# WiDS QRL - Quantum Search

Nilabha Saha

January 2023

## 1 Quantum Search

### 1.1 The Oracle

Suppose we wish to search through a zero-indexed search space of $N$ elements. For convenience, we assume $N = 2^n$, so that the index can be stored in $n$ bits, and we assume that the search problem has exactly $M$ solutions where $1 \leq M \leq N$. A particular instance of the search problem can be represented by a function $f$ defined as $f(x) = 1$ if $x$ is a solution to the search problem, and $f(x) = 0$ if $x$ is not a solution to the search problem. We assume that we are supplied with a *quantum oracle* - a black box with the ability to recognise solutions to the search problem signalled by making use of an *oracle qubit*.
The oracle is a unitary operator $O$ defined by its action on the computational basis:

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$$

where $|x\rangle$ is the *index register*, and $|q\rangle$ is the oracle qubit.
If the oracle is applied with the oracle qubit in the state $|-\rangle$, then the action of the oracle is given as:

$$|x\rangle(|-\rangle) \xrightarrow{O} (-1)^{f(x)}|x\rangle|-\rangle$$

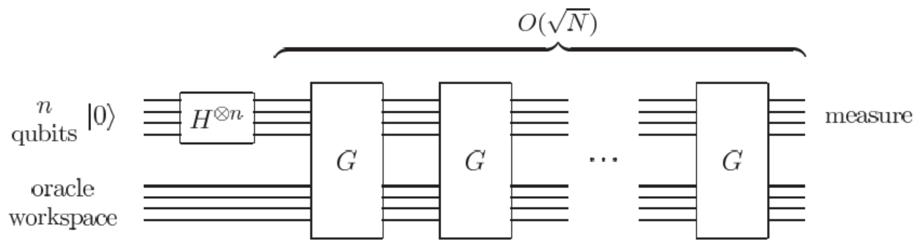
The state of the oracle qubit isn't changed and it turns out that it remains as $|-\rangle$ throughout the quantum search algorithm and hence can be omitted from further discussion. With this convention, the action of the oracle can be written as:

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$$

The oracle "marks" the solutions to the search problem by shifting the phase of the solution. For an $N$ item search problem with $M$ solutions, the search oracle need be applied $O(\sqrt{\frac{N}{M}})$ times in order to obtain a solution on a quantum computer.

### 1.2 The Procedure

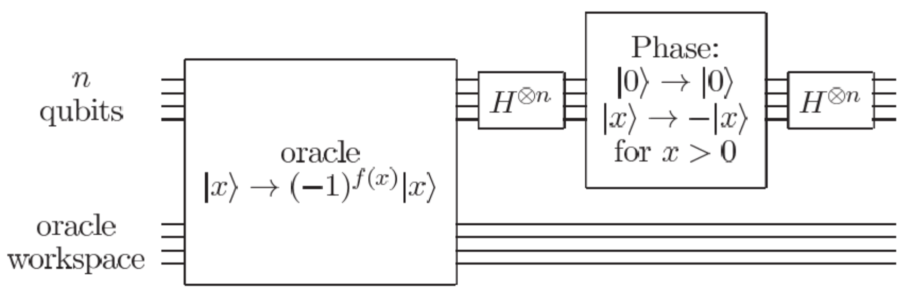
Schematically, the search algorithm operates as shown:




The algorithm proper makes use of a single $n$ qubit register. The goal of the algorithm is to find a solution to the search problem using the smallest possible number of applications of the oracle.
The Hadamard transform is used to put the computer in an *equally weighted superposition state*:

$$|\psi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle$$

The quantum search algorithm then consists of repeated application of a quantum subroutine, know as the *Grover iteration* or *Grover operator*, which we denote $G$. The quantum circuit of the Grover iteration is illustrated as follows:




The iteration can be broken into four steps:

- Apply the oracle $O$.
- Apply the Hadamard transform $H^{\otimes n}$.
- Perform a conditional phase shift on the computer, with every computational basis state except $|0\rangle$ receiving a phase shift of $-1$,

$$|x\rangle \to -(-1)^{\delta_{x0}}|x\rangle.$$

- Apply the Hadamard transform $H^{\otimes n}$.

The unitary operator corresponding to the phase shift in the Grover iteration is $2|0\rangle\langle 0| - I$.

The Grover iteration requires a single oracle call. The combined effect of the steps 2, 3, 4 of the Grover iteration is:

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I,$$

where $|\psi\rangle$ is the equally weighted superposition of states. Thus, the Grover iteration $G$ may be written $G = (2|\psi\rangle\langle\psi| - I)O$. The operation $(2|0\rangle\langle 0| - I)$ applied to a general state $\sum_k \alpha_k|k\rangle$ produces

$$\sum_k [-\alpha_k + 2\langle\alpha\rangle]|k\rangle,$$

where $\langle\alpha\rangle \equiv \sum_k \alpha_k/N$ is the mean value of the $\alpha_k$. For this reason, $(2|\psi\rangle\langle\psi| - I)$ is sometimes referred to as the *inversion about mean* operation.

