

Grover's Quantum Search Algorithm

Samuel J. Lomonaco, Jr.

ABSTRACT. This paper is a written version of a one hour lecture given on Lov Grover's quantum database search algorithm. It is based on [5], [6], and [11].

CONTENTS

1. Problem definition
2. Two examples
3. The quantum mechanical perspective
4. Properties of the inversion $I_{|\psi\rangle}$
5. The method in Lov's "madness"
6. Summary of Grover's algorithm
7. An example of Grover's algorithm

References

1. Problem definition

We consider the problem of searching an unstructured database of $N = 2^n$ records for exactly one record which has been specifically marked. This can be rephrased in mathematical terms as an oracle problem as follows:

2000 *Mathematics Subject Classification*. Primary 81P68; Secondary 81-01.

Key words and phrases. Grover's algorithm, database search, quantum computation, quantum algorithms.

This work was partially supported by Army Research Office (ARO) Grant #P-38804-PH-QC, by the National Institute of Standards and Technology (NIST), by the Defense Advanced Research Projects Agency (DARPA) and Air Force Materiel Command USAF under agreement number F30602-01-0522, and by the L-O-O-P Fund. The author gratefully acknowledges the hospitality of the University of Cambridge Isaac Newton Institute for Mathematical Sciences, Cambridge, England, where some of this work was completed. I would also like to thank the other AMS Short Course lecturers, Howard Brandt, Dan Gottesman, Lou Kauffman, Alexei Kitaev, Peter Shor, Umesh Vazirani and the many Short Course participants for their support. (Copyright 2000.)

©0000 (copyright holder)

Label the records of the database with the integers

$$0, 1, 2, \dots, N - 1,$$

and denote the label of the unknown marked record by x_0 . We are given an **oracle** which computes the n bit binary function

$$f : \{0, 1\}^n \longrightarrow \{0, 1\}$$

defined by

$$f(x) = \begin{cases} 1 & \text{if } x = x_0 \quad (\text{“Yes”}) \\ 0 & \text{otherwise} \quad (\text{“No”}) \end{cases}$$

By calling the function f an **oracle** we mean that we have neither access to the internal workings of the function f , nor immediate access to all argument-function pairs $(x, f(x))$. The oracle f operates simply as a blackbox function, which we can query as many times as we like. But with each such query comes an associated computational cost.

Search Problem for an Unstructured Database. *Find the record labeled as x_0 with the minimum amount of computational work, i.e., with the minimum number of queries of the oracle f .*

From elementary probability theory, we know that if we examine k random¹ records, i.e., if we compute the oracle f for k randomly chosen records, then the probability of finding the record labeled as x_0 is k/N . Hence, *on a classical computer*, finding the unknown record label x_0 comes with the computational price tag of $O(N) = O(2^n)$ computational steps.

2. Two examples

The above search problem for an unstructured database is a fundamental and practical problem which appears in many different guises.

2.1. Example 1. Searching a city phone book.

For example, consider a city phone book containing N phone numbers [3]. Find the name associated with the phone number

$$x_0 = (123) \quad 456 - 7890$$

As mentioned earlier, the best classical algorithm for finding the associated name, say Jane Doe, would search through $N/2$ phone numbers (i.e., $O(N)$ phone numbers) on average before finding the name Jane Doe.

¹We are assuming the uniform probability distribution.

2.2. Example 2. A plaintext/ciphertext attack on DES.

As another example, consider a **plaintext/ciphertext attack** by brute force key search on a message encrypted with the **Data Encryption Standard (DES)**, where the key K is a 56 bit number.

