COL7160 : Quantum Computing

Lecture 7: Oracle Model and Deutsch's Algorithm

Instructor: Rajendra Kumar **Scribe:** Abhinav Rajesh Shripad

1 Proving U_f is unitary

We begin by solving the last lecture's homework problem of proving the operation defined by

$$U_f : |z, b\rangle \to |z, b \oplus f(z)\rangle$$

Where $f : \{0,1\}^n \to \{0,1\}^m$.

Proof. To show that U_f is unitary, we must prove that

$$\langle \psi \mid \varphi \rangle = \langle U_f \psi \mid U_f \varphi \rangle \quad \text{for all } |\psi\rangle, |\varphi\rangle.$$

It suffices to verify this condition on an orthonormal basis.
Consider two computational basis states

$$|z, b\rangle \quad \text{and} \quad |z', b'\rangle,$$

where $z, z' \in \{0,1\}^n$ and $b, b' \in \{0,1\}^m$. Their inner product is

$$\langle z, b \mid z', b' \rangle = \delta_{z,z'}\, \delta_{b,b'}.$$

Applying U_f, we obtain

$$U_f|z, b\rangle = |z,\, b \oplus f(z)\rangle,$$
$$U_f|z', b'\rangle = |z',\, b' \oplus f(z')\rangle.$$

The inner product of the transformed states is

$$\langle z, b \oplus f(z) \mid z', b' \oplus f(z') \rangle = \delta_{z,z'}\, \delta_{b \oplus f(z),\, b' \oplus f(z')}.$$

If $z \neq z'$, the inner product is zero on both sides. If $z = z'$, then

$$b \oplus f(z) = b' \oplus f(z) \quad \iff \quad b = b',$$

since XOR with a fixed string is invertible.
Therefore,

$$\langle U_f(z, b) \mid U_f(z', b') \rangle = \delta_{z,z'}\, \delta_{b,b'} = \langle z, b \mid z', b' \rangle.$$

Hence U_f preserves inner products. □

Aliter. Alternatively, one may observe that U_f maps the computational basis to a permutation of the computational basis. Since permutations of an orthonormal basis preserve orthonormality, U_f maps 'an' orthonormal basis to 'an' orthonormal basis. Therefore, U_f is unitary. This argument is left as an exercise for the reader.

2 Parity Problem / Deutsch Problem

Consider the class of Boolean functions

$$A = \{\, f \mid f : \{0,1\} \to \{0,1\} \,\}.$$

We partition this class into two disjoint subsets:

$$\textbf{Constant} = \{\, f \in A \mid f(0) = f(1) \,\}, \tag{1}$$
$$\textbf{Balanced} = \{\, f \in A \mid f(0) \neq f(1) \,\}. \tag{2}$$

Problem Statement. Given oracle access to a function $f \in A$, determine whether f is **Constant** or **Balanced**.

Classical (Naive) Algorithm

Classically, one can evaluate $f(0)$ and $f(1)$ using two queries and decide with certainty whether f is constant or balanced. Thus, any classical deterministic algorithm requires two queries in the worst case.
The goal is to reduce the number of queries using a quantum algorithm.

Deutsch's Algorithm

Let the oracle be implemented as the unitary operator

$$U_f|a\rangle|b\rangle = |a\rangle|b \oplus f(a)\rangle.$$

Consider the second register initialized in the state

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Then,

$$\begin{aligned} U_f|a\rangle|-\rangle &= \frac{1}{\sqrt{2}}|a\rangle\big(|0 \oplus f(a)\rangle - |1 \oplus f(a)\rangle\big) && (3) \\ &= \frac{1}{\sqrt{2}}(-1)^{f(a)}|a\rangle(|0\rangle - |1\rangle) && (4) \\ &= (-1)^{f(a)}|a\rangle|-\rangle. && (5) \end{aligned}$$

This operation is known as a *phase query*, and is often denoted by

$$U_{f,\pm}|a\rangle = (-1)^{f(a)}|a\rangle.$$

Homework. If f is an $n \to m$ bit function, can phase be taken out similarly ?

Note that the above query alone does not suffice to solve the problem, since it encodes information about only a single value $f(a)$.
For comparison, consider

$$U_f|+\rangle|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\big),$$

which computes both $f(0)$ and $f(1)$, but contains no relative phase information.
Motivated by this observation, we instead consider

$$U_f|+\rangle|-\rangle = \frac{1}{\sqrt{2}}\big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\big)|-\rangle.$$

Ignoring the unchanged second qubit, the state of the first qubit is

$$\frac{1}{\sqrt{2}}\big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\big).$$

Applying a Hadamard measurement to the first qubit:

- If f is **Constant**, then $(-1)^{f(0)} = (-1)^{f(1)}$, and the state collapses to $|+\rangle$ with certainty.
- If f is **Balanced**, then $(-1)^{f(0)} \neq (-1)^{f(1)}$, and the state collapses to $|-\rangle$ with certainty.

