Quantum Information and Computing- Grover's Search Algorithm-

Dipan Kumar Ghosh
Department of Physics
Indian Institute of Technology Bombay
Powai, Mumbai 400076

March 17, 2017

1 Introduction

Search algorithms are useful in locating an item in a database, which may either be structured or unstructured. For instance, in a traditional telephone directory, the names are arranged alphabetically but the associated telephone numbers are randomly distributed. The database in this case is structured with respect to names but is unstructured with respect to the phone numbers. While it is relatively easy to locate a telephone number of a person whose name we know, it is next to impossible to locate who a particular phone number belongs to. Searching for an element in an unstructured database is like the proverbial searching for a "needle in a haystack".

One can formulate the problem mathematically by defining a function $f(k)$ which has a value zero for all values of $k, (1 \ll N = 2^n)$ except for one particular value of $k = k_0$ for which $f(k_0) = 1$. If the database of N values are random, then, in order to locate the element $k = k_0$, one has to search through the entire database, evaluate $f(k)$ for each k until such time that we locate a k for which $f(k) = 1$. To locate k_0 with a probability of $1/2$, we require $N/2$ trials. Thus a classical search requires $O(N)$ number of queries.

Structured database clearly reduces the number of queries. An example of such a database search is given by a function $f(k)$ which takes distinct values for different values of the argument k. The task here is to find $k = k_0$ such that $f(k_0) = a$. If the values of k are sorted such that $f(k_1) > f(k_2) > \ldots > f(k_N)$, it is easy to locate k_0 by a scheme similar to the method of successive division in finding the roots of a polynomial. If $N = 2^n$, we first find the value of $f(k_i)$ for $i = 2^{n-1}$, i.e. for the value of function corresponding to the central element. If $f(k_i) > a$, then k_0 is located to the left of the central element, otherwise, it is located to its right. Thus every evaluation of $f(k)$ shrinks the look up range by a factor of 2 and we may, therefore, locate the solution by a maximum of $\log_2 N$

queries.
Grover designed an algorithm for search of an element in an unstructured database in a quantum computer. If the search has a unique solution, Grover's algorithm can locate the item with a high probability in $O(\sqrt{N})$ number of trials resulting in a quadratic speeding up with respect to classical algorithms. The algorithm attains this by a selective amplification of the amplitude of the state corresponding to the item to be found. It may be mentioned that it has been shown that Grover's algorithm is optimal in the sense that no other algorithm can perform the same task with a number of trials less than $O(\sqrt{N})$.

2 The Oracle

The quantum oracle calculates a function f for n qubit inputs and returns 1 when the input matches a particular string w, called the *marked string*, in all other cases it returns zero. Thus $f : \{0,1\}^{\otimes n} \rightarrow \{0,1\}$ with the property

$$f_w(x) = \begin{cases} 0 & \text{for } x \neq w \\ 1 & \text{for } x = w \end{cases}$$

Being a quantum oracle, it can evaluate superpositions of strings. As the oracle evaluates a function that is not uniquely invertible (a function that evaluates to zero could have arisen from many different strings), the operation cannot be unitarily performed using a single input register. The oracle, therefore, uses a second register whose final state depends on what happens to the content of the first register. The oracle is schematically represented by the following figure In the Deutsch-Jozsa algorithm, we had seen that if

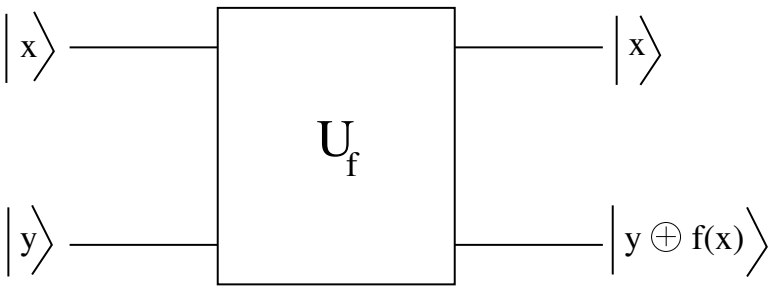

Figure 1: The Oracle

the content of the second register $\mid y\rangle$ is taken to be $(\mid 0\rangle - \mid 1\rangle)/\sqrt{2}$, the output can be written as

$$(-1)^{f_w(x)} \mid x\rangle \frac{1}{\sqrt{2}}(\mid 0\rangle - \mid 1\rangle) \tag{1}$$

which shows that the second register is unaltered but the sign of the state in the first register depends on the function $f_w(x)$. Thus we focus our attention on the state of the first register. If the input string does not match with the marked string w, then

$f - w(x) = 0$ and the sign of the first register is unaltered. However, if $x = w$, the sign of the state is flipped. The unitary operator which can achieve this is given by

$$U_w = I - 2 \mid w\rangle\langle w \mid \tag{2}$$

where $\mid w\rangle$ is the state of the marked item, which is orthogonal to the states associated with the remaining items in the database.

3 Grover Operator and its Geometric Interpretation

The first stage of the algorithm consists of creating a standard state $\mid s\rangle$ which is a combination of all 2^n basis states of n qubits. The state $\mid s\rangle$ is a linear combination of N basis states, each with the same amplitude and phase. As has been seen earlier, such a state is obtained by Hadamard transform of an initial state $\mid 0\rangle^{\otimes n}$. we associate a unique basis with each of the items in the database. as the marked state $\mid w\rangle$ is a member of the basis, we have,

$$\mid \langle w \mid s\rangle \mid = \frac{1}{\sqrt{N}} \tag{3}$$

Corresponding to the state $\mid s\rangle$, we define a *reflection operator* U_s which has the property that acting on an arbitrary state $\mid \psi\rangle$, it leaves the component of $\mid \psi\rangle$ along $\mid s\rangle$ undisturbed but flips the sign of the component perpendicular to $\mid s\rangle$. Such an operator is given by

$$U_s = 2 \mid s\rangle\langle s \mid -I \tag{4}$$

Grover rotation operator R_G is product of the sign flip operator U_w and the reflection operator U_s defined in (2) and (4),

$$R_G = U_s U_w \tag{5}$$

A simple geometrical interpretation of the Grover operator R_G can be seen by operating R_G on an arbitrary state $\mid \psi\rangle$ in the plane defined by $\mid s\rangle$ and $\mid w\rangle$ (see Figure 2). Let

$$\mid \langle w \mid s\rangle \mid = \frac{1}{\sqrt{N}} = \sin\theta \tag{6}$$

so that the angle between the vectors $\mid s\rangle$ and $\mid w\rangle$ is $\frac{\pi}{2} - \theta$. Figure 2 illustrates the successive application of U_w and U_s on the state $\mid \psi\rangle$. From the figure, it is clear that the angle between $\mid \psi\rangle$ and its state $\mid \psi_2\rangle$, after application of Grover rotation is $2(\phi+\chi) = 2\theta$. This rotation provides a basis for Grover's search.

As a simple illustration, consider Figure 2 for $N = 4$, i.e. for an unsorted database of just 4 elements from which one state is to be found. We consider what happens when Grover rotation is applied to the state $\mid s\rangle$. In this case we have, using (3), $\mid \langle w \mid s\rangle \mid = \frac{1}{\sqrt{4}} = \frac{1}{2}$, so that $\theta = 30^\circ$. Recall that θ is the angle between $\mid s\rangle$ and $\mid w_\perp\rangle$. Thus a single rotation

