Rapid solutions of problems by quantum computation

David Deutsch and Richard Jozsa (1997)

School of Air Transport, Transportation & Logistics **2018310015 Dongsin Kim**

Deutsch-Jozsa Problem

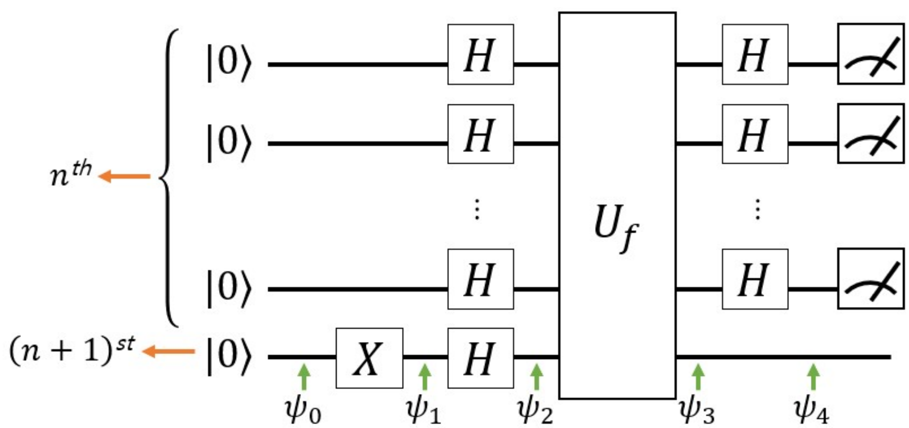
Given n-bit function $f:\{0,1\}^n \to \{0,1\}$ which is guaranteed to either be *balanced or constant*, determine whether which is the case. *Balanced* means $f(x) = 0$ for half of the $x \in \{0,1\}^n$ and $f(x) = 1$ for the remaining input domain, and *constant* means f is the same for all $x \in \{0,1\}^n$.

Classicaly, we can randomly choose $k(\leq n)$ inputs $x_1, \ldots, x_k \in \{0,1\}^n$, evaluate $f(x_i)$ for $i = 1, \ldots, k$, and answer "constant" if $f(x_1) = \cdots = f(x_k)$ and "balanced" otherwise. If we want to get a correct answer every time with this approaches, $(2^{n-1} + 1)$-queries are needed in the worst case. However, we claim that a single query is sufficient to determine the solution with certainty.

Please note that *this problem* is the n-bit generalization of the *Deutsch's problem*.

Deutsch-Jozsa Algorithm

Deutsch-Jozsa algorithm can be implemented with the following $(n + 1)$-qubits quantum circuit (represented by $(n + 1)$-lines) initialized with, respectively, $|0\rangle$:



To analyze the state of the quantum circuit, we first need to understand what $H^{\otimes n}|a\rangle$ equals for arbitrary $a \in \{0,1\}$. (Here, $H^{\otimes n} = H \otimes \cdots \otimes H$ (n times)). For this, we begin with a clean and formal way for the action of H one a single qubit. For $a_1 \in \{0,1\}$, we have

$$H|a_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{a_1}|1\rangle = \frac{1}{\sqrt{2}}\sum_{b_1 \in \{0,1\}}(-1)^{a_1 b_1}|b_1\rangle.$$

If we instead had two qubits, starting in state $|a\rangle$ for $a = a_1 a_2 \in \{0,1\}^2$, and applied Hadamard transforms to both, we would obtain

$$(H \otimes H)|a\rangle = H|a_1\rangle \otimes H|a_2\rangle$$
$$= \left(\frac{1}{\sqrt{2}}\sum_{b_1 \in \{0,1\}}(-1)^{a_1 b_1}|b_1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}\sum_{b_2 \in \{0,1\}}(-1)^{a_2 b_2}|b_2\rangle\right) = \frac{1}{(\sqrt{2})^2}\sum_{b \in \{0,1\}^2}(-1)^{a_1 b_1 + a_2 b_2}|b\rangle.$$

We can generalize this to n-qubit states. Specifically, if we write the state $|a\rangle = |a_1 \cdots a_n\rangle$ as $|a_1\rangle \otimes \cdots \otimes |a_n\rangle$, we have

