**MAT 4930: Quantum Algorithms and Complexity** **Spring 2021**

# Lecture 8: The Deutsch-Jozsa Algorithm

*Lecturer: Jean-François Biasse* *TA: Robert Hart*



The Deutsch-Jozsa algorithm is our first example of an algorithm that achieves an exponential speed-up over classical ones. In other words, this means that there is no constant $k > 0$ such that

$$\text{Cost}_{\text{classical}}(S) \in O\left(\text{Cost}_{\text{quantum}}(S)^k\right),$$

where $S$ is the input size of the problem, and $\text{Cost}_{\text{classical}}(S)$ is the cost of solving the problem with a classical computer while $O\left(\text{Cost}_{\text{quantum}}(S)^k\right)$ is the cost solving it with a quantum one. The problem to be solve (which has little practical use), consists in deciding whether an input function $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced (returns 0 on half the inputs, and 1 on the other half). Here, the cost will is measured as the number of evaluations of a circuit that implements $f$. The quantum Deutsch-Jozsa solution to the problem as the astonishing property to require only one evaluation of the quantum circuit implementing $f$.

## 8.1 Uniform superposition with Hadamard gates

While the Deutsch-Jozsa does not directly solve a search problem per se, it uses one of the main ingredients of Grover's algorithm that will be introduced later in this course: namely the creation of the uniform superposition of elements.

**Definition 8.1 (Uniform superposition)** *Let $n > 1$ and $S \subseteq \{0, \dots, 2^n - 1\}$. The $n$-qubit state that is the superposition of all elements of $S$ is*

$$|\psi\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle,$$

*where $|S|$ denote the cardinality of $S$.*

**Proposition 8.2** *Let $n > 1$ and $S \subseteq \{0, \dots, 2^n - 1\}$. The measurement of the state that is the superposition of all elements of $S$ yields any given $x \in S$ with probability $1/|S|$.*

**Proof:** We have that the state is decomposed as

$$|\psi\rangle = \sum_{x \in S} a_x |x\rangle = \sum_{x \in S} \frac{1}{\sqrt{|S|}} |x\rangle.$$

Hence we measure $x$ with probability $|a_x|^2 = 1/|S|$. ∎

It is generally admitted that we can prepare the input state to a quantum algorithm in one of the basis states, typically $|0\rangle^{\otimes n}$. However, it is not necessarily straightforward to create a uniform superposition over

a given set $S$. Here, we focus on the case where $S = \{0, \ldots, n-1\}$. This means that we'd like to create the state

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x<2^n} |x\rangle .$$

Such a state has the property that we measure any canonical basis vector label with uniform probability. Now, remember how the Hadamard gate acts on $|0\rangle$:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{where } H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Hence, the Hadamard gate produces the uniform superposition of all 1-qubit states. Let's see what happens on 2 qubits.

$$\begin{aligned} H^{\otimes 2}|0\rangle^{\otimes 2} &= H \otimes H(|0\rangle \otimes |0\rangle) \\ &= (H|0\rangle) \otimes (H|0\rangle) \\ &= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{2}\left(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right) \\ &= \frac{1}{2}\left(\sum_{x<4} |x\rangle\right). \end{aligned}$$

This means that we have realized the uniform superposition over 2 qubits with the Hadamard gate tensored with itsef. Could this fact be generalized to $n$ qubits? The answer is yes.