Given the plaintext/ciphertext pair

PlainText	At0500BlowUpTheEmbassyAt
CipherText	xjejpwwziderkqldievmsfkfdlqye

crack the entire cipher by encrypting the PlainText

At0500BlowUpTheEmbassyAt

with each of the $N = 2^{56}$ keys

$$K = 0, 1, 2, \dots, 2^{56} - 1 ,$$

in turn, until the key K_0 is found that produces the CipherText

xjejpwwziderkqldievmsfkfdlqye

In other words, if

$$(P, C)$$

denotes the available plaintext/ciphertext pair, and if

$$K_0$$

denotes the key such that

$$DES(P, K_0) = C ,$$

then the **oracle** is

$$f(K) = \begin{cases} 1 & \text{if } K = K_0 \quad (\text{"Yes"}) \\ 0 & \text{otherwise} \quad (\text{"No"}) \end{cases}$$

3. The quantum mechanical perspective

As we have seen, any classical algorithm for searching an unstructured database of N records must take on average at least $O(N)$ computational steps. However, much to everyone's surprise, Lov Grover actually found a non-classical quantum algorithm for searching such a database even faster, with an average of $O(\sqrt{N})$ steps, and with an average total computational cost of $O(\sqrt{N} \lg N)$. Although this is not exponentially faster, it is indeed a significant speedup.

Let \mathcal{H}_2 be a 2 dimensional Hilbert space with orthonormal basis

$$\{|0\rangle, |1\rangle\} ;$$

and let

$$\{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$$

denote the induced orthonormal basis of the Hilbert space

$$\mathcal{H} = \bigotimes_0^{n-1} \mathcal{H}_2 .$$

From the quantum mechanical perspective, the oracle function f is given as a blackbox unitary transformation U_f , i.e., by

$$\mathcal{H} \otimes \mathcal{H}_2 \xrightarrow{U_f} \mathcal{H} \otimes \mathcal{H}_2$$

$$|x\rangle \otimes |y\rangle \longmapsto |x\rangle \otimes |f(x) \oplus y\rangle$$

where ‘ \oplus ’ denotes exclusive ‘OR’, i.e., addition modulo 2.²

Instead of U_f , we will use the computationally equivalent unitary transformation

$$I_{|x_0\rangle}(|x\rangle) = (-1)^{f(x)} |x\rangle = \begin{cases} -|x_0\rangle & \text{if } x = x_0 \\ |x\rangle & \text{otherwise} \end{cases}$$

That $I_{|x_0\rangle}$ is computationally equivalent to U_f follows from the easily verifiable fact that

$$U_f \left(|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = (I_{|x_0\rangle}(|x\rangle)) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} ,$$

and also from the fact that U_f can be constructed from a controlled- $I_{|x_0\rangle}$ and two one qubit Hadamard transforms. (For details, please refer to [12], [13].)

The unitary transformation $I_{|x_0\rangle}$ is actually an **inversion** [1] in \mathcal{H} about the hyperplane perpendicular to $|x_0\rangle$. This becomes evident when $I_{|x_0\rangle}$ is rewritten in the form

$$I_{|x_0\rangle} = I - 2|x_0\rangle\langle x_0| ,$$

where ‘ I ’ denotes the identity transformation. More generally, for any unit length ket $|\psi\rangle$, the unitary transformation

$$I_{|\psi\rangle} = I - 2|\psi\rangle\langle\psi|$$

is an inversion in \mathcal{H} about the hyperplane orthogonal to $|\psi\rangle$.

²Please note that $U_f = (\nu \circ \iota)(f)$, as defined in sections 10.3 and 10.4 of [14].

4. Properties of the inversion $I_{|\psi\rangle}$

We digress for a moment to discuss the properties of the unitary transformation $I_{|\psi\rangle}$. To do so, we need the following definition.

DEFINITION 1. *Let $|\psi\rangle$ and $|\chi\rangle$ be two kets in \mathcal{H} for which the bracket product $\langle\psi|\chi\rangle$ is a real number. We define*

$$\mathcal{S}_{\mathbb{C}} = \text{Span}_{\mathbb{C}}(|\psi\rangle, |\chi\rangle) = \{\alpha|\psi\rangle + \beta|\chi\rangle \in \mathcal{H} \mid \alpha, \beta \in \mathbb{C}\}$$

as the sub-Hilbert space of \mathcal{H} spanned by $|\psi\rangle$ and $|\chi\rangle$. We associate with the Hilbert space $\mathcal{S}_{\mathbb{C}}$ a real inner product space lying in $\mathcal{S}_{\mathbb{C}}$ defined by

$$\mathcal{S}_{\mathbb{R}} = \text{Span}_{\mathbb{R}}(|\psi\rangle, |\chi\rangle) = \{a|\psi\rangle + b|\chi\rangle \in \mathcal{H} \mid a, b \in \mathbb{R}\} ,$$

where the inner product on $\mathcal{S}_{\mathbb{R}}$ is that induced by the bracket product on \mathcal{H} . If $|\psi\rangle$ and $|\chi\rangle$ are also linearly independent, then $\mathcal{S}_{\mathbb{R}}$ is a 2 dimensional real inner product space (i.e., the 2 dimensional Euclidean plane) lying inside of the complex 2 dimensional space $\mathcal{S}_{\mathbb{C}}$.