## 1.3 Geometric Visualisation

Let us adopt the convention that $\sum_x'$ indicates a sum over all $x$ which are solutions to the search problem, and $\sum_x''$ indicates a sum over all $x$ which are not solutions to the search problem. Define normalised states

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$$

$$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$$

We also have that:

$$|\psi\rangle = \sqrt{\frac{N-M}{M}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$$

Thus, the initial state of the quantum computer is in a state spanned by $|\alpha\rangle$ and $|\beta\rangle$.

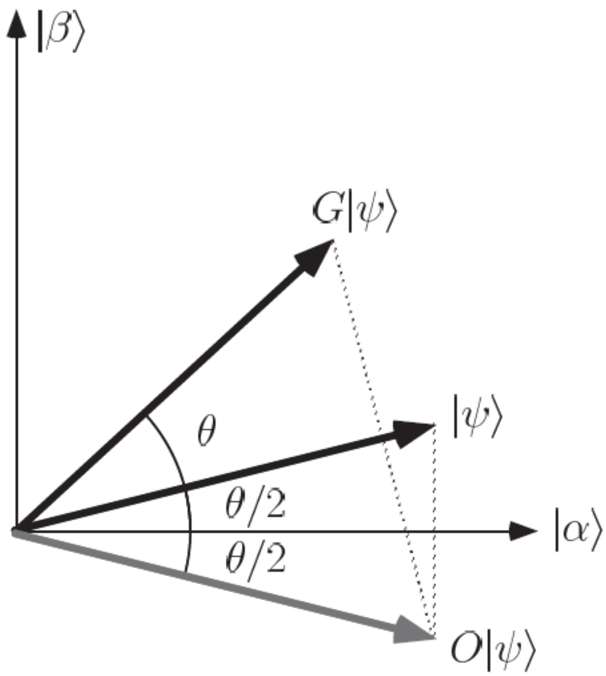
The effect of $G$ can be understood as follows: The oracle operation $O$ performs a reflection about the vector $|\alpha\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$, that is, $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$. Similarly, $2|\psi\rangle\langle\psi|$ - I also performs a reflection in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$ about the vector $|\psi\rangle$. And the product of two reflections is a rotation! In fact, in the $|\alpha\rangle$, $|\beta\rangle$ basis, the Grover iteration can be written as:

$$G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

where $\theta$ is a real number in the range 0 to $\pi/2$ (assuming for simplicity that $M \leq N/2$) chosen so that

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}$$

Thus, $G^k|\psi\rangle$ remains in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$ for all $k$. We can also find the rotation angle. Let $\cos(\theta/2) = \sqrt{(N-M)/N}$, so that $|\psi\rangle = \cos(\theta/2)|\alpha\rangle + \sin(\theta/2)|\beta\rangle$. The following figure shows the action of $G$:




Thus, the two reflections which comprise $G$ take $|\psi\rangle$ to

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$$

So the rotation angle is $\theta$. It follows that continued application of $G$ takes the state to

$$G^k|\psi\rangle = \cos(\frac{2k+1}{2}\theta)|\alpha\rangle + \sin(\frac{2k+1}{2}\theta)|\beta\rangle$$

Repeated application of the Grover iteration rotates the state vector close to $|\beta\rangle$. When this occurs, an observation in the computational basis produces with high probability one of the outcomes superposed in $|\beta\rangle$, that is, a solution to the search problem!

## 1.4 Performance

Let $CI(x)$ denote the integer closest to the real number $x$, where by convention we round halves down. Repeating the Grover iteration

$$R = CI(\frac{\cos^- 1\sqrt{M/N}}{\theta})$$

times rotates $|\psi\rangle$ to within an angle $\theta/2$ of $|\beta\rangle$. Observation of the state in the computational basis then yields a solution to the search problem with probability

of error at most $M/N$ for $M << N$.
The upper bound on the number of iterations is given by:

$$R \leq \lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \rceil$$

Thus, $R$ is, in fact, $O(\sqrt{N/M})$, a quadratic improvement over the $O(N/M)$ oracle calls required classically.

## 1.5 Quantum Search for M=1

**Inputs:**

- a black box oracle $O$ which performs the transformation $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$, where $f(x) = 0$ for all $0 \leq x < 2^n$ except $x_0$, for which $f(x_0) = 1$
- $n+1$ qubits in the state $|0\rangle$

**Outputs:** $x_0$
**Runtime:** $O(\sqrt{2^n})$ operations. Succeeds with probability $O(1)$
**Procedure:**

- initial state

$$|0\rangle^{\otimes n}|0\rangle$$

- apply $H^{\otimes n}$ to the first $n$ qubits, and $HX$ to the last qubit

$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle[\frac{|0\rangle - |1\rangle}{2}]$$

- apply the Grover iteration $R \approx \lceil \pi\sqrt{2^n}/4 \rceil$ times

$$\rightarrow [(2|\psi\rangle\langle\psi| - I)O]^R \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle[\frac{|0\rangle - |1\rangle}{\sqrt{2}}] \approx |x_0\rangle[\frac{|0\rangle - |1\rangle}{\sqrt{2}}]$$

- measure the first $n$ qubits

$$\rightarrow x_0$$