**Proposition 8.3** *Let $n \geq 1$, the following always hold:*

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x<2^n} |x\rangle .$$

**Proof:** We could prove this by directly expanding the product (and being comfortable with large products), but this is perhaps even easier to see by induction. We already showed that the property was true for $n = 1, 2$. Assume that that for some $n > 1$, we have $H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x<2^n} |x\rangle$. Then we have

$$\begin{aligned} H^{\otimes(n+1)}|0\rangle^{\otimes(n+1)} &= (H^{\otimes n} \otimes H)|0\rangle^{\otimes n)\otimes|0\rangle} \\ &= (H^{\otimes n}|0\rangle^{\otimes n}) \otimes (H|0\rangle) \\ &= \left(\frac{1}{2^{n/2}} \sum_{x<2^n} |x\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \text{ by induction} \\ &= \frac{1}{2^{(n+1)/2}} \sum_{x<2^n} |x\rangle \otimes |0\rangle + \frac{1}{2^{(n+1)/2}} \sum_{x<2^n} |x\rangle \otimes |1\rangle \\ &= \frac{1}{2^{(n+1)/2}} \sum_{x<2^n} \underbrace{|x\rangle}_{\in \mathbb{C}^{2^{n+1}}} + \frac{1}{2^{(n+1)/2}} \sum_{2^n \leq x < 2^{n+1}} |x\rangle \\ &= \frac{1}{2^{(n+1)/2}} \sum_{x<2^{n+1}} |x\rangle \end{aligned}$$

■

**Proposition 8.4** *Let $n \geq 1$, the following always hold:*

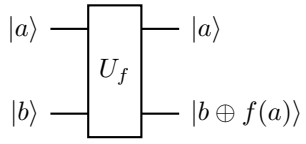
$$H^{\otimes n} |x\rangle = \frac{1}{2^{n/2}} \sum_{y<2^n} (-1)^{x \cdot y} |y\rangle ,$$

*where $x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \ldots x_{n-1} y_{n-1}$ is the dot product of their binary digits $x = \sum_i x_i 2^i$, $y = \sum_i y_i 2^i$ in $\mathbb{F}_2^n$*

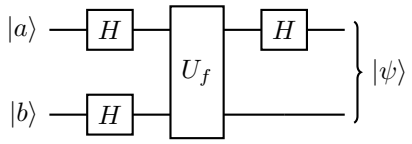
**Proof:** As a homework assignement. ■

## 8.2 The Deutsch algorithm

Prior work of Deutsch involved a special case of the Deutsch-Jozsa algorithm, namely when $n = 1$. This can be rephrased as checking whether a function $f : \{0,1\} \to \{0,1\}$ satisfies $f(0) = f(1)$ or $f(0) \neq f(1)$. This can be done by computing $f$ twice (on input 0 and on input 1) and checking whether the resulting values are equal. Deutsch's algorithm shows how a quantum computer can perform this task with only one call to an implementation of $f$. We show how this work because it is a nice introduction to the more general Deutsch-Jozsa algorithm. We assume that $f$ is given under the form of a quantum circuit that does




Remember that we have seen that this is always possible, modulo the use of ancilla qubits which are not represented here. We use the circuit $U_f$ as follows:




**Proposition 8.5** *With the above notation, when $a = 0$, $b = 1$, the measurement of the first qubit of $|\psi\rangle$ yields*

- *0 if $f(0) = f(1)$.*
- *1 if $f(0) \neq f(1)$.*

**Proof:** We have that $|\psi\rangle = (H \otimes I)(U_f)H^{\otimes 2}(|0\rangle \otimes |1\rangle)$. Let us evaluate these products from right to left. We have

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

Then the action of $U_f$ on this state yields

$$\begin{aligned} U_f H^{\otimes 2}(|0\rangle \otimes |1\rangle) &= \frac{1}{2}(|0\rangle \otimes (|f(0)\oplus 0\rangle - |f(0)\oplus 1\rangle) + |1\rangle \otimes (|f(1)\oplus 0\rangle - |f(1)\oplus 1\rangle) \\ &= \frac{1}{2}\left((-1)^{f(0)}|0\rangle \otimes (|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle \otimes (|0\rangle - |1\rangle)\right) \\ &= (-1)^{f(0)}\frac{1}{2}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}\right) \otimes (|0\rangle - |1\rangle) \\ &\sim \frac{1}{2}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}\right) \otimes (|0\rangle - |1\rangle) \quad \text{(we can ignore a global phase)} \end{aligned}$$

