COL7160 : Quantum Computing

Lecture 8: Deutsch–Jozsa Algorithm and Bernstein–Vazirani Problem

Instructor: Rajendra Kumar **Scribe:** Sahil Kumar

1 Oracle Model

We work in the *oracle model*, where an unknown Boolean function

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

can be accessed only through queries. In the quantum setting, the oracle must be reversible and is implemented as a unitary operator U_f defined by

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

where $x \in \{0, 1\}^n$ and $y \in \{0, 1\}$. This allows querying f coherently on superpositions of inputs.

2 Quantum Parallelism

If the input register is prepared in a superposition, the oracle acts on all inputs simultaneously. Consider the uniform superposition

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

Applying the oracle yields

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

Although this state encodes values of $f(x)$ for all x, measurement reveals only one outcome. Hence quantum parallelism alone does not give an exponential speedup.

3 Phase Kickback

To extract global information, we encode $f(x)$ as a phase. Prepare the second register in the state

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

Then

$$U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle .$$

Thus the value of $f(x)$ is transferred as a phase on the state $|x\rangle$.

4 Binary Inner Product

For bit strings $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, the binary inner product is defined as

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \pmod 2.$$

5 Hadamard Transform

In this section we prove the explicit form of the Hadamard transform acting on an n-qubit computational basis state.

Theorem 1. *For any $x \in \{0,1\}^n$, the Hadamard transform satisfies*

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

Proof. We first recall that for a single qubit,

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^y |y\rangle .$$

Hence, for $x_i \in \{0,1\}$,

$$H|x_i\rangle = \frac{1}{\sqrt{2}} \sum_{y_i \in \{0,1\}} (-1)^{x_i y_i} |y_i\rangle .$$

For an n-bit string $x = (x_1, \ldots, x_n)$, we apply H independently to each qubit:

$$H^{\otimes n} |x\rangle = \bigotimes_{i=1}^{n} H|x_i\rangle = \frac{1}{\sqrt{2^n}} \sum_{y_1, \ldots, y_n \in \{0,1\}} (-1)^{\sum_{i=1}^{n} x_i y_i} |y_1 \ldots y_n\rangle .$$

Recognizing that $\sum_i x_i y_i \equiv x \cdot y \pmod 2$ for our problem completes the proof. $\square$

6 Deutsch–Jozsa Problem

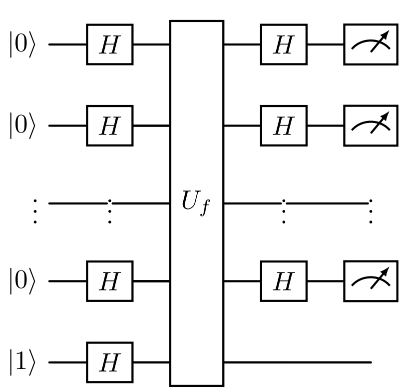
Input: A function $f : \{0,1\}^n \to \{0,1\}$.
Promise: f is either constant or balanced.
Goal: Decide which of the two cases holds.

6.1 Classical Algorithms

A deterministic classical algorithm must evaluate f on more than half of the input domain to be certain that f is constant, requiring $2^{n-1} + 1$ queries in the worst case.
A probabilistic classical algorithm may sample inputs uniformly at random. After k independent queries, the algorithm incorrectly declares a balanced function to be constant with probability at most 2^{-k+1}. This happens because the probability that after the first query all remaining $k-1$ come from the same subset would happen with at most $2^{-(k-1)}$ probability. Thus, achieving error probability at most ε requires $k = O(\log(1/\varepsilon))$ queries. However, this algorithm can never achieve zero error with fewer than $2^{n-1} + 1$ queries.

6.2 Quantum Algorithm

The quantum Deutsch–Jozsa algorithm uses a single oracle query. Starting from the state $|0\rangle^{\otimes n} |1\rangle$, Hadamard gates are applied to all qubits, followed by the oracle U_f and a final Hadamard transform on the first register.



The resulting state of first n-qubits before final measurement is

$$\frac{1}{2^n} \sum_{y \in \{0,1\}^n} \left(\sum_{x \in \{0,1\}^n} (-1)^{f(x)+x\cdot y} \right) |y\rangle .$$

If f is constant, the outcome is always $y = 0^n$ because we can see that its amplitude is 1. If f is balanced, the amplitude of $|0^n\rangle$ is zero. Thus, the two cases are distinguished with certainty.

6.3 Quantum Advantage

The Deutsch–Jozsa algorithm achieves an exponential separation in query complexity when compared with deterministic classical algorithms. The quantum algorithm requires only a single query, whereas any deterministic classical algorithm requires $2^{n-1} + 1$ queries. In comparison with probabilistic classical algorithms, the quantum algorithm has no error.

7 Finding a Hidden String: The Bernstein–Vazirani Problem

Input: A function $f : \{0,1\}^n \to \{0,1\}$ of the form

$$f(x) = s \cdot x \pmod 2,$$

for an unknown string $s \in \{0,1\}^n$.
Goal: Determine the hidden string s.

7.1 Classical Algorithms

In the classical setting, each oracle query reveals only one bit of information about s. A natural deterministic strategy is to query the oracle on the standard basis vectors $e_1, \ldots, e_n$, from which one can recover each bit $s_i = f(e_i)$. Thus, any deterministic classical algorithm requires n oracle queries in the worst case. Randomized algorithms do not asymptotically improve this bound informally the idea is that the information we are interested in is of n bits, Each classical query reveals only 1 bit of information so to be able to say correctly with more than $1/2$ probability for the complete n bit information we would need n queries.

7.2 Quantum Algorithm

The Bernstein–Vazirani quantum algorithm follows the same high-level structure as the Deutsch–Jozsa algorithm, but exploits the specific form of the function $f(x) = s \cdot x$.
We begin with the $(n+1)$-qubit state

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

Applying Hadamard gates to all qubits yields

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

where $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.
Next, we apply the oracle U_f. Using phase kickback, the state becomes

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

We now apply $H^{\otimes n}$ to the first register. We obtain

$$\frac{1}{2^n} \sum_{y \in \{0,1\}^n} \left(\sum_{x \in \{0,1\}^n} (-1)^{s\cdot x + x\cdot y} \right) |y\rangle |-\rangle .$$

Rewriting the exponent as $x \cdot (s + y)$, the amplitude of $|y\rangle$ is

$$\sum_{x \in \{0,1\}^n} (-1)^{x \cdot (s+y)}.$$

This sum evaluates to 2^n if $y = s$ and to 0 otherwise. Consequently, the final state simplifies to

$$|s\rangle \, |-\rangle \, .$$

Measurement under standard computational basis of first n-qubits outputs the string s.

7.3 Quantum Advantage

The algorithm recovers the entire n-bit string s using a single quantum oracle query, compared to n classical queries. This provides a linear-to-constant separation in query complexity and further demonstrates the power of quantum interference.

References