XI. Operators, Gates, Algorithms, Polarization: Query Models - Oracles

Tutorial: Quantum Computing, An Applied Approach, Jack Hidary

The earliest quantum algorithms are known as "**black box" or "query model" quantum algorithms**. Black boxes are theoretical constructs; they may or may not have an efficient implementation. For this reason, they are often called **oracles**. In these cases, there is an **underlying function which is unknown to us.** However, we are able to construct another function, called an oracle, which we can **query to determine the relationship of specific inputs with specific outputs.** More specifically, we can query the oracle function with specific inputs in the quantum register and reversibly write the output of the oracle function into that register. That is, we have access to an oracle O_f such that

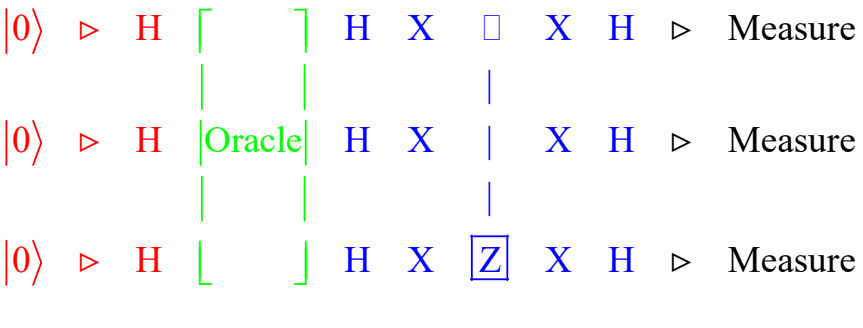
$$O_f|x\rangle = |x \oplus f(x)\rangle$$

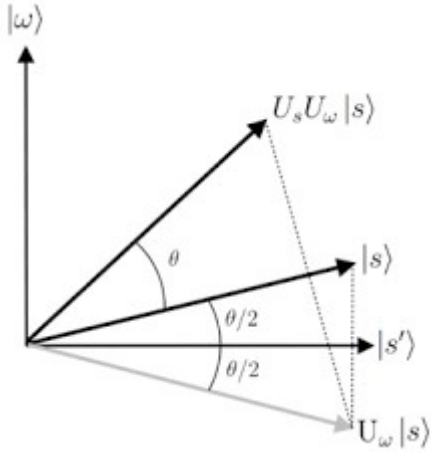
where $\oplus$ denotes addition modulo-2. .This can seem like "cheating" at first — how could we construct a circuit to perform O_f? And how could we know it's an efficient circuit? One reason to think about quantum algorithms in the query model is because it **provides a lower bound on the number of steps (gates)**. Each query is *at least* one step in the algorithm, so if it cannot be done efficiently with queries, it can certainly not be done efficiently with gates. Thus, the query model can be useful for ruling out fast quantum algorithms.

However, the query model can also be used to prove fast quantum algorithms relative to the oracle. We can give both a quantum computer and a classical computer access to the same oracle and see which performs better. It's possible to prove lower bounds or exact expressions for the number of queries in the classical and quantum cases, thereby making it possible to prove computational advantages relative to oracles. Examples of quantum algorithms with provable relativized speedups include Deutsch's algorithm and the Berstein-Vazirani algorithm.

These black box/oracle algorithms are one particular class of quantum algorithms. There are other algorithm classes such as quantum simulation.

Example: Grover's Quantum Search Algorithm (See Section XVII)





Grover's algorithm relies on an oracle. An oracle can be viewed as a black box that performs an operation on a quantum state that is not readily specified by universal quantum gates. In Grover's algorithm, an oracle is implemented such that it flips the sign of |x> iff x is a state we are looking for (the 'correct' quantum state). This can be expressed as

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

with $f(x) = 1$ if x is the correct state and $f(x) = 0$ otherwise. We assume that a function f is given as a black box, or oracle, means that it is not possible to obtain knowledge about f by any other means than by evaluating it on points of its domain.

Methodology for Grover's Search Algorithm

Mathematically, one can think of the algorithm as inverting a function
$f(x) : \{0, 1, 2 \cdots n\} \rightarrow \{0, 1\}$, where $f(x) = 0$, $x \neq a$; $f(x) = 1$, $x = a$, and the goal is to find a.

Exploring Unary Quantum Operators - Gates

We will examine the set of **one-qubit**, or unary, quantum operators. The first three operators we will examine are the **Pauli matrices, X Y Z**. These three matrices along with the identity matrix and all of their ±1 and ±i multiples constitute what is known as the Pauli group. **A unary operator is a gate** that takes **single input bit**, and a **binary** operator is one that takes **two input bits**. For example, it is a linear transformation of the **Hamiltonian Operator, *H***, that maps normalized (unit) vectors to other normalized vectors. Since H is 2-dimensional, a unary quantum operator can be represented by a 2 × 2 matrix.

X Operator: which is the NOT operator. It is denoted by the symbol ⊕. It is also denoted by the Pauli Matrix, σ_x,

Y Operator, also denoted σ_y, which **rotates the state vector about the y axis**.

Z Operator, also denoted σ_z, which **rotates the state vector about the z axis** (also called the **phase flip operator** since it flips it by π radians or 180 degrees) (also known as the bit flip operator and can be referred to as x)

R(φ) General phase shift operator. When we apply this operator we leave the **state |0> as is** and we take the state |1> and rotate it by the angle (or phase) denoted by φ, as specified in the matrix

$$R_1(\varphi) := \begin{pmatrix} 1 & 0 \\ 0 & e^{-\varphi} \end{pmatrix}$$

S Operator, additional phase shift operators that are special cases of the Rφ matrix where φ = π/2. The S operator thus rotates the state **about the z-axis by 90°**.

T Operator which rotates the state **about the z-axis by 45°**. If we give φ the value of π=4. Note: S = T^2

H, Hadamard Operator: --> qubit in **superposition state** where probability of measuring 0 = probability measuring 1.

Pauli Spin Matrices, X, Y, Z ($\sigma_x, \sigma_y, \sigma_z$) **Note:** Matrices X and Y on this page have Mathcad names of X_{dot} and Y_{dot}

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad R(\varphi) := \begin{pmatrix} 1 & 0 \\ 0 & e^{-\varphi} \end{pmatrix} \quad T := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

$$S := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad P(\varphi) := \begin{pmatrix} 1 & 0 \\ 0 & e^{\varphi} \end{pmatrix}$$

$$U(\theta, \phi, \lambda) := \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\cdot\lambda}\cdot\sin\left(\frac{\theta}{2}\right) \\ e^{i\cdot\phi}\cdot\sin\left(\frac{\theta}{2}\right) & e^{i\cdot(\phi+\lambda)}\cdot\cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$$L0 := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad H\cdot L0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} H$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e \\ f \end{pmatrix} \rightarrow \begin{pmatrix} a\cdot e + b\cdot f \\ c\cdot e + d\cdot f \end{pmatrix}$$

$$U\left(\frac{\pi}{2}, 0, \pi\right) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}}$$

$\alpha|0\rangle + \beta|1\rangle$ — X — $\beta|0\rangle + \alpha|1\rangle$

$\alpha|0\rangle + \beta|1\rangle$ — Z — $\alpha|0\rangle - \beta|1\rangle$

$\alpha|0\rangle + \beta|1\rangle$ — H — $\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$