Reflections in Hilbert Space I: Grover's search

James Daniel Whitfield[*][†]

March 20, 2012

> We dance around in a ring and suppose,
> But the Secret sits in the middle and knows.
> *–Robert Frost*

The effect of using computational laws based in quantum physics can result dramatic differences from the classical counterpart and in this series of lectures we'll explore a class of quantum algorithms that are quadratically faster than the classical counterparts based on bi-involutions.

An involution, or a reflection, is an operation that is its own inverse. An operator, A is an involution if $A^2 = \mathbf{1}$. This is the generalization of reflections. Involutions are operations of the form

$$R = 2\mathbf{P} - \mathbf{1} \tag{1}$$

where $\mathbf{P}$ is some projector ($\mathbf{P}^2 = \mathbf{P}$). These form the basis for the classical Householder transformation for obtaining the QR decomposition which is essentially the Gram-Schmidt procedure performed as a matrix decomposition.

Involutions have found wide usage in quantum computation beginning with the Grover's search providing quadratically faster performance over classical algorithms. Many of these examples are based on involutions. The speed-up speed limit was first codified by [1] which stated the difference between classical and quantum computation was at most quadratic for black box oracles. While a large part of quantum algorithms have produced quadratic speed ups, notable exceptions are found in hidden subgroup problems such as phase estimation and the quantum Fourier transform.

Grover's search was the first devised and accordingly it will be discussed first. The motivation and an explanation of its advantage is given graphically and algebraically. A few comments on optimality are given at the close.

[*] Columbia University, NEC Labs America, Institute for Scientific Interchange

[†] *Current address:* Institute for Scientific Interchange, Via Alassio 11/c, 10126 Torino - Italy

1 Grover's search

Grover's quantum search algorithm, is one of the most important applications of quantum information science to date. Grover developed this algorithm in 1996 [2, 3] and remarkably it was optimal for the task it set out to solve. This task was to identify a marked state among $N = 2^n$ unsorted items using the fewest number of calls to an oracle. The canonical example is that of finding a particular name given a phone number and a phone book.

Database search, classical results, and oracles

The database search problem is to find a marked state among $N = 2^n$ unsorted items. The canonical example is that of finding a particular name when given a phone number and a phone book.

Classically, if we want to find items from a set W it will take $O(N)$ time to search if W only has one element. To formalize these ideas suppose for database D we have function $f : D \to \{0, 1\}$ defined as

$$f(x) = \begin{cases} 1, & x \in W \\ 0, & x \notin W \end{cases} \tag{2}$$

In this section, we only discuss the case where one item is marked. To find marked item s, we will have to apply $f(x)$ to each $x \in \{0, 1, \cdots, N-1\}$. On average this will take $N/2$ tries and the worst case it will take $N - 1$ tries. In other words, as the database increases in size the time required to search it will scale linearly with the size of the database. The advantage of the quantum algorithm is only in the case of unsorted databases. If a database can be sorted according to some enumeration, the quantum speed-up is only a constant [4]. If the classical algorithm is allowed to spend $O(N \log N)$ time to structure the database searches such as binary search can be performed in $O(\log(N))$ queries and in some cases better.

The scaling of the queries was given the using standard notation for asymptotic analysis. The notation, $f(x) = O(g(x))$, implies that f is dominated by g at asymptotically large values of x. To indicated that f is asymptotically larger than g, we write $f(x) = \Omega(g(x))$. If f is dominated by and dominates function g, we write $f(x) = \Theta(g(x))$. This notation is used throughout the thesis.

