimate $j = |X_1|$, we will estimate the phase $2\pi\omega_j$. How accurately should we estimate ω_j to determine j? There are $N+1$ such ω_j for $j = 0, 1, \ldots N$, all between 0 and $1/2$, so by the Pigeon Hole Principle at least 2 of them are at most distance $1/2N$ apart and our phase estimation will have to be quite accurate to distinguish all of them: we would require on the order of N applications of G.
More precisely, we have the following lemmas which follow by looking at the derivative of the function in equation (11).

Lemma 5 *For any integer j satisfying $0 \leq j \leq N/2$,*

$$1/\sqrt{(j+1)(N-j-1)} \leq 2\pi|\omega_{j+1} - \omega_j|$$

and for $1 \leq j \leq N/2$,

$$2\pi|\omega_{j+1} - \omega_j| \leq 1/\sqrt{j(N-j)}.$$

Lemma 6 *For any integer j satisfying $0 \leq j \leq N/4$,*

$$2\pi|\omega_{2j} - \omega_j| \leq \sqrt{j/N}.$$

Combining Lemma 5 and Lemma 3 tells us that $\Omega(\sqrt{(j+1)(N-j+1)}$ are sufficient to distinguish ω_j from all of the other possible phases with high probability. The problem is that we do not know what j is ahead of time. However, if we first estimate j within a factor of $1+o(1)$, we will then be able to exactly determine j in time $O(\sqrt{(j+1)(N-j+1)})$. We will show how to get this lower bound later (see Corollary 3), as this permits us to exactly count the solutions to $f(x) = 1$ with high probability of correctness.

4 Quantum Counting

We are now ready to combine the facts about the eigenvectors and eigenvalues of G in Section 3 with the techniques in Section 2 to approximately count. The parameter M represents the number of times we will iterate G and thus corresponds to the running time of the algorithm in terms of evaluations of U_f. It is chosen depending on the quality of the estimate we seek. Start with the state

$$\sum_{x=0}^{M-1} |\, x\rangle\, A\,|\, 0\rangle = e^{-2\pi i\theta_j} \sum_{x=0}^{M-1} |\, x\rangle\,|\,\Psi_-\rangle + e^{2\pi i\theta_j} \sum_{x=0}^{M-1} |\, x\rangle\,|\,\Psi_+\rangle$$

apply G to the second register x times when the first register is in state $|\, x\rangle$ to produce

$$e^{-2\pi i\theta_j} \sum_{x=0}^{M-1} e^{-2\pi i\omega_j x}\,|\, x\rangle\,|\,\Psi_-\rangle + e^{2\pi i\theta_j} \sum_{x=0}^{M-1} e^{2\pi i\omega_j x}\,|\, x\rangle\,|\,\Psi_+\rangle\,.$$

Lastly apply F_M^{-1} to the first register to output

$$e^{-2\pi i\theta_j}\left|\,\widetilde{-\omega_j}\right\rangle\,|\,\Psi_-\rangle + e^{2\pi i\theta_j}\,|\,\widetilde{\omega_j}\rangle\,|\,\Psi_+\rangle\,.$$

Observing the first register will output (each with probability 1/2) either an estimate of ω_j, or of $1-\omega_j$, where there are j solutions to $f(x) = 1$ and $0 \leq \omega_j \leq 1/2$. When we observe an integer y between 0 and $M/2$, we will estimate ω_j with the number $\widetilde{\omega_j} = y/M$. If we observe an integer y between $M/2$ and M we will estimate ω_j with the number $1 - y/M$. It is easy to see that this protocol will produce an estimate of ω_j that is no worse (that is, the probability of getting an error less than ϵ does not increase for any $\epsilon > 0$) than if we only ever observed $|\,\widetilde{\omega_j}\rangle\,|\,\Psi_+\rangle$.