PROPOSITION 1. *Let $|\psi\rangle$ and $|\chi\rangle$ be two linearly independent unit length kets in \mathcal{H} with real bracket product; and let $\mathcal{S}_{\mathbb{C}} = \text{Span}_{\mathbb{C}}(|\psi\rangle, |\chi\rangle)$ and $\mathcal{S}_{\mathbb{R}} = \text{Span}_{\mathbb{R}}(|\psi\rangle, |\chi\rangle)$. Then*

- 1) *Both $\mathcal{S}_{\mathbb{C}}$ and $\mathcal{S}_{\mathbb{R}}$ are invariant under the transformations $I_{|\psi\rangle}$, $I_{|\chi\rangle}$, and hence $I_{|\psi\rangle} \circ I_{|\chi\rangle}$, i.e.,*

$I_{ \psi\rangle}(\mathcal{S}_{\mathbb{C}}) = \mathcal{S}_{\mathbb{C}}$	and	$I_{ \psi\rangle}(\mathcal{S}_{\mathbb{R}}) = \mathcal{S}_{\mathbb{R}}$
$I_{ \chi\rangle}(\mathcal{S}_{\mathbb{C}}) = \mathcal{S}_{\mathbb{C}}$	and	$I_{ \chi\rangle}(\mathcal{S}_{\mathbb{R}}) = \mathcal{S}_{\mathbb{R}}$
$I_{ \psi\rangle}I_{ \chi\rangle}(\mathcal{S}_{\mathbb{C}}) = \mathcal{S}_{\mathbb{C}}$	and	$I_{ \psi\rangle}I_{ \chi\rangle}(\mathcal{S}_{\mathbb{R}}) = \mathcal{S}_{\mathbb{R}}$

- 2) *If $L_{|\psi^\perp\rangle}$ is the line in the plane $\mathcal{S}_{\mathbb{R}}$ which passes through the origin and which is perpendicular to $|\psi\rangle$, then $I_{|\psi\rangle}$ restricted to $\mathcal{S}_{\mathbb{R}}$ is a reflection in (i.e., a Möbius inversion [1] about) the line $L_{|\psi^\perp\rangle}$. A similar statement can be made in regard to $|\chi\rangle$.*
- 3) *If $|\psi^\perp\rangle$ is a unit length vector in $\mathcal{S}_{\mathbb{R}}$ perpendicular to $|\psi\rangle$, then*

$$-I_{|\psi\rangle} = I_{|\psi^\perp\rangle} .$$

(Hence, $\langle\psi^\perp|\chi\rangle$ is real.)

Finally we note that, since $I_{|\psi\rangle} = I - 2|\psi\rangle\langle\psi|$, it follows that

PROPOSITION 2. *If $|\psi\rangle$ is a unit length ket in \mathcal{H} , and if U is a unitary transformation on \mathcal{H} , then*

$$UI_{|\psi\rangle}U^{-1} = I_{U|\psi\rangle} .$$

5. The method in Lov's "madness"

Let $H : \mathcal{H} \rightarrow \mathcal{H}$ be the Hadamard transform, i.e.,

$$H = \bigotimes_{0}^{n-1} H^{(2)} ,$$

where

$$H^{(2)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

with respect to the basis $|0\rangle, |1\rangle$.