The Grover quantum search algorithm uses discrete steps to evolve the uniform superposition of all states to the desired state in approximately $\sqrt{N}$ steps. Beginning the quantum search at the uniform superposition is different from starting from the uniform probability distribution due to the coherences between the states. In the classical search, one must guess randomly which item to query. The quantum algorithm proceeds by using the oracle to change the sign of marked items as explained in the next section. A second operator reflects each amplitude about the mean amplitude and is examined in Section 1. The combination of the two operations is called a Grover operation (Section 1) and we'll see that this operator acts non-trivially in the two-dimensional space which is spanned by the initial state and the answer state. As the composition of two reflections is a rotation, the Grover operator has a quaint geometrical interpretation which we will see in the final section.

Phase shift oracle

Using an oracle that computes function f of (2), we would like to create an operator that changes the sign of marked items. First we give the form of a unitary oracle, second we show how we can pick input states to create the desired operation.

Now suppose we had an oracle U_o that operates as $U_o|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$. The reason for the oracle to be implemented as a two qubit operation is that we wish it to be unitary. Each unitary operation is invertible so each input must map to a unique output (in other words: the operation must be injective or one-to-one). For functions that aren't injective using extra space to keep the input allows the operation to be reversible [5]. In our case, U_o calculates $f(x)$ corresponding to (2).

Note that if we let the second qubit, $|y\rangle$, be the state $|X-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ then oracle changes the sign of an input vector if it is a marked state. Observe:

$$U_o\left(\frac{|x\rangle|0\rangle - |x\rangle|1\rangle}{\sqrt{2}}\right) = \left(\frac{|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}}\right).$$

Temporarily ignoring normalization, either $f(x) = 0$ and the output state is $|x\rangle(|0\rangle - |1\rangle)$ or $f(x) = 1$ and output state is $|x\rangle(|0\rangle - |1\rangle)$. Therefore, we write

$$U_o|x\rangle|X-\rangle = (-1)^{f(x)}|x\rangle|X-\rangle.$$

If the second qubit is always in state $|X-\rangle$, then the sign of answer state, $|w\rangle$, changes and the other $N-1$ basis vectors are left unchanged. Thus,

$$U_o = -R_w = \mathbf{1} - 2|w\rangle\langle w| \tag{3}$$

Here R_w is a reflection about the $|w\rangle$ state.

Reflection about the mean

The oracle followed by a second operator called a diffusion operator by Grover [2, 3] completes a single Grover iteration. Denote the diffusion operator as U_{mean} and it is defined as:

$$U_{mean} = R_s = 2|s\rangle\langle s| - \mathbf{1}. \tag{4}$$

The state $|s\rangle$ is selected as to have some overlap with all vectors including those of the answer space. We pick:

$$|s\rangle = \mathsf{H}^{\otimes n}|0\cdots 0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle, \tag{5}$$

Here $N = 2^n$ is the normalization constant assuming there are n qubits in the array.

The operator U_{mean} with s defined as in (5) is called an inversion about the mean. First, define the mean of $|v\rangle$ as:

$$\bar{v} = \sum_k \frac{\langle k|v\rangle}{N}.$$

Starting from $|s\rangle\langle s|$, inserting the resolution of the identity in the same basis as the answer state w, $\mathbf{1} = \sum |i\rangle\langle i|$,

$$\begin{aligned}
|s\rangle\langle s|v\rangle &= \sum_{i=0}^{N-1} |s\rangle\langle s|i\rangle\langle i|v\rangle = \sum_i \left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle\right)\left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\langle k|\right)|i\rangle\langle i|v\rangle \quad (6)\\
&= \frac{1}{N}\sum_{ijk}|j\rangle\langle k|i\rangle\langle i|v\rangle = \frac{1}{N}\sum_{ijk}\delta_{ki}\langle i|v\rangle|j\rangle = \sum_j \frac{\sum_i\langle i|v\rangle}{N}|j\rangle \quad (7)\\
&= \sum_j \bar{v}|j\rangle \quad (8)
\end{aligned}$$

Putting it all together, U_{mean} performs the following operation: $U_{mean}|v\rangle \rightarrow \sum_j(2\bar{v} - v_j)|j\rangle$ with $v_j \equiv \langle j|v\rangle$. Looking at figure 1, this operation has the form of an inversion.