So let us assume that $\widetilde{\omega_j} = y/M$ is our estimate of ω_j. Define ϵ so that $\omega_j = y/M + \epsilon$. We know that

$$\cos(y/N) = \cos(\omega_j)\cos(-\epsilon) - \sin(\omega_j)\sin(-\epsilon).$$

With M applications of G we can obtain an estimate such that with probability at least $2/3$ we have $|\epsilon| \leq 1/M$ (see Section 2), and so $|\cos(\epsilon) - 1| < 1/2M^2$ and $|\sin(\epsilon)| < 1/M$. Using these bounds we get an estimate for j:

$$\tilde{j} = N(1 - \cos(y/M))/2, \tag{12}$$

and with probability at least $2/3$

$$|\tilde{j} - j| \leq |N - 2j|/4M^2 + \sqrt{j(N-j)}/M. \tag{13}$$

Some corollaries, (similar to ones pointed out in [3] and [11]), are the following.

Corollary 1 *If $M = \lceil c\sqrt{N} \rceil$, then with probability at least $2/3$ we will have*

$$|\tilde{j} - j| \leq 1/4c^2 + \sqrt{j}/c \in O(\sqrt{j}/c)$$

.

Corollary 2 *If $M = \lceil c\sqrt{N/(j+1)} \rceil$, then with probability at least $2/3$ we will have*

$$(1 - \epsilon)j \leq \tilde{j} \leq (1 + \epsilon)j$$

where $\epsilon = 1/(4c^2\sqrt{j}) + 1/c \in O(1/c)$.

We now get the following Lemma (as in [11]).

Lemma 7 *There is a quantum RAS for the number of solutions, j, to $f(x) = 1$, $0 \leq x < N$, with running time $O(1/\epsilon + \log\log(N))\sqrt{N/(j+1)})$.*

Proof(sketch): We first find a lower bound j_1 for j, with $4j_1 \geq j \geq j_1$. One scheme for finding such a lower bound j_1 for j is to first test if $j \geq N/4 - 1$. If not, then test if $j \geq N/8 - 1$, and so on, testing if $j \geq N/2^k - 1$ until we get a positive answer (this test combines Corollary 2 and Lemma 6). By applying the *bootstrapping* methods [10] mentioned earlier, we repeat the test (which uses $O(\sqrt{2^k})$ applications of G) $O(\log\log(N))$ times and guarantee that each of these tests gives a false "YES" with probability at most $1/6\log(N)$. When we do get a positive answer to "Is $j \geq N/2^k - 1$?", it will be a true lower bound with probability at least $5/6$. We can then estimate ω_j with $M = O(\frac{1}{\epsilon}\sqrt{\frac{N}{j_1+1}}) = O(\frac{1}{\epsilon}\sqrt{\frac{N}{j+1}})$ applications of G so that with probability at least $4/5$ we have an ϵ-approximation of j. □
Corollary 1 gives us the bound on j that we need to carry out exact counting (combining Lemma 4 and Lemma 5).

Corollary 3 *Given $G = -AU_0A^{-1}U_f$, where f has j solutions to $f(x) = 1$, with $\Theta(\sqrt{(j+1)(N-j+1)})$ applications of G we can distinguish ω_j and correctly determine j with probability at least $2/3$.*

The fact that $O(\sqrt{jN})$ applications sufficed was pointed out in [3].

5 Quantum Searching

The quantum searching algorithm can be succinctly analysed as follows. Start in the state

$$A\,|\,0\rangle = \exp(-2\pi i\theta_j)\,|\,\Psi_+\rangle + \exp(2\pi i\theta_j)\,|\,\Psi_-\rangle$$

and apply G to this state k times to produce

$$\exp(2\pi i(k\omega_j - \theta_j))\,|\,\Psi_+\rangle + \exp(-2\pi ik(\omega_j - \theta_j))\,|\,\Psi_-\rangle$$

and observe. The number of repetitions k will correspond to the running time of the algorithm since each G uses U_f once. Since we want to observe $|\,X_1\rangle = |\,\Psi_+\rangle + |\,\Psi_-\rangle$, we want to align the phases so that the relative phase between the two eigenvectors is 0, that is, $4\pi(k\omega_j - \theta_j)$ is 0 or some other multiple of 2π. Conversely, $|\,X_0\rangle = |\,\Psi_+\rangle - |\,\Psi_-\rangle$, so we want $k\omega_j - \theta_j$ to be far from any fraction the form $\frac{1}{4} + \frac{1}{2}\mathbf{Z}$. The probability of observing an element of X_1 is in fact equal to $\frac{1+\cos(2\pi\delta)}{2}$ where $\delta = 2(k\omega_j - \theta_j)$. Given the relation between θ_j and ϕ_j, this is equivalent to finding a k such that $\cos(2\pi(k + 1/2)\phi_j)$ is close to 0.