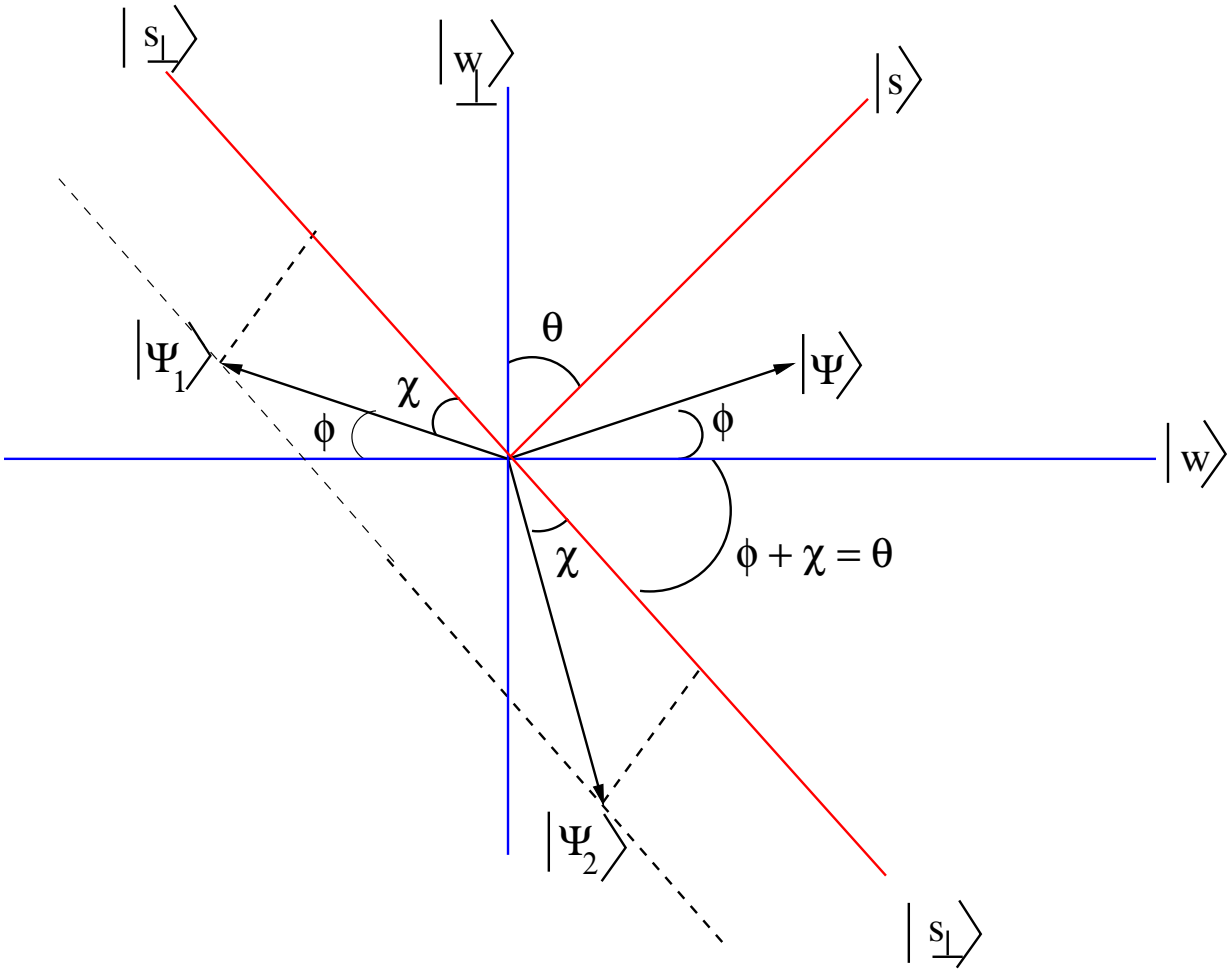

Figure 2: Grover Rotation

R_G would rotate the state $|\, s\rangle$ by $2\theta = 60°$, i.e. align the state $|\, s\rangle$ with $|\, w\rangle$.

Consider the case of $N = 8$. In this case $\sin\theta = \dfrac{1}{2\sqrt{2}}$ so that $\theta = 20.7°$. The angle between $|\, s\rangle$ and $|\, w\rangle$ is thus $69.3°$. Since each application of R_G rotates $|\, s\rangle$ by $2\theta = 41.4°$, after the first iteration, the angle between $|\, s\rangle$ and $|\, w\rangle$ is $27.9°$. A second iteration makes this angle $-13.5°$ which is closer to $|\, w\rangle$ than it was after the first iteration. A third iteration, however, takes it farther away at $54.9°$. Thus for $N = 8$ a maximum of two iteration is indicated. One can check that the amplitude of the marked state becomes the largest after two iterations. We thus need to know, a-priori, how many iterations are required. As N increases, every rotation step becomes smaller and we can control the process of approaching the marked state much better. In the next lecture we will get an estimate of the number of iterations required.

The operation of U_w on an arbitrary state flips the sign of the component of $|\, \psi\rangle$ parallel to $|\, w\rangle$. This is followed by the application of the reflection operator U_s on the

resulting state. It is instructive to look at the action of U_s on an arbitrary state. Consider its effect on an arbitrary state $\mid \phi\rangle$ where the state is expressed in the computational basis $\{\mid x\rangle\}$

$$\mid \phi\rangle = \sum_x a_x \mid x\rangle \tag{7}$$

Using (4), we have

$$\langle s \mid \phi\rangle = \frac{1}{\sqrt{N}} \sum_x a_x = \sqrt{N}\bar{a}$$

where $\bar{a} = \frac{1}{N}\sum_x a_x$ is the mean amplitude of $\mid \phi\rangle$ in the computational basis. We then have,

$$\begin{aligned} U_s \mid \phi\rangle &= [2 \mid s\rangle\langle s \mid -I] \mid \phi\rangle \\ &= 2 \mid s\rangle\langle s \mid\mid \phi\rangle - \mid \phi\rangle \\ &= 2\sqrt{N}\bar{a} \mid s\rangle - \mid \phi\rangle \\ &= \sum_x (2\bar{a} - a_x) \mid x\rangle \end{aligned} \tag{8}$$

Equation (34) shows that the amplitude a_x under reflection becomes $2\bar{a} - a_x$ so that the amplitude of the state with respect to the mean $a_x - \bar{a}$ becomes $\bar{a} - a_x$, i.e. it gets inverted. To illustrate this consider the case of $N = 8$. In the state $\mid s\rangle$ each of the state in the computational basis has an amplitude $\frac{1}{2\sqrt{2}}$. In Figure 5 the top panel shows equal amplitude of the eight states in $\mid s\rangle$. Since each state has the same amplitude, the mean is also $\frac{1}{2\sqrt{2}}$. The application of U_w on the state $\mid s\rangle$ inverts the component parallel to $\mid w\rangle$. In the figure, we have taken the marked state $\mid w\rangle$ to be the 4th state so that in the second panel, only the 4th component is shown inverted. Calling this state $\mid \phi\rangle$, we have the amplitude $a_w = -\frac{1}{2\sqrt{2}}$ and $a_x = \frac{1}{2\sqrt{2}}$ for all $x \neq w$. Thus the mean amplitude at this stage is $\frac{1}{8}\left(7\frac{1}{2\sqrt{2}} - \frac{1}{2\sqrt{2}}\right) = \frac{3}{8\sqrt{2}}$. An application of U_s on this state will let $a_x \to 2\bar{a} - a_x$, i.e., for all states other than the marked state $\mid w\rangle$, the amplitude will become $a_{x'} = \frac{3}{4\sqrt{2}} - \frac{1}{2\sqrt{2}} = \frac{1}{2\sqrt{2}}$. The amplitude of the marked state $\mid w\rangle$ becomes $a_{w'} = \frac{3}{4\sqrt{2}} + \frac{1}{2\sqrt{2}} = \frac{5}{4\sqrt{2}}$ which has a magnitude five times that of each of the other component, i.e., the probability density of the state is amplified 25 times with respect to each of the ummarked states.

4 Maximum Number of Iteration

We saw that the function of the Grover operator R_G is to selectively amplify the amplitude of the state $\mid w\rangle$. The angle between $\mid s\rangle$ and $\mid w\rangle$ is $\frac{\pi}{2} - \theta$. thus the number of

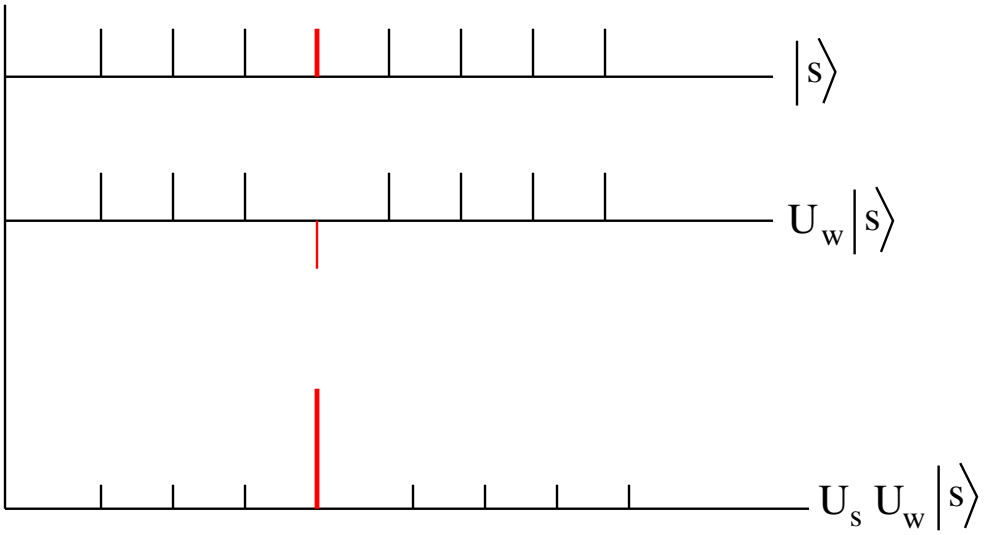

Figure 3: Selective Amplification

iteration should be such that $\mid s\rangle$ is rotated by an angle as close to $\frac{\pi}{2} - \theta$ as possible. This requires an *a priori* knowledge of the number of iteration.

We can get an estimate of the number of iterations m for large N for which $\sin\theta \approx \theta = \frac{1}{\sqrt{N}}$. For this we require

$$m \times 2\theta \approx \frac{\pi}{2} - \theta$$

which gives

$$m = \frac{\pi}{4\theta} - 2$$

The number of iterations for large N is, therefore, given by

$$m \approx \frac{\pi}{4}\sqrt{N} \tag{9}$$

which shows that unlike the classical search, the number of queries is $O(\sqrt{N})$. after m it erations, the angle between $\mid s\rangle$ and $\mid w\rangle$ is $\frac{\pi}{2} - (2m+1)\theta$ whoch gives the amplitude of the state $\mid w\rangle$ in $\mid s\rangle$ to be

$$\begin{aligned} \mid \sin(2m+1)\theta \mid &= \left|\sin\left((\frac{\pi}{2}\sqrt{N}+1)\frac{1}{\sqrt{N}}\right)\right| \\ &= \left|\sin\left(\frac{\pi}{2}+\frac{1}{\sqrt{N}}\right)\right| \\ &= \mid \cos\frac{1}{\sqrt{N}} \mid \\ &\approx 1 - \frac{1}{2N} \end{aligned} \tag{10}$$

which shows the amplitude to be very close to 1.

5 Matrix Representation of Grover Operator

Grover's algorithm is implemented in the following steps.

1. We first construct a state $\mid s\rangle$ which is a uniform linear combination of N states in the computational basis. This is obtained by starting with an initial state $\mid 0\rangle^{\otimes n}$ and subjecting it to Hadamard transform, which gives

$$\mid s\rangle = \frac{1}{2^{n/2}} \sum_x \mid x\rangle$$

2. The $(n+1)$-th quit is initialised to $\mid y\rangle = \dfrac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$

we carry out repeated Grover iteration, starting with the standard state $\mid s\rangle$. Such iterations will randomise the state $\mid s\rangle$. It is thus instructive to see what these do, acting on an arbitrary state $\mid \psi\rangle = \sum_k a(k) \mid k\rangle$. We perform the following steps m times, where m will be computed later.