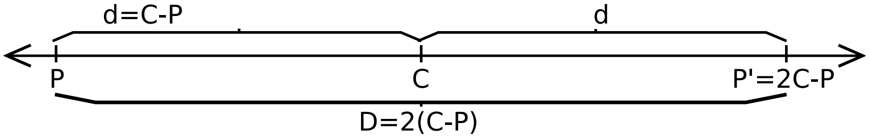

Figure 1: The reflection of point P about point C results in point P'. The distance from P to C is $d = C - P$ and the distance from P to P' is $D = 2d = 2(C - P)$. If follows that $P' = P + 2(C - P) = 2C - P$. In equation (8), the average amplitude $\bar{v}$ becomes the center C and v_j can be identified as P.

The Grover operator and its two-dimensional operation

The Grover operator is given by

$$G = U_{mean}U_o = -R_sR_w. \tag{9}$$

The Grover search works by evolving the state s toward the answer state $|w\rangle$ using only a two-dimensional space. This is because the Grover operator does not evolve state outside of this two-dimensional space. The states that have no overlap with $|s\rangle$ and $|w\rangle$ are eigenstates of G with eigenvalue -1. Using equations (3) and (4) to expand G as:

$$G = 2|s\rangle\langle s| + 2|w\rangle\langle w| - 4\langle s|w\rangle|s\rangle\langle w| - \mathbf{1}. \tag{10}$$

If $|t\rangle$ has no overlap with w or s then $G|t\rangle = -|t\rangle$. Although $|s\rangle$ is a superposition of all states in the database basis, the vectors w and s cannot span the entire space. An example of such a vector t is any superposition of an even number of states with alternating sign is orthogonal to $|s\rangle$, for instance $|t\rangle = \mathsf{H}^{\otimes n}|1\cdots 1\rangle = (1/\sqrt{N})\sum(-1)^x|x\rangle$. If the superposition t does not include the answer state, then t is in the $N-2$ dimensional space orthogonal to span$\{|w\rangle, |s\rangle\}$.

The trajectory generated by repeated application of G on $|s\rangle$ explores this two-dimensional space of span$\{|w\rangle, |s\rangle\}$. To use an orthonormal basis, we construct a normalized state $|r\rangle$ using a method like Gram-Schmidt decomposition [6].

$$|r\rangle = \sqrt{\frac{N}{N-1}}|s\rangle - \sqrt{\frac{1}{N-1}}|w\rangle = \sqrt{\frac{1}{N-1}}\sum_{x\neq w}|x\rangle. \tag{11}$$

$|r\rangle$ is orthogonal to $|w\rangle$ and span$\{|w\rangle, |r\rangle\}$ =span$\{|w\rangle, |s\rangle\}$. Now rewrite the initial superposition in this basis as $|s\rangle = \sqrt{(N-1)/N}|r\rangle + N^{-1/2}|w\rangle$. Now consider the effect of G on $|r\rangle$ using (10) and (11) yielding,

$$\begin{aligned} G|r\rangle &= (2|s\rangle\langle s| + 2|w\rangle\langle w| - 4\langle s|w\rangle|s\rangle\langle w| - \mathbf{1})|r\rangle & (12)\\ &= \left(1-\frac{2}{N}\right)|w\rangle + \frac{2\sqrt{N-1}}{N}|r\rangle & (13)\\ &= \cos\theta|w\rangle + \sin\theta|r\rangle & (14)\end{aligned}$$

Assuming that G is real, we know that G is unitary if and only if its two-dimensional matrix representation on the w, r space takes the following form[6]:

$$G = T(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}, \tag{15}$$

with θ defined through (14), assuming a matrix representation of arbitrary state $|v\rangle$ is given by:

$$|v\rangle = \begin{bmatrix} \langle w|v\rangle \\ \langle r|v\rangle \end{bmatrix}$$