We begin by using the Hadamard transform H to construct a state $|\psi_0\rangle$ which is an equal superposition of all the standard basis states $|0\rangle, |1\rangle, \dots, |N-1\rangle$ (including the unknown state $|x_0\rangle$), i.e.,

$$|\psi_0\rangle = H|0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle .$$

Both $|\psi_0\rangle$ and the unknown state $|x_0\rangle$ lie in the Euclidean plane $\mathcal{S}_{\mathbb{R}} = \text{Span}_{\mathbb{R}}(|\psi_0\rangle, |x_0\rangle)$. Our strategy is to rotate within the plane $\mathcal{S}_{\mathbb{R}}$ the state $|\psi_0\rangle$ about the origin until it is as close as possible to $|x_0\rangle$. Then a measurement with respect to the standard basis of the state resulting from rotating $|\psi_0\rangle$, will produce $|x_0\rangle$ with high probability.

To achieve this objective, we use the oracle $I_{|x_0\rangle}$ to construct the unitary transformation

$$Q = -HI_{|0\rangle}H^{-1}I_{|x_0\rangle} ,$$

which by proposition 2 above, can be rewritten as

$$Q = -I_{|\psi_0\rangle}I_{|x_0\rangle} .$$

Let $|x_0^\perp\rangle$ and $|\psi_0^\perp\rangle$ denote unit length vectors in $\mathcal{S}_{\mathbb{R}}$ perpendicular to $|x_0\rangle$ and $|\psi_0\rangle$, respectively. There are two possible choices for each of $|x_0^\perp\rangle$ and $|\psi_0^\perp\rangle$ respectively. To remove this minor, but nonetheless annoying, ambiguity, we select $|x_0^\perp\rangle$ and $|\psi_0^\perp\rangle$ so that the orientation of the plane $\mathcal{S}_{\mathbb{R}}$ induced by the ordered spanning vectors $|\psi_0\rangle, |x_0\rangle$ is the same orientation as that induced by each of the ordered bases $|x_0^\perp\rangle, |x_0\rangle$ and $|\psi_0\rangle, |\psi_0^\perp\rangle$. (Please refer to Figure 2.)

REMARK 1. *The removal of the above ambiguities is really not essential. However, it does simplify the exposition given below.*

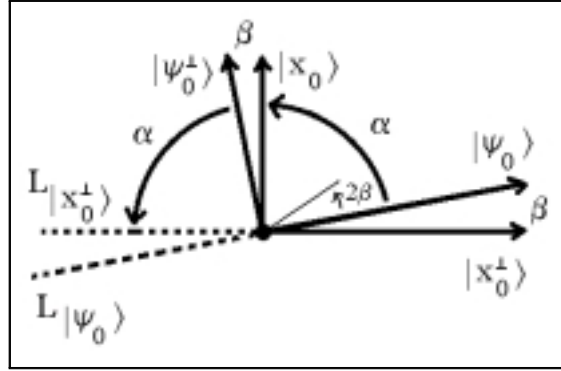


Figure 2. The linear transformation $Q|_{\mathcal{S}_R}$ is a reflection in the line $L_{|x_0^\perp\rangle}$ followed by reflection in the line $L_{|\psi_0\rangle}$. By Theorem 1, this is the same as rotation by the angle 2β . Thus, $Q|_{\mathcal{S}_R}$ rotates $|\psi_0\rangle$ by the angle 2β toward $|x_0\rangle$.

We proceed by noting that, by the above proposition 1, the plane \mathcal{S}_R lying in \mathcal{H} is invariant under the linear transformation Q , and that, when Q is restricted to the plane \mathcal{S}_R , it can be written as the composition of two inversions, i.e.,

$$Q|_{\mathcal{S}_R} = I_{|\psi_0^\perp\rangle} I_{|x_0\rangle} .$$

In particular, $Q|_{\mathcal{S}_R}$ is the composition of two inversions in \mathcal{S}_R , the first in the line $L_{|x_0^\perp\rangle}$ in \mathcal{S}_R passing through the origin having $|x_0\rangle$ as normal, the second in the line $L_{|\psi_0\rangle}$ through the origin having $|\psi_0^\perp\rangle$ as normal.³

We can now apply the following theorem from plane geometry:

THEOREM 1. *If L_1 and L_2 are lines in the Euclidean plane \mathbb{R}^2 intersecting at a point O , and if β is the angle in the plane from L_1 to L_2 , then the operation of reflection in L_1 followed by reflection in L_2 is just rotation by angle 2β about the point O .*

Let β denote the angle in \mathcal{S}_R from $L_{|x_0^\perp\rangle}$ to $L_{|\psi_0\rangle}$, which by plane geometry is the same as the angle from $|x_0^\perp\rangle$ to $|\psi_0\rangle$, which in turn is the same as the angle from $|x_0\rangle$ to $|\psi_0^\perp\rangle$. Then by the above theorem $Q|_{\mathcal{S}_R} = I_{|\psi_0^\perp\rangle} I_{|x_0\rangle}$ is a rotation about the origin by the angle 2β .