1. Apply the oracle. Here we calculate the value of the unitary map U_f and XOR it with the last qubit to obtain a phase factor $(-1)^{f(x)}$.

$$\mid s\rangle \mid y\rangle \rightarrow \sum_{x=0}^{N-1} a_x \mid x\rangle (-1)^{f(x)} \mid y\rangle$$

   (Initially $a_x = \dfrac{1}{\sqrt{N}}$ for each x). We denote this transformation by T.

2. Now apply on the resulting state a "diffusion operator" D defined below.

The matrix elements of the diffusion matrix is defined as follows:

$$\begin{aligned} D_{ii} &= -1 + \frac{2}{N} \\ D_{ij} &= \frac{2}{N}, \quad \text{for } i \neq j \end{aligned} \tag{11}$$

It is easily seen that if we define a $N \times N$ matrix J which has each element as 1, the "diffusion operator" has the representation

$$D = -I + \frac{2J}{N} \tag{12}$$

It is easily checked that $\dfrac{J}{N}$ is a projection operator as $\dfrac{J}{N} = \left(\dfrac{J}{N}\right)^2$. Using this, it follows that D is unitary. Since each element of J is 1, it follows that acting on a column vector

$(a_1, a_2, \ldots, a_N)^T$, we get

$$\frac{J}{N}\begin{pmatrix} a_1 \\ a_2 \\ \ldots \\ \ldots \\ a_N \end{pmatrix} = \begin{pmatrix} \frac{a_1+a_2+\ldots+a_N}{N} \\ \frac{a_1+a_2+\ldots+a_N}{N} \\ \ldots \\ \ldots \\ \frac{a_1+a_2+\ldots+a_N}{N} \end{pmatrix} = \begin{pmatrix} \bar{a} \\ \bar{a} \\ \ldots \\ \ldots \\ \bar{a} \end{pmatrix} \tag{13}$$

where $\bar{a} = \frac{1}{N}\sum_i a_i$. Thus if we take an arbitrary vector $\mid v\rangle = \sum_x v_x \mid x\rangle$ in a basis $\{\mid x\rangle\}$, we get,

$$\frac{J}{N} \mid v\rangle = \frac{J}{N}\sum_x v_x \mid x\rangle = \sum_x \bar{v} \mid x\rangle$$

Thus the action of the diffusion operator on an arbitrary vector is given by the following.

$$\begin{aligned} D \mid v\rangle &= \left(-I + \frac{J}{N}\right) \mid v\rangle = - \mid v\rangle + 2\sum_x \bar{v} \mid x\rangle \\ &= -\sum_x v_x \mid x\rangle + 2\sum_x \bar{v} \mid x\rangle \\ &= \sum_x (2\bar{v} - v_x) \mid x\rangle \end{aligned} \tag{14}$$

This shows that the diffusion operator D represents the Grover operator $U_s = -I + 2\langle s \mid\mid s\rangle$.

The diffusion operator defined above can be obtained by application of the following sequence of operators:

$$D = WRW \tag{15}$$

where W is the Walsh Hadamard transform whose elements are given by

$$W_{ij} = \frac{1}{\sqrt{N}}(-1)^{i.j} \tag{16}$$

so that the Walsh-Hadamard transform of an $n-$ qubit state $\mid x\rangle$ is given by

$$H^{\otimes n} \mid x\rangle = \frac{1}{\sqrt{N}}\sum_y (-1)^{x\cdot y} \mid y\rangle \tag{17}$$

where $x \cdot y$ represents the sum bitwise product of the two strings x and y. The operator R is a selective phase rotation which is a diagonal matrix with its first element as 1 and others equal to -1.The matrix R can be represented as

$$R_{ij} = (2\delta_{i,0} - 1)\delta_{i,j} \equiv (-1)^{1-\delta_{i,0}}\delta_{i,j} \tag{18}$$

To show (15), we will consider the matrix elements of both sides of the equation in arbitrary states $\mid x\rangle$ and $\mid y\rangle$ and show that

$$\langle x \mid WRW \mid y\rangle = \langle x \mid D \mid y\rangle \tag{19}$$

Consider the r.h.s of (19). We have,

$$\begin{aligned}\langle x \mid WRW \mid y\rangle &= \sum_{u,v}\langle x \mid W \mid u\rangle\langle u \mid R \mid v\rangle\langle v \mid W \mid y\rangle \\ &= \frac{1}{N}\sum_{u,v}(-1)^{x\cdot u}\cdot(-1)^{1-\delta_{u,0}}\delta_{u,v}\cdot(-1)^{v\cdot y} \end{aligned}\tag{20}$$

where we have used (16) and (18). We will now perform the sum over u on the right of (20). We have, splitting the sum into a term for which $u = 0$ and another for which $u \neq 0$,

$$\begin{aligned}\sum_{u}(-1)^{x\cdot u}\cdot(-1)^{1-\delta_{u,0}}\delta_{u,v} &= (-1)^0(-1)^0\delta_{0,v} - \sum_{u=1}^{N}(-1)^{x\cdot u}\delta_{u,v} \\ &= 2\delta_{0,v} - \sum_{u=0}^{N}(-1)^{x\cdot u}\delta_{u,v} \\ &= 2\delta_{0,v} - \sum_{u=0}^{N}(-1)^{x_{n-1}u_{n-1}+\ldots+x_0u_0}\delta u_{n-1},v_{n-1}\delta u_{n-2},v_{n-2}\ldots\delta u_0,v_0 \\ &= 2\delta_{0,v} - \left(\sum_{u_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}}\delta u_{n-1},v_{n-1}\right)\left(\sum_{u_{n-2}=0}^{1}(-1)^{x_{n-2}u_{n-2}}\delta u_{n-2},v_{n-2}\right)\ldots\end{aligned}\tag{21}$$

In (21), in the second line, we have once again added and subtracted $u = 0$ term and in the third line we have written explicitly in terms of the bits.
Substituting (21) into the r.h.s. of (20), we can write the r.h.s as

$$\begin{aligned} r.h.s. &= \frac{1}{N}\sum_{v=0}^{N-1}\left[2\delta_{0,v} - \left(\sum_{u_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}}\delta u_{n-1},v_{n-1}\right)\ldots\left(\sum_{u_0=0}^{1}(-1)^{x_0u_0}\delta u_0,v_0\right)\right]\times(-1)^{v\cdot y} \\ &= \frac{2}{N} - \frac{1}{N}\left[\left(\sum_{u_{n-1},v_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}+v_{n-1}y_{n-1}}\delta u_{n-1},v_{n-1}\right)\ldots\left(\sum_{u_0,v_0=0}^{1}(-1)^{x_0u_0+v_0y_0}\delta u_0,v_0\right)\right] \\ &= \frac{2}{N} - \frac{1}{N}\left(1+(-1)^{x_{n-1}+y_{n-1}}\right)\ldots\left(1+(-1)^{x_0+y_0}\right) \\ &= \frac{2}{N} - \frac{2^n}{N}\delta_{x_{n-1},y_{n-1}}\ldots\delta_{x_0,y_0} \\ &= \frac{2}{N} - \delta_{x,y} \end{aligned}\tag{22}$$

Returning to the l.h.s of (20), we have, using $D = -I + 2 \mid s\rangle\langle s \mid$,

$$\begin{aligned}\langle x \mid D \mid y\rangle &= -\delta_{x,y} + 2\langle x \mid s\rangle\langle s \mid y\rangle \\ &= -\delta_{x,y} - 2\frac{1}{\sqrt{N}}\frac{1}{\sqrt{N}} \\ &= \frac{2}{N} - \delta_{x,y} \end{aligned} \tag{23}$$

Comparing (22) and (23), the relation (19) and hence (15) follows.

6 Quantum Circuit

The steps in the above analysis can be summarised as follows:

1. Construct an equal superposition of basis states starting with $\mid 0\rangle^{\otimes n}$. The $(n+1)$-th quit is set as $\mid y\rangle = \frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$. Thus we start with $\mid \psi_0\rangle = \sum_x a_x \mid x\rangle \mid y\rangle$ with $a_x = \frac{1}{\sqrt{N}}$ for all x.

2. Apply the oracle U_f which computes $f(x)$ to produce the phase factor $(-1)^{f(x)}$. Thus
$$\mid \psi_0\rangle \mid y\rangle \rightarrow \sum_{x=0}^{N-1} a_x \mid x\rangle(-1)^{f(x)} \mid y\rangle$$
This transformation will be denoted by T.

3. Apply the diffusion operator $D = WRW$ which isa Hadamard transform followed by a phase shift R followed by yet another Hadamard transform.

4. apply steps 2 and 3 $O(\sqrt{N})$ times.

5. Measure the state of the first register. with a very high degree of probability, it would identify the marked state. If it fails (probability $O(1/N)$), go back to step 1.