Thus, the Deutsch problem can be solved with *a single quantum query*, demonstrating a strict quantum advantage over classical deterministic algorithms.

3 Oracle Model

In the oracle model, we are given access to an unknown function

$$f : \{0,1\}^n \to \{0,1\}^m,$$

not by an explicit description, but via a unitary operator (oracle)

$$U_f : |x, b\rangle \longmapsto |x,\, b \oplus f(x)\rangle,$$

where $x \in \{0,1\}^n$ and $b \in \{0,1\}^m$.
The oracle U_f allows us to query the value of $f(x)$ coherently on superpositions of inputs, which is the key resource exploited by quantum algorithms.

Oracle as a Bit-String Access Model

An equivalent and often convenient formulation is obtained when the function values are encoded in a classical bit string. Let

$$y = y_0 y_1 \cdots y_{N-1} \in \{0,1\}^N.$$

We define an oracle

$$O_y : |i, b\rangle \longmapsto |i,\, b \oplus y_i\rangle,$$

where $i \in \{0, 1, \ldots, N-1\}$ and $b \in \{0,1\}$.
We may interpret y as defining a Boolean function

$$f : \{0, 1, \ldots, N-1\} \to \{0,1\}, \qquad f(i) = y_i.$$

Identifying the index set $\{0, 1, \ldots, N-1\}$ with $\{0,1\}^n$, we have

$$N = 2^n \qquad \text{and hence} \qquad n = \log_2 N.$$

Under this identification, the oracle O_y is precisely the standard function oracle U_f for a Boolean function, written in index notation rather than binary string notation.

4 Generalization of Parity Problem

Consider the class of Boolean functions

$$A = \{\, f \mid f : \{0,1\}^n \to \{0,1\} \,\}.$$

We partition this class into two disjoint subsets:

$$\textbf{Constant} = \{\, f \in A \mid f(x) = f(y),\ \forall x, y \in \{0,1\}^n \,\}, \tag{6}$$

$$\textbf{Balanced} = \{\, f \in A \mid f(x) = 0 \text{ for exactly } 2^{n-1} \text{ inputs and} \tag{7}$$

$$f(x) = 1 \text{ for exactly } 2^{n-1} \text{ inputs} \,\}. \tag{8}$$

Promise Problem. Given oracle access to a function $f \in A$, determine whether f is **Constant** or **Balanced**, under the promise that f belongs to one of these two classes.

Classical Complexity

Classically, in the worst case, one must evaluate f on more than half of all possible inputs to distinguish a constant function from a balanced one with certainty. In particular, any deterministic classical algorithm requires at least

$$2^{n-1} + 1$$

queries in the worst case.

Quantum Algorithm

The oracle is given by the unitary operator

$$U_f : |x, b\rangle \longmapsto |x,\, b \oplus f(x)\rangle,$$

where $x \in \{0,1\}^n$ and $b \in \{0,1\}$.
Initialize the system in the state

$$|0\rangle^{\otimes n}|1\rangle.$$

Apply a Hadamard transform to all qubits to obtain

$$\left(H^{\otimes n} \otimes H\right) |0\rangle^{\otimes n}|1\rangle = \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes |-\rangle,$$

Next, apply the oracle U_f:

$$U_f \left(\frac{1}{2^{n/2}} \sum_x |x\rangle|-\rangle \right) = \frac{1}{2^{n/2}} \sum_x (-1)^{f(x)}|x\rangle|-\rangle.$$

The last qubit remains unchanged and may be ignored. Apply a Hadamard transform to the first n qubits:

$$H^{\otimes n} \left(\frac{1}{2^{n/2}} \sum_x (-1)^{f(x)}|x\rangle \right) = \sum_{z\in\{0,1\}^n} \alpha_z |z\rangle,$$

where

$$\alpha_z = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}(-1)^{x\cdot z}.$$

Measurement and Correctness

In particular, the amplitude of the state $|0\rangle^{\otimes n}$ is

$$\alpha_0 = \frac{1}{2^n} \sum_x (-1)^{f(x)}.$$

- If f is **Constant**, then either $f(x) = 0$ for all x or $f(x) = 1$ for all x, and hence

  $$\alpha_0 = \pm 1.$$

  Thus, the measurement outcome $|0\rangle^{\otimes n}$ occurs with probability 1.

- If f is **Balanced**, then exactly half the terms contribute $+1$ and half contribute -1, yielding

  $$\alpha_0 = 0.$$

  Thus, the measurement outcome $|0\rangle^{\otimes n}$ occurs with probability 0.

Therefore, measuring the first register:

- Outcome $|0\rangle^{\otimes n} \Rightarrow f$ is **Constant**,
- Any other outcome $\Rightarrow f$ is **Balanced**.