The key idea in Grover's algorithm is to move $|\psi_0\rangle$ toward the unknown state $|x_0\rangle$ by successively applying the rotation Q to $|\psi_0\rangle$ to rotate it around to $|x_0\rangle$.

³The line $L_{|x_0^\perp\rangle}$ is the intersection of the plane \mathcal{S}_R with the hyperplane in \mathcal{H} orthogonal to $|x_0\rangle$. A similar statement can be made in regard to $L_{|\psi_0\rangle}$.

This process is called **amplitude amplification**. Once this process is completed, the measurement of the resulting state (with respect to the standard basis) will, with high probability, yield the unknown state $|x_0\rangle$. This is the essence of Grover's algorithm.

But how many times K should we apply the rotation Q to $|\psi_0\rangle$? If we applied Q too many or too few times, we would over- or undershoot our target state $|x_0\rangle$.

We determine the integer K as follows:

Since

$$|\psi_0\rangle = \sin \beta |x_0\rangle + \cos \beta |x_0^\perp\rangle ,$$

the state resulting after k applications of Q is

$$|\psi_k\rangle = Q^k |\psi_0\rangle = \sin [(2k + 1) \beta] |x_0\rangle + \cos [(2k + 1) \beta] |x_0^\perp\rangle .$$

Thus, we seek to find the smallest positive integer $K = k$ such that

$$\sin [(2k + 1) \beta]$$

is as close as possible to 1. In other words, we seek to find the smallest positive integer $K = k$ such that

$$(2k + 1) \beta$$

is as close as possible to $\pi/2$. It follows that

$$K = k = \text{round} \left(\frac{\pi}{4\beta} - \frac{1}{2} \right) = \left\lfloor \frac{\pi}{4\beta} \right\rfloor ,$$

where “round” is the function that rounds to the nearest integer, and where “ $\lfloor - \rfloor$ ” denotes the floor function.

We can determine the angle β by noting that the angle α from $|\psi_0\rangle$ to $|x_0\rangle$ is complementary to β , i.e.,

$$\alpha + \beta = \pi/2 ,$$

and hence,

$$\frac{1}{\sqrt{N}} = \langle x_0 | \psi_0 \rangle = \cos \alpha = \cos \left(\frac{\pi}{2} - \beta \right) = \sin \beta .$$

Thus, the angle β is given by

$$\beta = \sin^{-1} \left(\frac{1}{\sqrt{N}} \right) \approx \frac{1}{\sqrt{N}} \quad (\text{for large } N) ,$$

and hence,

$$K = k = \left\lfloor \frac{\pi}{4 \sin^{-1} \left(\frac{1}{\sqrt{N}} \right)} \right\rfloor \approx \left\lfloor \frac{\pi}{4} \sqrt{N} \right\rfloor \quad (\text{for large } N).$$

6. Summary of Grover's algorithm

In summary, we provide the following outline of Grover's algorithm:

Grover's Algorithm	
STEP 0.	(Initialization) $ \psi\rangle \leftarrow H 0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} j\rangle$ $k \leftarrow 0$
STEP 1.	Loop until $k = \left\lfloor \frac{\pi}{4 \sin^{-1}(1/\sqrt{N})} \right\rfloor \approx \left\lfloor \frac{\pi}{4} \sqrt{N} \right\rfloor$ $ \psi\rangle \leftarrow Q \psi\rangle = -HI_{ 0\rangle}HI_{ x_0\rangle} \psi\rangle$ $k \leftarrow k + 1$
STEP 2.	Measure $ \psi\rangle$ with respect to the standard basis $ 0\rangle, 1\rangle, \dots, N-1\rangle$ to obtain the unknown state $ x_0\rangle$ with probability $\geq 1 - \frac{1}{N}$.