A schematic circuit representation for the above is given below:

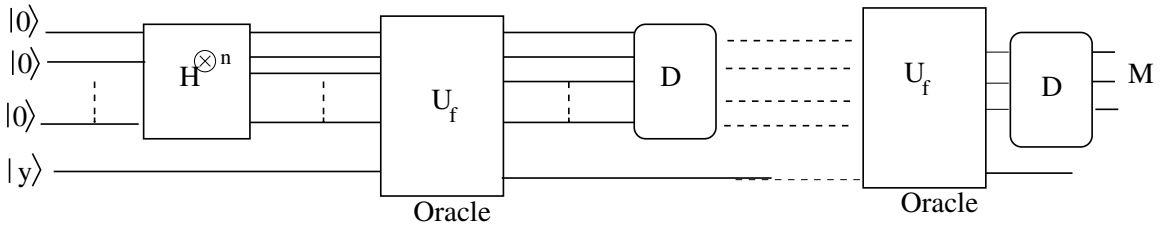

Figure 4: Schematic Circuit for Grover Algorithm

7 Success and Failure of Algorithm

Let us denote the marked state as $\mid \psi_m\rangle$ and unmarked state as $\mid \psi_u\rangle$,

$$\mid \psi_u\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq m} \mid x\rangle$$

Thus the state $\mid s\rangle$ can be written as

$$\mid s\rangle = \frac{1}{\sqrt{N}} \mid \psi_m\rangle + \sqrt{\frac{N-1}{N}} \sum_{x \neq m} \mid x\rangle$$

The operation T inverts the marked state. On applying the diffusion operator D, the amplitude of the marked state increases. Suppose at the j-th iteration, the amplitude of the marked state is m_j and that of each unmarked state is u_j, i.e. after $j-$th iteration, the state is written as $(u_j, u_j, \ldots, u_j, m_j, u_j \ldots u_j)^T$. The diffusion operator $D = -I + \frac{2}{N}J$ will transform this as follows:

$$\begin{pmatrix} u_{j+1} \\ \cdots \\ u_{j+1} \\ m_{j+1} \\ u_{j+1} \\ \cdots \\ u_{j+1} \end{pmatrix} = \begin{pmatrix} -u_j \\ \cdots \\ -u_j \\ -m_j \\ -u_j \\ \cdots \\ -u_j \end{pmatrix} + \frac{2}{N} \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \end{pmatrix} \begin{pmatrix} u_j \\ \cdots \\ u_j \\ m_j \\ u_j \\ \cdots \\ u_j \end{pmatrix}$$

Multiplying the last two matrices and recognising that the expression correspondingto u_{j+1} is the same for all the $N-1$ locations while at the marked location, the expression is different, we may write this as

$$m_{j+1} = \left(\frac{2}{N} - 1\right) m_j + \frac{2}{N}(N-1)u_j \tag{24}$$

$$u_{j+1} = \frac{2}{N} m_j + \frac{N-2}{N} u_j \tag{25}$$

The coupled equations above can be solved. If we assume that at the beginning of each iteration, m_j has been made negative by application of the operator T, we can write

$$m_{j+1} = \left(1 - \frac{2}{N}\right) m_j + \frac{2}{N} u_j \tag{26}$$

$$u_{j+1} = -\frac{2}{N} m_j + \frac{N-2}{N} u_j \tag{27}$$

Define $c_j = \sqrt{N-1}u_j$ This enables us to write the coupled equations as

$$\begin{pmatrix} m_{j+1} \\ c_{j+1} \end{pmatrix} = \begin{pmatrix} 1 - \frac{2}{N} & \frac{2\sqrt{N-1}}{N} \\ -\frac{2\sqrt{N-1}}{N} & \frac{N-2}{N} \end{pmatrix} \begin{pmatrix} m_j \\ c_j \end{pmatrix} \tag{28}$$

$$= \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ -\sin(2\theta) & \cos(2\theta) \end{pmatrix} \begin{pmatrix} m_j \\ c_j \end{pmatrix} \tag{29}$$

where $\sin\theta = \frac{1}{\sqrt{N}}$ and $\cos\theta = \sqrt{1 - \frac{1}{N}}$.

The equations shows that the effect is one of rotation by 2θ. Denoting the rotation matrix above by M, we have

$$\begin{pmatrix} m_j \\ c_j \end{pmatrix} = M^j \begin{pmatrix} m_1 \\ c_1 \end{pmatrix} = M^j \begin{pmatrix} \sin\theta \\ \cos\theta \end{pmatrix} \tag{30}$$

$$= \begin{pmatrix} \sin(2j+1)\theta \\ cos(2j+1)\theta \end{pmatrix} \tag{31}$$

In the above, we have used $m_1 = \frac{1}{\sqrt{N}} = \sin\theta$ and since $(N-1)u_1^2 + m_1^2 = c_1^2 + m_1^2 = 1$, $c_1 = \cos\theta$.

Thus application of Grover iteration k times gives

$$G^k \mid s\rangle = \sin[(2k+1)\theta] \mid \psi_m\rangle + \frac{1}{\sqrt{N-1}} \cos[(2k+1)\theta] \sum_{x \neq m} \mid x\rangle \tag{32}$$

Thus measurement of the first register would yield the marked state with a probability $\sin^2[(2k+1)\theta]$.

8 Example

Consider $N = 8$. Let us assume that the 4th state is marked. Using $D = -I + 2J/N = -I + J/4$. Recall that each element of J is 1. The matrix $G = DT$ is given by

$$\begin{pmatrix} \text{-0.75} & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & \text{-0,75} & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & \text{-0.75} & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.75} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & \text{-0.75} & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & \text{-0.75} & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & \text{-0.75} & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & \text{-0.75} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \text{-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Multiplying the two matrices, one notices that the resulting matrix is different from D in that the fourth column is different.

$$DT = \begin{pmatrix} \text{-0.75} & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & \text{-0,75} & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & \text{-0.75} & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.75 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & \text{-0.75} & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & \text{-0.75} & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & \text{-0.75} & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & \text{-0.75} \end{pmatrix}$$

Thus id the matrix is to act on $(u, u, u, m, u, u, u, u)^T$, we would get, because of symmetry,

$$DT \begin{pmatrix} u \\ u \\ u \\ m \\ u \\ u \\ u \\ u \end{pmatrix} = \begin{pmatrix} 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 1.75u + 0.75m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \end{pmatrix}$$

which shows

$$u_1 = 0.75u_0 - 0.25m_0$$
$$m_1 = 1.75u_0 + 0.75m_0$$

It can be checked that norm is preserved in the transformation $7u_1^2 + m_1^2 = 7u_0^2 + m_0^2$. Thus effectively, n iterations can be performed by application of the following:

$$\begin{pmatrix} u_n \\ m_n \end{pmatrix} = \begin{pmatrix} 0.75 & -0,25 \\ 1.75 & 0.75 \end{pmatrix}^n \begin{pmatrix} u_0 \\ m_0 \end{pmatrix}$$

9 The Quadratic Speeding

We begin by providing a somewhat different interpretation of Grover rotation $R_s = U_s U_w$. The operation of U_w on an arbitrary state flips the sign of the component of $\mid \psi\rangle$ parallel to $\mid w\rangle$. This is followed by the application of the reflection operator U_s on the resulting state. It is instructive to look at the action of U_s on an arbitrary state. Consider its effect on an arbitrary state $\mid \psi\rangle$ where the state is expressed in the computational basis $\{\mid x\rangle\}$

$$\mid \psi\rangle = \sum_x a_x \mid x\rangle \tag{33}$$

Using (4), we have, using $\mid s\rangle = \frac{1}{\sqrt{N}} \sum_x \mid x\rangle$

$$\langle s \mid \psi\rangle = \frac{1}{\sqrt{N}} \sum_{x,x'} a_{x'} \langle x \mid x'\rangle = \frac{1}{\sqrt{N}} \sum_x a_x = \sqrt{N}\bar{a}$$

where $\bar{a} = \frac{1}{N}\sum_x a_x$ is the mean amplitude of $\mid \phi\rangle$ in the computational basis. We then have,

$$\begin{aligned} U_s \mid \psi\rangle &= [2 \mid s\rangle\langle s \mid -I] \mid \psi\rangle \\ &= 2 \mid s\rangle\langle s \mid\mid \psi\rangle - \mid \psi\rangle \\ &= 2\sqrt{N}\bar{a} \mid s\rangle - \mid \psi\rangle \\ &= \sum_x (2\bar{a} - a_x) \mid x\rangle \end{aligned} \tag{34}$$

Equation (34) shows that the amplitude a_x under reflection becomes $2\bar{a} - a_x$ so that the amplitude of the state with respect to the mean $a_x - \bar{a}$ becomes $\bar{a} - a_x$, i.e. it gets inverted. To illustrate this consider the case of $N = 8$. In the state $\mid s\rangle$ each of the state in the computational basis has an amplitude $\frac{1}{2\sqrt{2}}$. In Figure 5 the top panel shows equal amplitude of the eight states in $\mid s\rangle$. Since each state has the same amplitude, the mean is also $\frac{1}{2\sqrt{2}}$. The application of U_w on the state $\mid s\rangle$ inverts the component parallel to $\mid w\rangle$. In the figure, we have taken the marked state $\mid w\rangle$ to be the 4th state so that in the second panel, only the 4th component is shown inverted. Calling this state $\mid \phi\rangle$, we have the amplitude $a_w = -\frac{1}{2\sqrt{2}}$ and $a_x = \frac{1}{2\sqrt{2}}$ for all $x \neq w$. Thus the mean amplitude at this stage is $\frac{1}{8}\left(7\frac{1}{2\sqrt{2}} - \frac{1}{2\sqrt{2}}\right) = \frac{3}{8\sqrt{2}}$. An application of U_s on this state will let $a_x \rightarrow 2\bar{a} - a_x$, i.e., for all states other than the marked state $\mid w\rangle$, the amplitude will become $a_{x'} = \frac{3}{4\sqrt{2}} - \frac{1}{2\sqrt{2}} = \frac{1}{2\sqrt{2}}$. The amplitude of the marked state $\mid w\rangle$ becomes $a_{w'} = \frac{3}{4\sqrt{2}} + \frac{1}{2\sqrt{2}} = \frac{5}{4\sqrt{2}}$ which has a magnitude five times that of each of the other component, i.e., the probability density of the state is amplified 25 times with respect to each of the ummarked states.