When j is known, this is easy. For example, suppose $j = 1$, then $\cos(2\pi\omega_1) = 1 - 2/N$ and so ω_1 is roughly $1/\pi\sqrt{N}$ and $e^{2\pi i\theta_j} = \sqrt{\frac{1}{2N}} + i\sqrt{1 - \frac{1}{2N}}$ so θ_j is roughly $1/4$. Thus we should choose k to be roughly $\frac{\pi}{4}\sqrt{N}$.

Consider, also, as done in [3], the case that $j = \frac{N}{4}$. Then $\cos(2\pi\theta_j) = \frac{1}{2}$ implying $\theta_j = \frac{1}{6}$, and $\cos(2\pi\omega_j) = \frac{1}{2}$ implying $\omega_j = \frac{1}{6}$. So we want $k = 1$ which means we get $|\,X_1\rangle$ with exactly one iteration of G.

When j is not known, it is not as simple. One idea is to estimate ω_j using the techniques of the previous section, and to use this to approximate θ_j and then pick the number of repetitions k so that $k\omega_j - \theta_j$ is likely to be close to 0 and far from $\pm 1/4$.

We will describe an alternative approach, different from the one presented in [3] but with the same expected running time of $O(\sqrt{N/(j+1)})$ applications of U_f.

Note that when we approximately count and produce the state

$$e^{-2\pi i\theta_j}\,|\,\widetilde{\omega_j}\rangle\,|\,\Psi_+\rangle + e^{2\pi i\theta_j}\,\left|\,\widetilde{-\omega_j}\right\rangle\,|\,\Psi_-\rangle$$

we could also observe the second register and test the answer. Note that as $|\,\widetilde{\omega_j}\rangle$ and $\left|\,\widetilde{-\omega_j}\right\rangle$ become better and better estimates of ω_j and $-\omega_j$, they become more and more orthogonal (provided $j \neq 0, N$), and the amount of interference between $|\,\Psi_+\rangle$ and $|\,\Psi_-\rangle$ diminishes. Observing either $|\,\Psi_+\rangle$ or $|\,\Psi_-\rangle$ will reveal an element of X_1 with probability $1/2$.

If we approximate ω_j using $4M$ iterations of G where $1/M < \omega_j$ then the magnitude of the amplitude of the best estimate y for ω in $|\,\widetilde{\omega_j}\rangle$ will be at least $2/\pi$ and in $\left|\,\widetilde{-\omega_j}\right\rangle$ it will be at most [5] $1/\sqrt{15}$, and thus the size of the amplitude of $|\,y\rangle\,|\,X_1\rangle$ in

$$|\,\widetilde{\omega}\rangle\,|\,\Psi_+\rangle + \left|\,\widetilde{-\omega}\right\rangle\,|\,\Psi_-\rangle$$

will be at least $2/\pi - 1/\sqrt{15} \geq 0.378$. We thus have a probability of observing a solution bounded below by

$$p = |2/\pi - 1/\sqrt{15}|^2/2 \geq 0.0716.$$

Our strategy is thus to set $M = 1$ and go through the following steps.

[5] If $y/4M$ corresponds to the best estimate of ω_j as a fraction of $4M$, then as an estimate of $-\omega_j$ it is off by at least $8/M$ and by Lemma 2 it will be observed with probability at most $1/15$.