We complete our summary with the following theorem:

THEOREM 2. *With a probability of error*

$$Prob_E \leq \frac{1}{N},$$

Grover's algorithm finds the unknown state $|x_0\rangle$ at a computational cost of

$$O(\sqrt{N} \lg N)$$

PROOF.

Part 1. The probability of error $Prob_E$ of finding the hidden state $|x_0\rangle$ is given by

$$Prob_E = \cos^2[(2K+1)\beta],$$

where

$$\begin{cases} \beta = \sin^{-1}\left(\frac{1}{\sqrt{N}}\right) \\ K = \left\lfloor \frac{\pi}{4\beta} \right\rfloor \end{cases},$$

and where " $\lfloor - \rfloor$ " denotes the floor function. Hence,

$$\frac{\pi}{4\beta} - 1 \leq K \leq \frac{\pi}{4\beta} \implies \frac{\pi}{2} - \beta \leq (2K+1)\beta \leq \frac{\pi}{2} + \beta$$

$$\implies \sin \beta = \cos\left(\frac{\pi}{2} - \beta\right) \geq \cos[(2K+1)\beta] \geq \cos\left(\frac{\pi}{2} + \beta\right) = -\sin \beta$$

Thus,

$$Prob_E = \cos^2 [(2K + 1) \beta] \leq \sin^2 \beta = \sin^2 \left(\sin^{-1} \left(\frac{1}{\sqrt{N}} \right) \right) = \frac{1}{N}$$

Part 2. The computational cost of the Hadamard transform $H = \otimes_0^{n-1} H^{(2)}$ is $O(n) = O(\lg N)$ single qubit operations. The transformations $-I_{|0\rangle}$ and $I_{|x_0\rangle}$ each carry a computational cost of $O(1)$.

STEP 1 is the computationally dominant step. In STEP 1 there are $O(\sqrt{N})$ iterations. In each iteration, the Hadamard transform is applied twice. The transformations $-I_{|0\rangle}$ and $I_{|x_0\rangle}$ are each applied once. Hence, each iteration comes with a computational cost of $O(\lg N)$, and so the total cost of STEP 1 is $O(\sqrt{N} \lg N)$. □

7. An example of Grover's algorithm

As an example, we search a database consisting of $N = 2^n = 8$ records for an unknown record with the unknown label $x_0 = 5$. The calculations for this example were made with OpenQuacks [15], an open source publically available quantum simulator Maple package developed at UMBC.

We are given a blackbox computing device

$$\text{In} \rightarrow \boxed{\boxed{I_{|?\rangle}}} \rightarrow \text{Out}$$

that implements as an oracle the unitary transformation

$$I_{|x_0\rangle} = I_{|5\rangle} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We cannot open up the blackbox $\rightarrow \boxed{\boxed{I_{|?\rangle}}} \rightarrow$ to see what is inside. So we do not know what $I_{|x_0\rangle}$ and x_0 are. The only way that we can glean some information about x_0 is to apply some chosen state $|\psi\rangle$ as input, and then make use of the resulting output.

Using of the blackbox \rightarrow $I_{|?\rangle}$ \rightarrow as a component device, we construct a computing device \rightarrow $-HI_{|0\rangle}HI_{|?\rangle}$ \rightarrow which implements the unitary operator

$$Q = -HI_{|0\rangle}HI_{|x_0\rangle} = \frac{1}{4} \begin{pmatrix} -3 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -3 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -3 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -3 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -3 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & -3 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 & -3 \end{pmatrix}$$

We do not know what unitary transformation Q is implemented by the device \rightarrow $-HI_{|0\rangle}HI_{|?\rangle}$ \rightarrow because the blackbox \rightarrow $I_{|?\rangle}$ \rightarrow is one of its essential components.

STEP 0. We begin by preparing the known state

$$|\psi_0\rangle = H|0\rangle = \frac{1}{\sqrt{8}}(1, 1, 1, 1, 1, 1, 1, 1)^{transpose}$$

STEP 1. We proceed to loop

$$K = \left\lfloor \frac{\pi}{4 \sin^{-1}(1/\sqrt{8})} \right\rfloor = 2$$

times in STEP 1.