10 Maximum Number of Iteration

We saw that the function of the Grover operator R_G is to selectively amplify the amplitude of the state $\mid w\rangle$. The angle between $\mid s\rangle$ and $\mid w\rangle$ is $\frac{\pi}{2} - \theta$. thus the number of iteration should be such that $\mid s\rangle$ is rotated by an angle as close to $\frac{\pi}{2} - \theta$ as possible. This requires an *a priori* knowledge of the number of iteration.

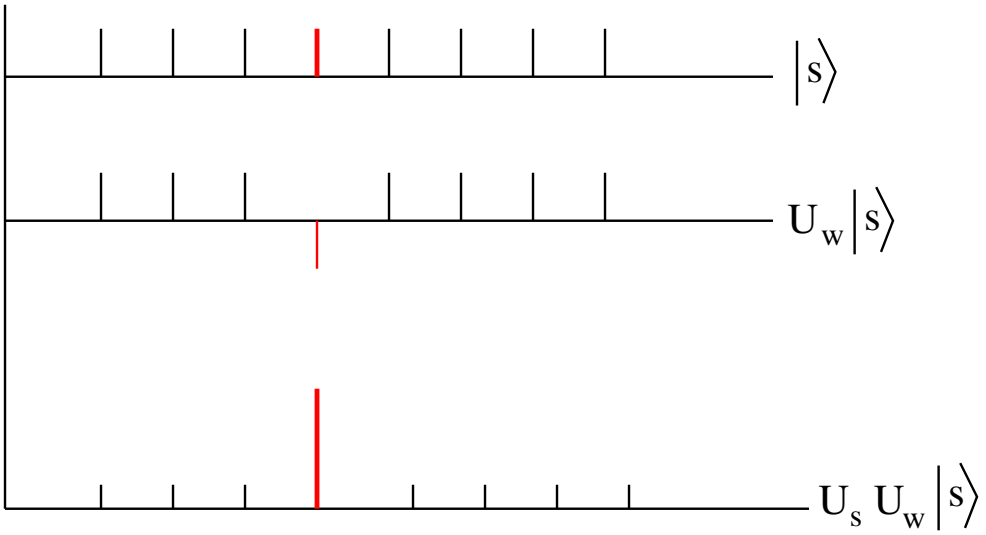

Figure 5: Selective Amplification

We can get an estimate of the number of iterations m for large N for which $\sin\theta \approx \theta = \frac{1}{\sqrt{N}}$. For this we require

$$m \times 2\theta \approx \frac{\pi}{2} - \theta$$

which gives

$$m = \frac{\pi}{4\theta} - 2$$

The number of iterations for large N is, therefore, given by

$$m \approx \frac{\pi}{4}\sqrt{N} \tag{35}$$

which shows that unlike the classical search, the number of queries is $O(\sqrt{N})$. after m iterations, the angle between $\mid s\rangle$ and $\mid w\rangle$ is $\frac{\pi}{2} - (2m+1)\theta$ which gives the amplitude of the state $\mid w\rangle$ in $\mid s\rangle$ to be

$$\begin{aligned} \mid \sin(2m+1)\theta \mid &= \left|\sin\left((\frac{\pi}{2}\sqrt{N}+1)\frac{1}{\sqrt{N}}\right)\right| \\ &= \left|\sin\left(\frac{\pi}{2}+\frac{1}{\sqrt{N}}\right)\right| \\ &= \mid \cos\frac{1}{\sqrt{N}} \mid \\ &\approx 1 - \frac{1}{2N} \end{aligned} \tag{36}$$

which shows the amplitude to be very close to 1. This shows the quadratic acceleration of the algorithm referred to in the introduction. Figure 6 shows that for N=4096, the maximum amplitude is obtained by iterating the algorithm 49 times after which it starts decreasing again, which is in agreement with the large N formula (35) obtained above.

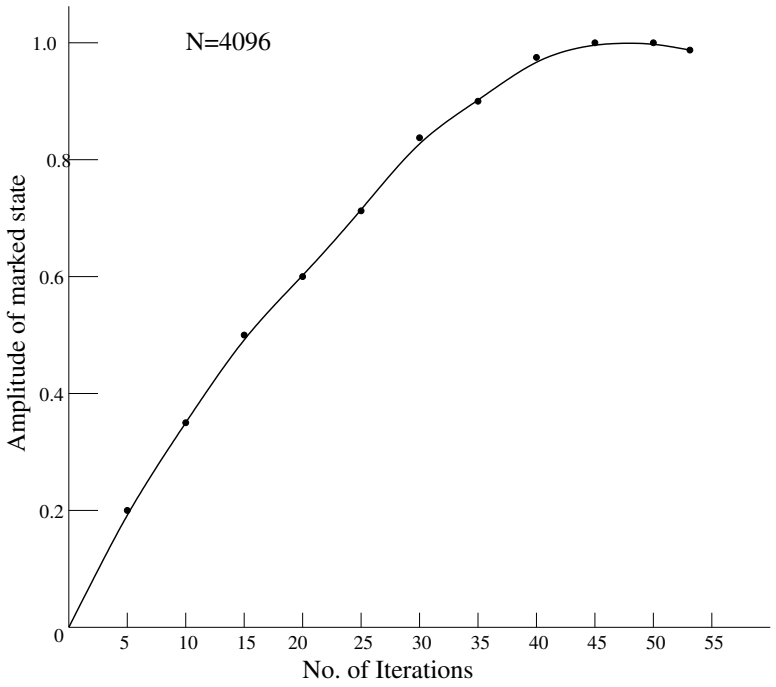

Figure 6: Grover Iterations for N=4096

11 Matrix Representation of Grover Operator

Grover's algorithm is implemented in the following steps.

1. We first construct a state $\mid s\rangle$ which is a uniform linear combination of N states in the computational basis. This is obtained by starting with an initial state $\mid 0\rangle^{\otimes n}$ and subjecting it to Hadamard transform, which gives
$$\mid s\rangle = \frac{1}{2^{n/2}} \sum_x \mid x\rangle$$
2. The $(n+1)$-th quit is initialised to $\mid y\rangle = \dfrac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$

we carry out repeated Grover iteration, starting with the standard state $\mid s\rangle$. Such iterations will randomise the state $\mid s\rangle$. It is thus instructive to see what these do, acting on an arbitrary state $\mid \psi\rangle = \sum_k a(k) \mid k\rangle$. We perform the following steps m times, where m will be computed later.

1. Apply the oracle. Here we calculate the value of the unitary map U_f and XOR it with the last qubit to obtain a phase factor $(-1)^{f(x)}$.
$$\mid s\rangle \mid y\rangle \rightarrow \sum_{x=0}^{N-1} a_x \mid x\rangle (-1)^{f(x)} \mid y\rangle$$
(Initially $a_x = \dfrac{1}{\sqrt{N}}$ for each x). We denote this transformation by T.

2. Now apply on the resulting state a "diffusion operator" D defined below.

The matrix elements of the diffusion matrix is defined as follows:

$$D_{ii} = -1 + \frac{2}{N}$$
$$D_{ij} = \frac{2}{N}, \quad \text{for } i \neq j \tag{37}$$

It is easily seen that if we define a $N \times N$ matrix J which has each element as 1, the "diffusion operator" has the representation

$$D = -I + \frac{2J}{N} \tag{38}$$

It is easily checked that $\frac{J}{N}$ is a projection operator as $\frac{J}{N} = \left(\frac{J}{N}\right)^2$. Using this, it follows that D is unitary. Since each element of J is 1, it follows that acting on a column vector $(a_1, a_2, \ldots, a_N)^T$, we get

$$\frac{J}{N}\begin{pmatrix} a_1 \\ a_2 \\ \ldots \\ \ldots \\ a_N \end{pmatrix} = \begin{pmatrix} \frac{a_1 + a_2 + \ldots + a_N}{N} \\ \frac{a_1 + a_2 + \ldots + a_N}{N} \\ \ldots \\ \ldots \\ \frac{a_1 + a_2 + \ldots + a_N}{N} \end{pmatrix} = \begin{pmatrix} \bar{a} \\ \bar{a} \\ \ldots \\ \ldots \\ \bar{a} \end{pmatrix} \tag{39}$$

where $\bar{a} = \frac{1}{N}\sum_i a_i$. Thus if we take an arbitrary vector $\mid v\rangle = \sum_x v_x \mid x\rangle$ in a basis $\{\mid x\rangle\}$, we get,

$$\frac{J}{N} \mid v\rangle = \frac{J}{N}\sum_x v_x \mid x\rangle = \sum_x \bar{v} \mid x\rangle$$

Thus the action of the diffusion operator on an arbitrary vector is given by the following.

$$\begin{aligned} D \mid v\rangle &= \left(-I + \frac{J}{N}\right) \mid v\rangle = - \mid v\rangle + 2\sum_x \bar{v} \mid x\rangle \\ &= -\sum_x v_x \mid x\rangle + 2\sum_x \bar{v} \mid x\rangle \\ &= \sum_x (2\bar{v} - v_x) \mid x\rangle \end{aligned} \tag{40}$$

This shows that the diffusion operator D represents the Grover operator $U_s = -I + 2\langle s \mid\mid s\rangle$.