Step 1: Using M applications of G compute

$$|\widetilde{\omega}\rangle|\Psi_+\rangle + \left|\widetilde{-\omega}\right\rangle|\Psi_-\rangle$$

and observe the second register. Test the observed $|x\rangle$ to see if $f(x) = 1$. If $f(x) = 1$, then stop. Otherwise repeat up to 10 times.
Step 2: If after 10 repetitions no solution has been found, double M and return to Step 1.

Once $M > 1/\omega_j$, the probability of observing a solution in Step 1 is at least

$$1 - (1-p)^{10} > 1/2.$$

This implies that the expected running time of this algorithm is $O(\sqrt{N/(j+1)})$ applications of G.

6 Amplitude Amplification and Exact Searching

In [4] and [8] we see that we can in fact replace A with any transformation which maps $|0\rangle$ to $\sqrt{a}|X_1\rangle + \sqrt{b}|X_0\rangle$, where $|X_1\rangle$ is *any* superposition (of norm 1) of basis states $|x\rangle$ satisfying $f(x) = 1$ and $|X_0\rangle$ is *any* superposition (of norm 1) of basis states $|x\rangle$ satisfying $f(x) = 0$, and a and b are positive reals satisfying $a + b = 1$.
We can easily show that the eigenvectors of $G = -AU_0A^{-1}U_f$ have the same form

$$|\Psi_+\rangle = |X_1\rangle + i|X_0\rangle$$

$$|\Psi_-\rangle = |X_1\rangle - i|X_0\rangle$$

and eigenvalues

$$e^{2\pi i\omega_a} = 1 - 2a + 2i\sqrt{ab}$$
$$e^{-2\pi i\omega_a} = 1 - 2a - 2i\sqrt{ab}$$

(ω_j from the previous section would correspond to $\omega_{j/N}$ here) and

$$A|0\rangle = e^{-2\pi i\theta_a}|\Psi_+\rangle + e^{2\pi i\theta_a}|\Psi_-\rangle$$

where

$$e^{2\pi i\theta_a} = \sqrt{a} + i\sqrt{b}$$

and $\theta_a = 1/4 - \omega_a/2$.
Thus, knowing a we can apply the same searching technique described in Section 5 to find solutions to $f(x) = 1$ with only an expected $O(\sqrt{1/a})$ applications of G. We can use the same techniques of Section 4 to approximate a and the same strategy of Section 5 to search for a solution when we do not know a. When we do know a we know exactly how many applications of G we should use. We can also alter G so that the ideal number, M, of applications is an integer, making the search exact (this is done for $M = 1$ in [4] and [6]). Here we will describe another way of doing it [6].

Step 1: Knowing a we know ω_a and θ_a, so define $k = \lceil \theta_a/\omega_a \rceil$.
Step 2: Solve for $a' < a$ such that $k = \theta_{a'}/\omega_{a'}$.

[6] This fact was pointed out to me independently by H. Buhrman, W. van Dam, and P. Høyer in November 1997.

Step 3: Add an additional qubit in state $|0\rangle$ to the original register containing only $|0\rangle$s. Replace A with $\overline{A}$ which maps the additional $|0\rangle$ qubit to $\sqrt{1-a'/a}\,|0\rangle + \sqrt{a'/a}\,|1\rangle$ and applies A to original register. Further, replace f with a function $\overline{f}$ which also takes the additional bit as input, and outputs 0 if the additional qubit is in state $|0\rangle$, and outputs $f(x)$ if the additional qubit is in state $|1\rangle$ and the original register is in state $|x\rangle$. The operator $U_{\overline{f}}$ can be implemented as a controlled-U_f.

The output of $\overline{A}$ is now of the form

$$\sqrt{a'}\left|\overline{X_1}\right\rangle + \sqrt{b'}\left|\overline{X_0}\right\rangle$$

where $\left|\overline{X_1}\right\rangle$ and $\left|\overline{X_0}\right\rangle$ correspond to the superposition of basis states containing solutions to $\overline{f}(x) = 1$ and $\overline{f}(x) = 0$ respectively. It now follows that $k = \theta_{a'}/\omega_{a'}$ applications of

$$G = -\overline{A}U_0\overline{A}^{-1}U_{\overline{f}}$$

will produce exactly $\left|\overline{X_1}\right\rangle = |1\rangle\,|X_1\rangle$ thereby giving us a uniform generator with no error.