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots \otimes H|a_n\rangle$$
$$= \left(\frac{1}{\sqrt{2}}\sum_{b_1 \in \{0,1\}}(-1)^{a_1 b_1}|b_1\rangle\right) \otimes \cdots \otimes \left(\frac{1}{\sqrt{2}}\sum_{b_n \in \{0,1\}}(-1)^{a_n b_n}|b_n\rangle\right) = \frac{1}{(\sqrt{2})^n}\sum_{b \in \{0,1\}^n}(-1)^{a_1 b_1 + \cdots + a_n b_n}|b\rangle.$$

We also define $a \cdot b = \sum_{i=1}^{n} a_i b_i \pmod 2$, (here, the $\bmod 2$ arises since the base is (-1), so all we care about is if the exponent $a \cdot b$ is even or odd) so that we may write

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

First, the algorithm starts with $|\psi_0\rangle = |00 \cdots 0\rangle = |0\rangle \otimes \cdots \otimes |0\rangle$ $\big((n+1)$ times$\big) = |0\rangle^{\otimes n} \otimes |0\rangle$

Analogously to Deutsch's algorithm, It is clear that

$$|\psi_1\rangle = \left(I^{\otimes n} \otimes X\right)|\psi_0\rangle = I|00 \cdots 0\rangle \otimes X|0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle,$$

$$|\psi_2\rangle = \left(H^{\otimes n} \otimes H\right)|\psi_1\rangle = H^{\otimes n}|00 \cdots 0\rangle \otimes H|1\rangle$$

$$= \frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}(-1)^{0 \times x_1 + \cdots + 0 \times x_n}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

$$\because\ H^{\otimes n}|a\rangle = \frac{1}{(\sqrt{2})^n}\sum_{b \in \{0,1\}^n}(-1)^{a \cdot b}|b\rangle \text{ and } H|1\rangle = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Second, remembering that $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$:

$$|\psi_3\rangle = U_f|\psi_2\rangle = \frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}|x\rangle \otimes \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) = \frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}(-1)^{f(x)}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

$$\because\ |\psi_3\rangle = \begin{cases} \frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}|x\rangle \otimes \left(\frac{|0 \oplus 0\rangle - |1 \oplus 0\rangle}{\sqrt{2}}\right) = \frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right), & \text{if } f(x) = 0 \\ \frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}|x\rangle \otimes \left(\frac{|0 \oplus 1\rangle - |1 \oplus 1\rangle}{\sqrt{2}}\right) = \frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}|x\rangle \otimes \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right), & \text{if } f(x) = 1 \end{cases}$$

Lastly, we must apply the last set of Hadamard gates,

$$|\psi_4\rangle = \left(H^{\otimes n} \otimes I\right)|\psi_3\rangle = H^{\otimes n}\left(\frac{1}{(\sqrt{2})^n}\sum_{x \in \{0,1\}^n}(-1)^{f(x)}|x\rangle\right) \otimes I\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right),$$

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

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

Case 1: balanced f. Consider the amplitude on $|z\rangle = |00\cdots 0\rangle$:

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x_1\times 0+\cdots+x_n\times 0} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)} = \frac{1}{2^n}\times 0 = 0.$$

Since f is balanced, all the terms in this sum of $(-1)^{f(x)}$ cancel, i.e. the sum equals 0. Thus, we conclude that the amplitude on $|z\rangle = |00\cdots 0\rangle$ is 0, and so *we will never see outcome $|00\cdots 0\rangle$ in the final measurement*.

Case 2: Constant f. Consider the amplitude on $|z\rangle = |00\cdots 0\rangle$ and factor out $(-1)^{f(x)}$ in $|\psi_4\rangle$:

$$|\psi_4\rangle = (-1)^{f(x)}\left(\sum_{z\in\{0,1\}^n}\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle\right)\right)\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right),$$

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x_1\times 0+\cdots+x_n\times 0} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^0 = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}1 = \frac{1}{2^n}\times 2^n = 1.$$

In other words, the state $|0\rangle^{\otimes n}\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$ has amplitude 1. Since the quantum state is a unit vector, we can conclude that we must have $|\psi_4\rangle = (-1)^{f(x)}|00\cdots 0\rangle\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$, i.e. all the weight is on this one term. Thus, if f is constant, then *measuring the first n-qubits yields outcome $|00\cdots 0\rangle$ with certainty.*

Conclusion

By measureing the first n-qubits, we can conclude that f is balanced (any n-bit measurement outcome except $|00\cdots 0\rangle$) or constant (always $|00\cdots 0\rangle$ outcome) with just a single-query.