To characterize initial state s, let ϕ_r as the angle between $|s\rangle$ and $|r\rangle$. By inserting this angle of rotation into a rotation matrix we can rotate a vector beginning in state $|r\rangle$ to state $|s\rangle$, and the following equation is satisfied:

$$\begin{bmatrix} \cos\phi_r & \sin\phi_r \\ -\sin\phi_r & \cos\phi_r \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \sin\phi_r \\ \cos\phi_r \end{bmatrix} = \begin{bmatrix} \langle w|s\rangle \\ \langle r|s\rangle \end{bmatrix}. \tag{16}$$

From (11) we derive that

$$\begin{aligned} |s\rangle &= \sqrt{\frac{N-1}{N}}|r\rangle + \sqrt{\frac{1}{N}}|w\rangle = \sqrt{\frac{1}{N}}\begin{bmatrix} 1 \\ \sqrt{N-1} \end{bmatrix} & (17)\\ &= \cos\phi_r|r\rangle + \sin\phi_r|w\rangle & (18)\end{aligned}$$

and it follows $\cos\phi_r = \sqrt{(N-1)/N}$ and $\sin\phi_r = \sqrt{1/N}$.

Using geometric arguments we can show that

$$2\phi_r = \theta. \tag{19}$$

One proof using the double angle formula and (14) is given by:

$$\begin{aligned} \sin\ 2\phi_r &= 2(\sin\phi_r)(\cos\phi_r) && (20) \\ &= 2\sqrt{\frac{N-1}{N}}\sqrt{\frac{1}{N}} && (21) \\ &= \sin\theta && (22) \end{aligned}$$

A summary of these geometric results is given in Fig. 2.

Thus, after k iterations, the initial state with angle ϕ_r has been rotated to a vector characterized by angle $\Phi_k = k(2\phi_r) + \phi_r$. When Φ_k is close to $\pi/2$, we have accomplished to goal of creating high overlap with the answer. So if N is large then the state $|s\rangle$ is approximately $|r\rangle$. Then we will need the following to be approximately satisfied.

$$\begin{aligned} \Phi_k = \frac{\pi}{2} &= (2k+1)\phi_r && (23) \\ \frac{\pi}{2\phi_r} &= 2k+1 && (24) \\ k &= \frac{\pi}{4\phi_r} - \frac{1}{2} && (25) \end{aligned}$$

From (17) and (18) we have that $\sin\phi_r = 1/\sqrt{N}$. Using the small angle approximation, we say $\phi_r \approx 1/\sqrt{N}$. Substituting into (25) we have:

$$k = \frac{\pi}{4}\sqrt{N} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{N}. \tag{26}$$

Hence, the algorithm obtains the answer with high probability after a number of iterations that is quadratic in N.

Lower bound for Grover's search

Briefly, note that Grover's search is optimal with respect to the number of oracle calls it makes [7, 1]. Historically, its proof is important because of the technique that was used in the proof: the adversary method.

Grover's algorithm, which relies on the oracle to find a marked item in time $O(\sqrt{N})$ can be proven optimal by changing a critical subset of oracle outputs such that the errors cannot be detected in time $\Omega(\sqrt{N})$ [1]. This lower bound proof technique is known as the adversary method. The idea is an adversary makes modification of the true oracle on a subset of critical answers to trick you. The key is that the quantum algorithms that access the oracle less than some lower bound are not sensitive to critical changes of the oracle. For Grover's search problem if the oracle is accessed less than $O(\sqrt{N})$ times then for any algorithm (Grover or otherwise), there is an oracle for which the algorithm will