The diffusion operator defined above can be obtained by application of the following sequence of operators:

$$D = WRW \tag{41}$$

where W is the Walsh Hadamard transform whose elements are given by

$$W_{ij} = \frac{1}{\sqrt{N}}(-1)^{i\cdot j} \tag{42}$$

so that the Walsh-Hadamard transform of an $n-$ qubit state $\mid x\rangle$ is given by

$$H^{\otimes n} \mid x\rangle = \frac{1}{\sqrt{N}} \sum_{y} (-1)^{x\cdot y} \mid y\rangle \tag{43}$$

where $x \cdot y$ represents the sum bitwise product of the two strings x and y. The operator R is a selective phase rotation which is a diagonal matrix with its first element as 1 and others equal to -1.The matrix R can be represented as

$$R_{ij} = (2\delta_{i,0} - 1)\delta_{i,j} \equiv (-1)^{1-\delta_{i,0}}\delta_{i,j} \tag{44}$$

To show (15), we will consider the matrix elements of both sides of the equation in arbitrary states $\mid x\rangle$ and $\mid y\rangle$ and show that

$$\langle x \mid WRW \mid y\rangle = \langle x \mid D \mid y\rangle \tag{45}$$

Consider the r.h.s of (19). We have,

$$\begin{aligned} \langle x \mid WRW \mid y\rangle &= \sum_{u,v} \langle x \mid W \mid u\rangle\langle u \mid R \mid v\rangle\langle v \mid W \mid y\rangle \\ &= \frac{1}{N} \sum_{u,v} (-1)^{x\cdot u} \cdot (-1)^{1-\delta_{u,0}}\delta_{u,v} \cdot (-1)^{v\cdot y} \end{aligned} \tag{46}$$

where we have used (16) and (18). We will now perform the sum over u on the right of (20). We have, splitting the sum into a term for which $u = 0$ and another for which $u \neq 0$,

$$\begin{aligned} \sum_{u} (-1)^{x\cdot u} \cdot (-1)^{1-\delta_{u,0}}\delta_{u,v} &= (-1)^0(-1)^0\delta_{0,v} - \sum_{u=1}^{N} (-1)^{x\cdot u}\delta_{u,v} \\ &= 2\delta_{0,v} - \sum_{u=0}^{N} (-1)^{x\cdot u}\delta_{u,v} \\ &= 2\delta_{0,v} - \sum_{u=0}^{N} (-1)^{x_{n-1}u_{n-1}+\ldots+x_0u_0}\delta u_{n-1}, v_{n-1}\delta u_{n-2}, v_{n-2}\ldots\delta u_0, v_0 \\ &= 2\delta_{0,v} - \left(\sum_{u_{n-1}=0}^{1} (-1)^{x_{n-1}u_{n-1}}\delta u_{n-1}, v_{n-1}\right)\left(\sum_{u_{n-2}=0}^{1} (-1)^{x_{n-2}u_{n-2}}\delta u_{n-2}, v_{n-2}\right)\ldots \end{aligned} \tag{47}$$

In (21), in the second line, we have once again added and subtracted $u = 0$ term and in the third line we have written explicitly in terms of the bits.

Substituting (21) into the r.h.s. of (20), we can write the r.h.s as

$$\begin{aligned} r.h.s. &= \frac{1}{N}\sum_{v=0}^{N-1}\left[2\delta_{0,v} - \left(\sum_{u_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}}\delta u_{n-1}, v_{n-1}\right)\ldots\left(\sum_{u_0=0}^{1}(-1)^{x_0u_0}\delta u_0, v_0\right)\right]\times(-1)^{v\cdot y} \\ &= \frac{2}{N} - \frac{1}{N}\left[\left(\sum_{u_{n-1},v_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}+v_{n-1}y_{n-1}}\delta u_{n-1}, v_{n-1}\right)\ldots\left(\sum_{u_0,v_0=0}^{1}(-1)^{x_0u_0+v_0y_0}\delta u_0, v_0\right)\right] \\ &= \frac{2}{N} - \frac{1}{N}\left(1+(-1)^{x_{n-1}+y_{n-1}}\right)\ldots\left(1+(-1)^{x_0+y_0}\right) \\ &= \frac{2}{N} - \frac{2^n}{N}\delta_{x_{n-1},y_{n-1}}\ldots\delta_{x_0,y_0} \\ &= \frac{2}{N} - \delta_{x,y} \end{aligned} \tag{48}$$

Returning to the l.h.s of (20), we have, using $D = -I + 2 \mid s\rangle\langle s \mid$,

$$\begin{aligned} \langle x \mid D \mid y\rangle &= -\delta_{x,y} + 2\langle x \mid s\rangle\langle s \mid y\rangle \\ &= -\delta_{x,y} - 2\frac{1}{\sqrt{N}}\frac{1}{\sqrt{N}} \\ &= \frac{2}{N} - \delta_{x,y} \end{aligned} \tag{49}$$

Comparing (22) and (23), the relation (19) and hence (15) follows.

12 Quantum Circuit

The steps in the above analysis can be summarised as follows:

1. Construct an equal superposition of basis states starting with $\mid 0\rangle^{\otimes n}$. The $(n+1)$-th quit is set as $\mid y\rangle = \frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$. Thus we start with $\mid \psi_0\rangle = \sum_x a_x \mid x\rangle \mid y\rangle$ with $a_x = \frac{1}{\sqrt{N}}$ for all x.

2. Apply the oracle U_f which computes $f(x)$ to produce the phase factor $(-1)^{f(x)}$. Thus
$$\mid \psi_0\rangle \mid y\rangle \rightarrow \sum_{x=0}^{N-1} a_x \mid x\rangle(-1)^{f(x)} \mid y\rangle$$
This transformation will be denoted by T.

3. Apply the diffusion operator $D = WRW$ which isa Hadamard transform followed by a phase shift R followed by yet another Hadamard transform.

4. apply steps 2 and 3 $O(\sqrt{N})$ times.

5. Measure the state of the first register. with a very high degree of probability, it would identify the marked state. If it fails (probability $O(1/N)$), go back to step 1.

A schematic circuit representation for the above is given below:

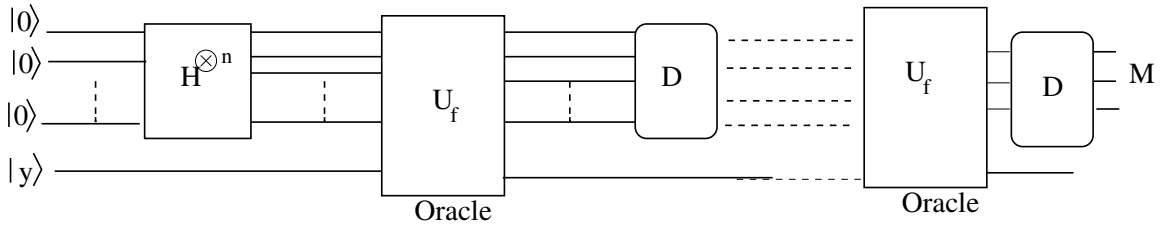

Figure 7: Schematic Circuit for Grover Algorithm

13 Success and Failure of Algorithm

Let us denote the marked state as $\mid \psi_m\rangle$ and unmarked state as $\mid \psi_u\rangle$,

$$\mid \psi_u\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq m} \mid x\rangle$$

Thus the state $\mid s\rangle$ can be written as

$$\mid s\rangle = \frac{1}{\sqrt{N}} \mid \psi_m\rangle + \sqrt{\frac{N-1}{N}} \sum_{x \neq m} \mid x\rangle$$

The operation T inverts the marked state. On applying the diffusion operator D, the amplitude of the marked state increases. Suppose at the j-th iteration, the amplitude of the marked state is m_j and that of each unmarked state is u_j, i.e. after $j-$th iteration, the state is written as $(u_j, u_j, \ldots, u_j, m_j, u_j \ldots u_j)^T$. The diffusion operator $D = -I + \frac{2}{N}J$ will transform this as follows:

$$\begin{pmatrix} u_{j+1} \\ \cdots \\ u_{j+1} \\ m_{j+1} \\ u_{j+1} \\ \cdots \\ u_{j+1} \end{pmatrix} = \begin{pmatrix} -u_j \\ \cdots \\ -u_j \\ -m_j \\ -u_j \\ \cdots \\ -u_j \end{pmatrix} + \frac{2}{N} \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \end{pmatrix} \begin{pmatrix} u_j \\ \cdots \\ u_j \\ m_j \\ u_j \\ \cdots \\ u_j \end{pmatrix}$$

Multiplying the last two matrices and recognising that the expression correspondingto u_{j+1} is the same for all the $N-1$ locations while at the marked location, the expression

is different, we may write this as

$$m_{j+1} = \left(\frac{2}{N} - 1\right) m_j + \frac{2}{N}(N-1)u_j \tag{50}$$

$$u_{j+1} = \frac{2}{N} m_j + \frac{N-2}{N} u_j \tag{51}$$

The coupled equations above can be solved. If we assume that at the beginning of each iteration, m_j has been made negative by application of the operator T, we can write

$$m_{j+1} = \left(1 - \frac{2}{N}\right) m_j + \frac{2}{N} u_j \tag{52}$$

$$u_{j+1} = -\frac{2}{N} m_j + \frac{N-2}{N} u_j \tag{53}$$

Define $c_j = \sqrt{N-1}u_j$ This enables us to write the coupled equations as

$$\begin{pmatrix} m_{j+1} \\ c_{j+1} \end{pmatrix} = \begin{pmatrix} 1 - \frac{2}{N} & \frac{2\sqrt{N-1}}{N} \\ -\frac{2\sqrt{N-1}}{N} & \frac{N-2}{N} \end{pmatrix} \begin{pmatrix} m_j \\ c_j \end{pmatrix} \tag{54}$$

$$= \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ -\sin(2\theta) & \cos(2\theta) \end{pmatrix} \begin{pmatrix} m_j \\ c_j \end{pmatrix} \tag{55}$$

where $\sin\theta = \frac{1}{\sqrt{N}}$ and $\cos\theta = \sqrt{1 - \frac{1}{N}}$.