7 Acknowledgments

Many thanks to Artur Ekert for many helpful discussions and for emphasising to me the relationship between quantum computing and interferometry. Thanks also to Alain Tapp, Peter Høyer, and Richard Cleve for helpful discussions.

A The remaining eigenvectors and starting from arbitrary states

In addition to the eigenvectors $|\Psi_+\rangle$ and $|\Psi_-\rangle$ there are of course $N-2$ other eigenvectors. Exactly $N-j-1$ of them, spanned only by elements of X_0, have eigenvalue -1 and $j-1$ of them, spanned only by elements of X_1, have eigenvalue 1. It is easy to find a spanning set of these eigenvectors.

One interesting use of this fact is to study the effect of applying the quantum searching algorithms with arbitrary input states. The optimal number of applications G before observing was studied in detail in [2] (by different methods). Applying G to any of the $j-1$ eigenvectors with eigenvalue 1 will only invert the sign. Applying G has no effect on the eigenvectors with eigenvalue 1, and flips the sign in front of the eigenvectors with eigenvalue -1. So unless the amplitudes of $|\Psi_+\rangle$ and $|\Psi_-\rangle$ in the initial state are significant, Grover's algorithm will be of little help in searching. Further, if we start off with the state

$$ce^{-2\pi i\theta}\,|\Psi_+\rangle + de^{2\pi i\theta}\,|\Psi_-\rangle$$

where c and d are positive reals, then to maximise the amplitude of the states $|x\rangle$ with $f(x) = 1$ we should again apply G to the starting state k times where $\theta - k\omega_j$ is close to an integer multiple of $1/2$.

References

[1] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, "Quantum lower bounds by polynomials", preprint, (see also http://xxx.lanl.gov/quant-ph/9802049).

[2] David Biron, Ofer Biham, Eli Biham, Markus Grassl and Daniel A. Lidar, " Generalized Grover Search Algorithm for Arbitrary Initial Amplitude Distribution" , to appear in *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications*, (1998) (see also http://xxx.lanl.gov/abs/quant-ph/9801066).

[3] Michel Boyer, Gilles Brassard, Peter Høyer and Alain Tapp (1996), "Tight Bounds on Quantum Searching", *Proceedings of the Fourth Workshop on Physics and Computation – PhysComp '96* (1996), 36–43. Final version to appear in *Forschritte Der Physik*.

[4] Gilles Brassard and Peter Høyer, "An exact quantum polynomial-time algorithm for Simon's problem", *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems – ISTCS '97* (1997), IEEE Computer Society Press, 12–23.

[5] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum Algorithms Revisited",*Proc. R. Soc. Lond. A* (1998) **454**, 339-354.

[6] Dong Pyo Chi and Jingsoo Kim, "Quantum database searching by a single query", to appear in *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications*, (1998), (http://xxx.lanl.gov/abs/quant-ph/9708005).

[7] L. Grover, "A fast quantum mechanical algorithm for database search", *Proc. 28th Annual ACM Symposium on the Theory of Computing* (1996), ACM Press New York, 212–219.

[8] Lov K. Grover, "A framework for fast quantum mechanical algorithms", to appear in *Proc. 30th Annual ACM Symposium on the Theory of Computing* (1998).

[9] Michele Mosca, lecture entitled "Quantum Computer Algorithms and Interferometry", *BRICS Workshop on Algorithms in Quantum Information Processing '98*, Aarhus, Jan. 1998.

[10] Rajeev Motwani and Prabhakar Raghavan, *Randomized Algorithms*, Cambridge University Press, 1995.

[11] Alain Tapp, lecture entitled "Quantum Counting", *BRICS Workshop on Algorithms in Quantum Information Processing '98*, Aarhus, Jan. 1998. Joint work with G. Brassard and P. Høyer, to appear.