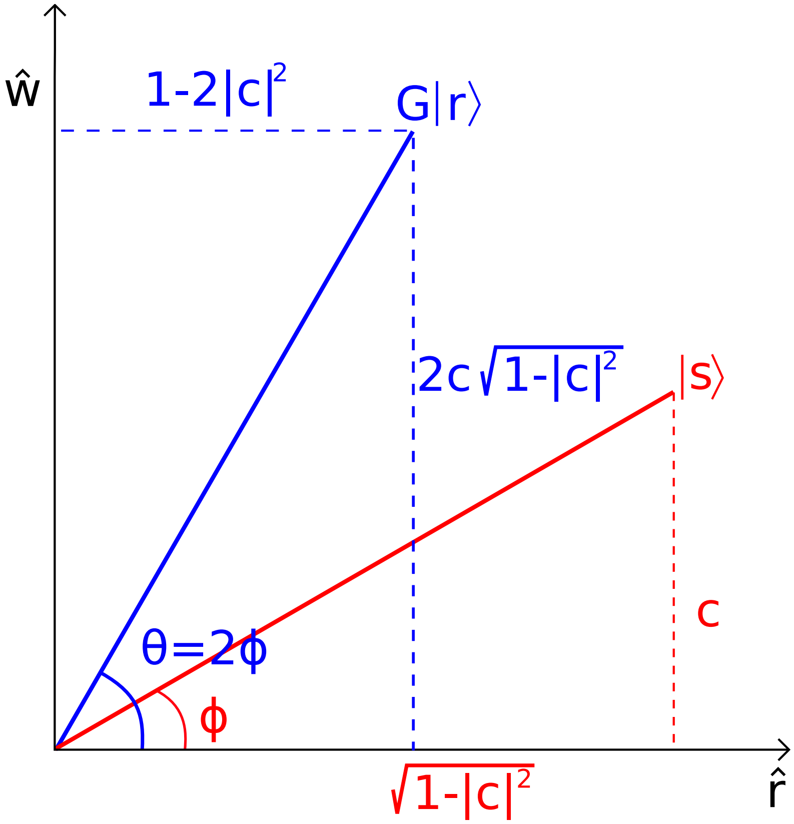

Figure 2: **Grover's search in the plane of the initial and target states.** To summarize equations (14), (17), (18) and (22), we depict the states $G|r\rangle$ and $|s\rangle$. The answer state $|w\rangle$ is parallel to the ordinate axis. The abscissa is the orthogonal state $|r\rangle$ defined in (11). The uniform superposition of all states is $|s\rangle$ and is characterized in (18) and (17). If ϕ_r is the angle between the $\hat{r}$ axis and $|s\rangle$ then the Grover operator G performs a rotation of $2\phi_r$. After $O(\sqrt{N})$ applications of the G to the state $|s\rangle$, there is high probability that measurement will result in marked state w.

fails to distinguishing the desired object from any other with high probability [1]. This technique, along with the polynomial method [8] and its many generalizations, are the two main techniques for proving lower bounds in the quantum query model.

In the next lecture, we move on to Szegedy's scheme for Markov chain quantization. Szegedy's scheme is an important generalization of Grover's algorithm because it simplifies access to the promised quadratic speed up of quantum computation. Finally, Szegedy's scheme can be applied to understanding discrete-time quantum walks and this is examined in the last section.

References

[1] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Computing*, 26(5):1510–1524, 1997.

[2] L. K. Grover. A fast quantum mechanical algorithm for database search. *Proc. 28th ACM Symp. on Theory of Comp. (STOC '96)*, page 212, 1996. Also see arxiv:quant-ph/9605043.

[3] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325, 1997.

[4] A. M. Childs, A. J. Landahl, and P. A. Parrilo. Quantum algorithm for ordered search problem via semidefinite programming. *Phys. Rev. A*, 75:032335, 2007.

[5] C. H. Bennett. Logical reversibility of computation. *IBM J. Res. Develop.*, 17, 1973.

[6] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge University Press, 2005.

[7] J. Preskill. Lecture notes for quantum computation. Available at .

[8] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proceedings of FOCS' 98*, pages 352–361, 1998.