COL7160 : Quantum Computing

Lecture 7: Oracle Model and Deutsch's Algorithm

Instructor: Rajendra Kumar **Scribe:** Mayank Giri

1 Oracle Model and Quantum Parallelism

Let $f : \{0,1\} \to \{0,1\}$ be a Boolean function. In the quantum setting, we do not access f directly; instead, we are given access to an oracle unitary U_f defined as

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

where $x, b \in \{0,1\}$ and $\oplus$ denotes addition modulo 2.

Remark 1. The oracle U_f is reversible even if f itself is not. This reversibility is essential since all quantum operations must be unitary.

Example 2. Applying U_f twice yields the identity:

$$U_f^2 |x, b\rangle = |x, b \oplus f(x) \oplus f(x)\rangle = |x, b\rangle\,.$$

Hence, $U_f^\dagger = U_f$ and U_f is unitary.

2 Quantum Parallelism

Quantum parallelism refers to the ability of a quantum computer to evaluate a function on a superposition of inputs in a single query .

Consider the initial two-qubit state $|0\rangle|0\rangle$. Applying a Hadamard gate to the first qubit gives

$$(H \otimes I)|0\rangle|0\rangle = |+\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|0\rangle).$$

Applying the oracle U_f yields

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

This state encodes information about both $f(0)$ and $f(1)$ simultaneously.

3 Deutsch's Problem (Parity Problem)

Let $f : \{0,1\} \to \{0,1\}$. There are four possible such functions:

$f(0)$	$f(1)$	Type
0	0	Constant
1	1	Constant
0	1	Balanced
1	0	Balanced

Definition 3. The function f is called *constant* if $f(0) = f(1)$, and *balanced* if $f(0) \neq f(1)$.

The goal of Deutsch's problem is to determine whether f is constant or balanced using as few oracle queries as possible.

4 Phase Kickback

Prepare the second qubit in the state

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

Applying the oracle gives

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

Remark 4. The phase $(-1)^{f(a)}$ is a global phase on the second qubit and cannot be directly measured. However, relative phases between components of a superposition can be detected.

5 Deutsch Algorithm Computation

Start with the state $|+\rangle |-\rangle$. Applying U_f:

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

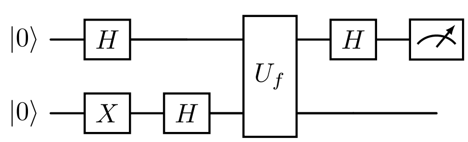
Factoring out a global phase $(-1)^{f(0)}$ gives

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

If f is constant, then $f(0) \oplus f(1) = 0$, and the first qubit is $|+\rangle$. If f is balanced, then $f(0) \oplus f(1) = 1$, and the first qubit is $|-\rangle$.
Measuring the first qubit in the $\{|+\rangle , |-\rangle\}$ basis distinguishes the two cases with certainty using a single oracle query.

5.1 Circuit Representation of Deutsch's Algorithm

The Deutsch algorithm can be represented using the following quantum circuit.



The second qubit is prepared in the state $|-\rangle$, enabling phase kickback. Only the first qubit is measured.

- If the measurement outcome is $|0\rangle$ (equivalently $|+\rangle$ before the final Hadamard), then f is *constant.*
- If the measurement outcome is $|1\rangle$ (equivalently $|-\rangle$), then f is *balanced.*

Thus, Deutsch's algorithm determines whether f is constant or balanced using a single oracle query.

6 Oracle Model for General Functions

Let $f : \{0,1\}^n \to \{0,1\}$. The oracle is defined as

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

where $x \in \{0,1\}^n$.

Preparing the state

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |-\rangle$$

and applying U_f yields

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle |-\rangle .$$

Thus, the function values $f(x)$ are encoded as relative phases on the computational basis states. This phase information can later be extracted using interference.

6.1 Oracle Model: Indexing Interpretation

Let $N = 2^n$ and consider a function

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

Each element of $\{0,1\}^n$ can be identified with an integer $i \in \{0, 1, \ldots, N-1\}$ via its binary representation. Under this identification, the function f can be equivalently viewed as a binary string

$$Y = (y_0, y_1, \ldots, y_{N-1}), \quad \text{where } y_i := f(i).$$

In this interpretation, the oracle U_f acts as

$$U_f |i, b\rangle = |i,\, b \oplus y_i\rangle ,$$

where $|i\rangle$ is represented using $\log N = n$ qubits.

Remark 5. This viewpoint treats the oracle as a black-box database storing the string Y, where a query at index i returns the bit y_i via a reversible transformation.

7 Balanced and Constant Functions (General Case)

Definition 6. A function $f : \{0,1\}^n \to \{0,1\}$ is:

- *constant* if $f(x) = f(y)$ for all x, y,
- *balanced* if exactly half the inputs map to 0 and half to 1.

If f is constant, the state becomes

$$\frac{1}{\sqrt{2^n}} \sum_{x} |x\rangle ,$$

up to a global phase. We will solve this problem in the next lecture.

8 Hadamard Transform

Proposition 7. *For* $x \in \{0,1\}^n$,

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle ,$$

where $x \cdot y = x_1 y_1 + \cdots + x_n y_n \pmod 2$.

Proof. The result follows from applying the single-qubit identity

$$H |x_i\rangle = \frac{1}{\sqrt{2}} \big(|0\rangle + (-1)^{x_i} |1\rangle \big)$$

to each qubit and expanding the tensor product. □

Remark 8. Applying $H^{\otimes n}$ to the uniform superposition returns $|0^n\rangle$, which is crucial for distinguishing constant functions in Deutsch–Jozsa–type algorithms.

9 Promise Problems

In many quantum algorithms, the function f is guaranteed (or *promised*) to belong to a specific class, such as being either balanced or constant.

Remark 9. Without the promise, it is impossible to classify f with certainty using a single oracle query.

References

[dW23] Ronald de Wolf. Quantum computing: Lecture notes, 2023.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, UK, 10th anniversary edition edition, 2010.