ITERATION 1. On the first iteration, we obtain the unknown state

$$|\psi_1\rangle = Q|\psi_0\rangle = \frac{1}{4\sqrt{2}}(1, 1, 1, 1, 5, 1, 1, 1)^{transpose}$$

ITERATION 2. On the second iteration, we obtain the unknown state

$$|\psi_2\rangle = Q|\psi_1\rangle = \frac{1}{8\sqrt{2}}(-1, -1, -1, -1, 11, -1, -1, -1)^{transpose}$$

and branch to STEP 2.

STEP 2. We measure the unknown state $|\psi_2\rangle$ to obtain either

$$|5\rangle$$

with probability

$$Prob_{Success} = \sin^2((2K+1)\beta) = \frac{121}{128} = 0.9453$$

or some other state with probability

$$Prob_{Failure} = \cos^2((2K + 1)\beta) = \frac{7}{128} = 0.0547$$

and then exit.

References

- [1] Beardon, Alan F., "The Geometry of Discrete Groups," Springer-Verlag, (1983).
- [2] Brassard, Gilles, and Paul Bratley, "**Algorithmics: Theory and Practice**," Printice-Hall, (1988).
- [3] Brassard, Gilles, **Searching a Quantum Phone Book**, Science, 275, (1997), pp 627-628.
- [4] Cormen, Thomas H., Charles E. Leiserson, and Ronald L. Rivest, "**Introduction to Algorithms**," McGraw-Hill, (1990).
- [5] Grover, Lov K., **Quantum computer can search arbitrarily large databases by a single query**, Phys. Rev. Letters (1997), pp 4709-4712.
- [6] Grover, Lov K., **A framework for fast quantum mechanical algorithms**, <http://xxx.lanl.gov/abs/quant-ph/9711043>.
- [7] Grover, L., Proc. 28th Annual ACM Symposium on the Theory of Computing, ACM Press, New Yorkm (1996), pp 212 - 219.
- [8] Grover, L., Phys. Rev. Lett. 78, (1997), pp 325 - 328.
- [9] Gruska, Jozef, "**Quantum Computing**," McGraw-Hill, (1999).
- [10] Hirvensalo, Mika, "**Quantum Computing**," Springer-Verlag, (2001).
- [11] Jozsa, Richard, **Searching in Grover's Algorithm**, <http://xxx.lanl.gov/abs/quant-ph/9901021>.
- [12] Jozsa, Richard, Proc. Roy. Soc. London Soc., Ser. A, 454, (1998), 323 - 337.
- [13] Kitaev, A., **Quantum measurement and the abelian stabiliser problem**, (1995), quant-ph preprint archive 9511026.
- [14] Lomonaco, Samuel J., Jr., **A Rosetta Stone for quantum mechanics with an introduction to quantum computation**, in "**Quantum Computation**," edited by S.J. Lomonaco, Jr., this AMS Proceedings of Symposia in Applied Mathematics (PSAPM). (<http://xxx.lanl.gov/abs/quant-ph/0007045>)
- [15] McCubbin, Christopher B., **OpenQuacks**, (masters thesis), <http://userpages.umbc.edu/~cmccub1/quacs/quacs.html>.
- [16] Nielsen, Michael A., and Isaac L. Chuang, "**Quantum Computation and Quantum Information**," Cambridge University Press, (2000).
- [17] Shor, Peter W., **Introduction to quantum algorithms**, n "**Quantum Computation**," this AMS Proceedings of Symposia in Applied Mathematics (PSAPM). (<http://xxx.lanl.gov/abs/quant-ph/0005003>)
- [18] Vazirani, Umesh, **Quantum complexity theory**, in "**Quantum Computation**," this AMS Proceedings of Symposia in Applied Mathematics (PSAPM).
- [19] Zalka, Christof, **Grover's quantum searching algorithm is optimal**, (2001). (<http://xxx.lanl.gov/abs/quant-ph/9711070>).

UNIVERSITY OF MARYLAND BALTIMORE COUNTY, BALTIMORE, MD 21250

E-mail address: Lomonaco@UMBC.EDU

URL: <http://www.csee.umbc.edu/~lomonaco>