The equations shows that the effect is one of rotation by 2θ. Denoting the rotation matrix above by M, we have

$$\begin{pmatrix} m_j \\ c_j \end{pmatrix} = M^j \begin{pmatrix} m_1 \\ c_1 \end{pmatrix} = M^j \begin{pmatrix} \sin\theta \\ \cos\theta \end{pmatrix} \tag{56}$$

$$= \begin{pmatrix} \sin(2j+1)\theta \\ cos(2j+1)\theta \end{pmatrix} \tag{57}$$

In the above, we have used $m_1 = \frac{1}{\sqrt{N}} = \sin\theta$ and since $(N-1)u_1^2 + m_1^2 = c_1^2 + m_1^2 = 1$, $c_1 = \cos\theta$.

Thus application of Grover iteration k times gives

$$G^k \mid s\rangle = \sin[(2k+1)\theta] \mid \psi_m\rangle + \frac{1}{\sqrt{N-1}} \cos[(2k+1)\theta] \sum_{x \neq m} \mid x\rangle \tag{58}$$

Thus measurement of the first register would yield the marked state with a probability $\sin^2[(2k+1)\theta]$.

14 Example

Consider $N = 8$. Let us assume that the 4th state is marked. Using $D = -I + 2J/N = -I + J/4$. Recall that each element of J is 1. The matrix $G = DT$ is given by

$$\begin{pmatrix} \text{-0.75} & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & \text{-0,75} & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & \text{-0.75} & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.75} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & \text{-0.75} & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & \text{-0.75} & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & \text{-0.75} & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & \text{-0.75} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \text{-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Multiplying the two matrices, one notices that the resulting matrix is different from D in that the fourth column is different.

$$DT = \begin{pmatrix} \text{-0.75} & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & \text{-0,75} & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & \text{-0.75} & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.75 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & \text{-0.75} & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & \text{-0.75} & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & \text{-0.75} & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & \text{-0.75} \end{pmatrix}$$

Thus id the matrix is to act on $(u, u, u, m, u, u, u, u)^T$, we would get, because of symmetry,

$$DT \begin{pmatrix} u \\ u \\ u \\ m \\ u \\ u \\ u \\ u \end{pmatrix} = \begin{pmatrix} 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 1.75u + 0.75m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \end{pmatrix}$$

which shows

$$u_1 = 0.75u_0 - 0.25m_0$$
$$m_1 = 1.75u_0 + 0.75m_0$$

It can be checked that norm is preserved in the transformation $7u_1^2 + m_1^2 = 7u_0^2 + m_0^2$. Thus effectively, n iterations can be performed by application of the following:

$$\begin{pmatrix} u_n \\ m_n \end{pmatrix} = \begin{pmatrix} 0.75 & -0,25 \\ 1.75 & 0.75 \end{pmatrix}^n \begin{pmatrix} u_0 \\ m_0 \end{pmatrix}$$

15 Matrix Representation of Grover Operator

Grover's algorithm is implemented in the following steps, using a matrix representation.

1. We first construct a state $\mid s\rangle$ which is a uniform linear combination of N states in the computational basis. This is obtained by starting with an initial state $\mid 0\rangle^{\otimes n}$ and subjecting it to Hadamard transform, which gives

$$\mid s\rangle = \frac{1}{2^{n/2}} \sum_x \mid x\rangle$$

2. The $(n+1)$-th quit is initialised to $\mid y\rangle = \dfrac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$

we carry out repeated Grover iteration, starting with the standard state $\mid s\rangle$. Such iterations will randomise the state $\mid s\rangle$. It is thus instructive to see what these do, acting on an arbitrary state $\mid \psi\rangle = \sum_k a(k) \mid k\rangle$. We perform the following steps m times, where m will be computed later.

1. Apply the oracle. Here we calculate the value of the unitary map U_f and XOR it with the last qubit to obtain a phase factor $(-1)^{f(x)}$.

$$\mid s\rangle \mid y\rangle \rightarrow \sum_{x=0}^{N-1} a_x \mid x\rangle (-1)^{f(x)} \mid y\rangle$$

   (Initially $a_x = \dfrac{1}{\sqrt{N}}$ for each x). We denote this transformation by T.

2. Now apply on the resulting state a "diffusion operator" D defined below.

The matrix elements of the diffusion matrix is defined as follows:

$$\begin{aligned} D_{ii} &= -1 + \frac{2}{N} \\ D_{ij} &= \frac{2}{N}, \quad \text{for } i \neq j \end{aligned} \tag{59}$$

It is easily seen that if we define a $N \times N$ matrix J which has each element as 1, the "diffusion operator" has the representation

$$D = -I + \frac{2J}{N} \tag{60}$$

It is easily checked that $\dfrac{J}{N}$ is a projection operator as $\dfrac{J}{N} = \left(\dfrac{J}{N}\right)^2$. Using this, it follows that D is unitary. Since each element of J is 1, it follows that acting on a column vector

$(a_1, a_2, \ldots, a_N)^T$, we get

$$\frac{J}{N}\begin{pmatrix} a_1 \\ a_2 \\ \ldots \\ \ldots \\ a_N \end{pmatrix} = \begin{pmatrix} \frac{a_1+a_2+\ldots+a_N}{N} \\ \frac{a_1+a_2+\ldots+a_N}{N} \\ \ldots \\ \ldots \\ \frac{a_1+a_2+\ldots+a_N}{N} \end{pmatrix} = \begin{pmatrix} \bar{a} \\ \bar{a} \\ \ldots \\ \ldots \\ \bar{a} \end{pmatrix} \tag{61}$$

where $\bar{a} = \frac{1}{N}\sum_i a_i$. Thus if we take an arbitrary vector $\mid v\rangle = \sum_x v_x \mid x\rangle$ in a basis $\{\mid x\rangle\}$, we get,

$$\frac{J}{N} \mid v\rangle = \frac{J}{N}\sum_x v_x \mid x\rangle = \sum_x \bar{v} \mid x\rangle$$

Thus the action of the diffusion operator on an arbitrary vector is given by the following.

$$\begin{aligned} D \mid v\rangle &= \left(-I + \frac{J}{N}\right) \mid v\rangle = - \mid v\rangle + 2\sum_x \bar{v} \mid x\rangle \\ &= -\sum_x v_x \mid x\rangle + 2\sum_x \bar{v} \mid x\rangle \\ &= \sum_x (2\bar{v} - v_x) \mid x\rangle \end{aligned} \tag{62}$$

This shows that the diffusion operator D represents the Grover operator $U_s = -I + 2 \mid s\rangle\langle s \mid$. The diffusion operator defined above can be obtained by application of the following sequence of operators:

$$D = WRW \tag{63}$$

where W is the Walsh Hadamard transform whose elements are given by

$$W_{ij} = \frac{1}{\sqrt{N}}(-1)^{i.j} \tag{64}$$

so that the Walsh-Hadamard transform of an $n-$ qubit state $\mid x\rangle$ is given by

$$H^{\otimes n} \mid x\rangle = \frac{1}{\sqrt{N}}\sum_y (-1)^{x\cdot y} \mid y\rangle \tag{65}$$

where $x \cdot y$ represents the sum bitwise product of the two strings x and y. The operator R is a selective phase rotation which is a diagonal matrix with its first element as 1 and others equal to -1.The matrix R can be represented as

$$R_{ij} = (2\delta_{i,0} - 1)\delta_{i,j} \equiv (-1)^{1-\delta_{i,0}}\delta_{i,j} \tag{66}$$

To show (15), we will consider the matrix elements of both sides of the equation in arbitrary states $\mid x\rangle$ and $\mid y\rangle$ and show that

$$\langle x \mid WRW \mid y\rangle = \langle x \mid D \mid y\rangle \tag{67}$$

Consider the r.h.s of (19). We have,

$$\begin{aligned}\langle x \mid WRW \mid y\rangle &= \sum_{u,v}\langle x \mid W \mid u\rangle\langle u \mid R \mid v\rangle\langle v \mid W \mid y\rangle \\ &= \frac{1}{N}\sum_{u,v}(-1)^{x\cdot u}\cdot(-1)^{1-\delta_{u,0}}\delta_{u,v}\cdot(-1)^{v\cdot y} \qquad (68)\end{aligned}$$

where we have used (16) and (18). We will now perform the sum over u on the right of (20). We have, splitting the sum into a term for which $u = 0$ and another for which $u \neq 0$,

$$\begin{aligned}\sum_{u}(-1)^{x\cdot u}\cdot(-1)^{1-\delta_{u,0}}\delta_{u,v} &= (-1)^0(-1)^0\delta_{0,v} - \sum_{u=1}^{N}(-1)^{x\cdot u}\delta_{u,v} \\ &= 2\delta_{0,v} - \sum_{u=0}^{N}(-1)^{x\cdot u}\delta_{u,v} \\ &= 2\delta_{0,v} - \sum_{u=0}^{N}(-1)^{x_{n-1}u_{n-1}+\ldots+x_0u_0}\delta u_{n-1},v_{n-1}\delta u_{n-2},v_{n-2}\ldots\delta u_0,v_0 \\ &= 2\delta_{0,v} - \left(\sum_{u_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}}\delta u_{n-1},v_{n-1}\right)\left(\sum_{u_{n-2}=0}^{1}(-1)^{x_{n-2}u_{n-2}}\delta u_{n-2},v_{n-2}\right)\ldots \qquad (69)\end{aligned}$$

In (21), in the second line, we have once again added and subtracted $u = 0$ term and in the third line we have written explicitly in terms of the bits.
Substituting (21) into the r.h.s. of (20), we can write the r.h.s as

$$\begin{aligned}r.h.s. &= \frac{1}{N}\sum_{v=0}^{N-1}\left[2\delta_{0,v} - \left(\sum_{u_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}}\delta u_{n-1},v_{n-1}\right)\ldots\left(\sum_{u_0=0}^{1}(-1)^{x_0u_0}\delta u_0,v_0\right)\right]\times(-1)^{v\cdot y} \\ &= \frac{2}{N} - \frac{1}{N}\left[\left(\sum_{u_{n-1},v_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}+v_{n-1}y_{n-1}}\delta u_{n-1},v_{n-1}\right)\ldots\left(\sum_{u_0,v_0=0}^{1}(-1)^{x_0u_0+v_0y_0}\delta u_0,v_0\right)\right] \\ &= \frac{2}{N} - \frac{1}{N}\left(1+(-1)^{x_{n-1}+y_{n-1}}\right)\ldots\left(1+(-1)^{x_0+y_0}\right) \\ &= \frac{2}{N} - \frac{2^n}{N}\delta_{x_{n-1},y_{n-1}}\ldots\delta_{x_0,y_0} \\ &= \frac{2}{N} - \delta_{x,y} \qquad (70)\end{aligned}$$

Returning to the l.h.s of (20), we have, using $D = -I + 2 \mid s\rangle\langle s \mid$,

$$\begin{aligned}\langle x \mid D \mid y\rangle &= -\delta_{x,y} + 2\langle x \mid s\rangle\langle s \mid y\rangle \\ &= -\delta_{x,y} - 2\frac{1}{\sqrt{N}}\frac{1}{\sqrt{N}} \\ &= \frac{2}{N} - \delta_{x,y} \qquad (71)\end{aligned}$$

Comparing (22) and (23), the relation (19) and hence (15) follows.