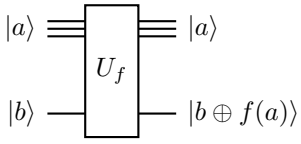
We are now dealing with a product state. Both qubits are independant, and we simply look at the action of $H$ on the first quit that is in the state which is given by

$$\begin{aligned} \frac{H}{\sqrt{2}}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}\right) &= \frac{1}{2}\left(|0\rangle + |1\rangle + (-1)^{f(0)\oplus f(1)}|0\rangle - (-1)^{f(0)\oplus f(1)}\right) \\ &= \frac{\left(1 + (-1)^{f(0)\oplus f(1)}\right)}{2}|0\rangle + \frac{\left(1 - (-1)^{f(0)\oplus f(1)}\right)}{2}|1\rangle . \end{aligned}$$

When $f(0)\oplus f(1) = 0$, this state equals $|0\rangle$ (and thus the final measurement is 0), and when $f(0)\oplus f(1) = 1$, this state equals $|1\rangle$. ■

## 8.3 The Deutsch-Jozsa algorithm

We assume that $f : \{0,1\}^n \to \{0,1\}$ is given under the form of a quantum circuit that does




This is the same as for the Deutsch algorithm, except that we have replace the first qubit by $n$ qubits. Then we use this circuit given in Figure 8.1.

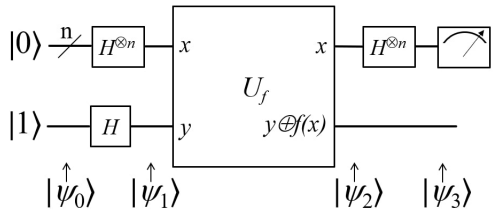



Figure 8.1: Deutsch-Jozsa algorithm

Let us analyze the algorithm step by step. First, $|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$. Then after applying $H^{\otimes(n+1)}$, we obtain

$$|\psi_1\rangle = (H^{\otimes n}|0\rangle^{\otimes n}) \otimes (H|1\rangle) = \frac{1}{\sqrt{2^{n+1}}}\sum_{x<2^n}|x\rangle \otimes (|0\rangle - |1\rangle).$$

Now we apply $U_f$. This yields the state

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x<2^n} |x\rangle \otimes \left( \underbrace{|0 \oplus f(x)\rangle}_{|f(x)\rangle} - |1 \oplus f(x)\rangle \right).$$

We have the following two possibilities:

- If $f(x) = 0$, then $|f(x)\rangle - |1 \oplus f(x)\rangle = |0\rangle - |1\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$.
- If $f(x) = 1$, then $|f(x)\rangle - |1 \oplus f(x)\rangle = |1\rangle - |0\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$.

Either way, we must have:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x<2^n} (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle).$$

This is a product state between $\frac{1}{\sqrt{2^n}} \sum_{x<2^n} (-1)^{f(x)} |x\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We focus on the first $n$ bits and ignore the last one. The first $n$ qubits of $|\psi_3\rangle$ are given by

$$\begin{aligned} \frac{1}{\sqrt{2^n}} \sum_{x<2^n} (-1)^{f(x)} H^{\otimes n} |x\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x<2^n} (-1)^{f(x)} \left( \frac{1}{\sqrt{2^n}} \sum_{y<2^n} (-1)^{x \cdot y} |y\rangle \right) \\ &= \frac{1}{2^n} \sum_{y<2^n} \left( \sum_{x<2^n} (-1)^{f(x)} (-1)^{x \cdot y} |x\rangle \right). \end{aligned}$$

We measure $y = 0$ with probability $\left| \frac{1}{2^n} \sum_{x<2^n} (-1)^{f(x)} \right|^2$. This probability is 1 if $f$ is constant, and 0 if $f$ is balanced, exactly like in the case $n = 1$ given by Deutsch algorithm.