16 Quantum Circuit

The steps in the above analysis can be summarized as follows:

1. Construct an equal superposition of basis states starting with $\mid 0\rangle^{\otimes n}$. The $(n+1)$-th quit is set as $\mid y\rangle = \frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}}$. Thus we start with $\mid \psi_0\rangle = \sum_x a_x \mid x\rangle \mid y\rangle$ with $a_x = \frac{1}{\sqrt{N}}$ for all x.

2. Apply the oracle U_f which computes $f(x)$ to produce the phase factor $(-1)^{f(x)}$. Thus
$$\mid \psi_0\rangle \mid y\rangle \rightarrow \sum_{x=0}^{N-1} a_x \mid x\rangle (-1)^{f(x)} \mid y\rangle$$
This transformation will be denoted by T.

3. Apply the diffusion operator $D = WRW$ which isa Hadamard transform followed by a phase shift R followed by yet another Hadamard transform.

4. apply steps 2 and 3 $O(\sqrt{N})$ times.

5. Measure the state of the first register. with a very high degree of probability, it would identify the marked state. If it fails (probability $O(1/N)$), go back to step 1.

A schematic circuit representation for the above is given below:

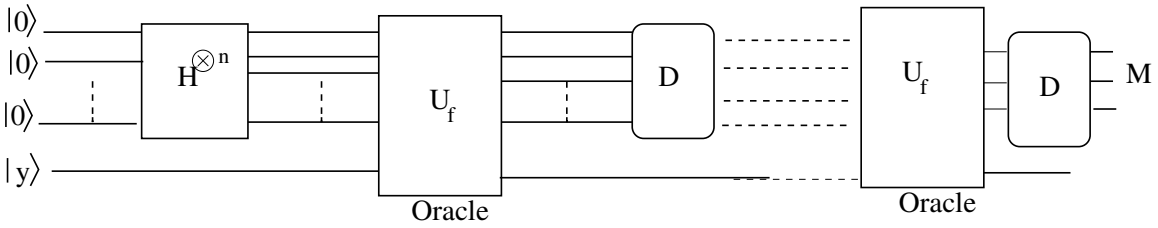

Figure 8: Schematic Circuit for Grover Algorithm

17 Success and Failure of Algorithm

Let us denote the marked state as $\mid \psi_m\rangle$ and unmarked state as $\mid \psi_u\rangle$,
$$\mid \psi_u\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq m} \mid x\rangle$$

Thus the state $\mid s\rangle$ can be written as
$$\mid s\rangle = \frac{1}{\sqrt{N}} \mid \psi_m\rangle + \sqrt{\frac{N-1}{N}} \sum_{x \neq m} \mid x\rangle$$

The operation T inverts the marked state. On applying the diffusion operator D, the amplitude of the marked state increases. Suppose at the j-th iteration, the amplitude of the marked state is m_j and that of each unmarked state is u_j, i.e. after $j-$th iteration, the state is written as $(u_j, u_j, \ldots, u_j, m_j, u_j \ldots u_j)^T$. The diffusion operator $D = -I + \frac{2}{N}J$ will transform this as follows:

$$\begin{pmatrix} u_{j+1} \\ \cdots \\ u_{j+1} \\ m_{j+1} \\ u_{j+1} \\ \cdots \\ u_{j+1} \end{pmatrix} = \begin{pmatrix} -u_j \\ \cdots \\ -u_j \\ -m_j \\ -u_j \\ \cdots \\ -u_j \end{pmatrix} + \frac{2}{N} \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1 & 1 \\ 1 & 1 & \ldots & 1 & 1 \end{pmatrix} \begin{pmatrix} u_j \\ \cdots \\ u_j \\ m_j \\ u_j \\ \cdots \\ u_j \end{pmatrix}$$

Multiplying the last two matrices and recognising that the expression corresponding to u_{j+1} is the same for all the $N-1$ locations while at the marked location, the expression is different, we may write this as

$$m_{j+1} = \left(\frac{2}{N} - 1\right) m_j + \frac{2}{N}(N-1)u_j \tag{72}$$

$$u_{j+1} = \frac{2}{N}m_j + \frac{N-2}{N}u_j \tag{73}$$

The coupled equations above can be solved. If we assume that at the beginning of each iteration, m_j has been made negative by application of the operator T, we can write

$$m_{j+1} = \left(1 - \frac{2}{N}\right) m_j + \frac{2}{N}u_j \tag{74}$$

$$u_{j+1} = -\frac{2}{N}m_j + \frac{N-2}{N}u_j \tag{75}$$

We will look into the solution of this pair of equations in the next lecture and illustrate the solution with an example.

Define $c_j = \sqrt{N-1}u_j$ This enables us to write the coupled equations as

$$\begin{pmatrix} m_{j+1} \\ c_{j+1} \end{pmatrix} = \begin{pmatrix} 1 - \frac{2}{N} & \frac{2\sqrt{N-1}}{N} \\ -\frac{2\sqrt{N-1}}{N} & \frac{N-2}{N} \end{pmatrix} \begin{pmatrix} m_j \\ c_j \end{pmatrix} \tag{76}$$

$$= \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ -\sin(2\theta) & \cos(2\theta) \end{pmatrix} \begin{pmatrix} m_j \\ c_j \end{pmatrix} \tag{77}$$

where $\sin\theta = \frac{1}{\sqrt{N}}$ and $\cos\theta = \sqrt{1 - \frac{1}{N}}$.

The equations shows that the effect is one of rotation by 2θ. Denoting the rotation matrix above by M, we have

$$\begin{pmatrix} m_j \\ c_j \end{pmatrix} = M^j \begin{pmatrix} m_1 \\ c_1 \end{pmatrix} = M^j \begin{pmatrix} \sin\theta \\ \cos\theta \end{pmatrix} \tag{78}$$

$$= \begin{pmatrix} \sin(2j+1)\theta \\ cos(2j+1)\theta \end{pmatrix} \tag{79}$$

In the above, we have used $m_1 = \dfrac{1}{\sqrt{N}} = \sin\theta$ and since $(N-1)u_1^2 + m_1^2 = c_1^2 + m_1^2 = 1$, $c_1 = \cos\theta$.

Thus application of Grover iteration k times gives

$$G^k \mid s\rangle = \sin[(2k+1)\theta] \mid \psi_m\rangle + \frac{1}{\sqrt{N-1}} \cos[(2k+1)\theta] \sum_{x \neq m} \mid x\rangle \tag{80}$$

Thus measurement of the first register would yield the marked state with a probability $\sin^2[(2k+1)\theta]$.

18 Example

Consider $N = 8$. Let us assume that the 4th state is marked. Using $D = -I + 2J/N = -I + J/4$. Recall that each element of J is 1. The matrix $G = DT$ is given by

$$\begin{pmatrix} \text{-0.75} & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & \text{-0,75} & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & \text{-0.75} & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.75} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & \text{-0.75} & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & \text{-0.75} & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & \text{-0.75} & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.25 & 0.25 & 0.25 & 0.25 & \text{-0.75} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \text{-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Multiplying the two matrices, one notices that the resulting matrix is different from D in that the fourth column is different.

$$DT = \begin{pmatrix} \text{-0.75} & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & \text{-0,75} & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & \text{-0.75} & \text{-0.25} & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & 0.75 & 0.25 & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & \text{-0.75} & 0.25 & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & \text{-0.75} & 0.25 & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & \text{-0.75} & 0.25 \\ 0.25 & 0,25 & 0.25 & \text{-0.25} & 0.25 & 0.25 & 0.25 & \text{-0.75} \end{pmatrix}$$

Thus id the matrix is to act on $(u, u, u, m, u, u, u, u)^T$, we would get, because of symmetry,

$$DT \begin{pmatrix} u \\ u \\ u \\ m \\ u \\ u \\ u \\ u \end{pmatrix} = \begin{pmatrix} 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 1.75u + 0.75m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \\ 0.75u - 0.25m \end{pmatrix}$$

which shows

$$u_1 = 0.75u_0 - 0.25m_0$$
$$m_1 = 1.75u_0 + 0.75m_0$$

It can be checked that norm is preserved in the transformation $7u_1^2 + m_1^2 = 7u_0^2 + m_0^2$. Thus effectively, n iterations can be performed by application of the following:

$$\begin{pmatrix} u_n \\ m_n \end{pmatrix} = \begin{pmatrix} 0.75 & -0,25 \\ 1.75 & 0.75 \end{pmatrix}^n \begin{pmatrix} u_0 \\ m_0 \end{pmatrix}$$