PHY 4105: Quantum Information Theory
Lecture 24

Anil Shaji
School of Physics, IISER Thiruvananthapuram
(Dated: November 7, 2013)

Deutsch-Jozsa Algorithm

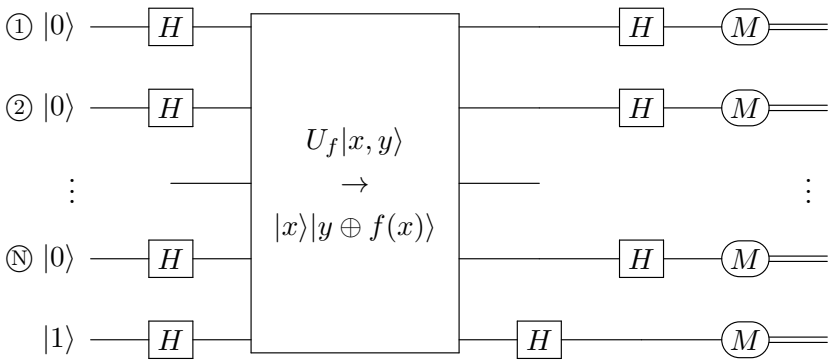
The Deutsch-Jozsa algorithm is one of the simplest cases in which one can demonstrate that a quantum computational device can perform a task exponentially faster than the best known classical algorithm. The problem that it solves is a rather cooked up one and is as follows. One is given a Boolean function on N-bits,

$$f : \{0,1\}^N \longrightarrow \{0,1\},$$

and in addition given a promise that the function is either a constant or it is balanced. Balanced means that on half of the 2^N, N-bit strings the function takes as input, it outputs the value 0 and on the remaining it evaluates to 1. The challenge is to find which one of the two types the given function is.

Classically, there is no better algorithm known to solve this problem than to start picking bit strings, either in order or at random and evaluating the function on it. One can stop when the function, if at all, gives out a value different than the one it gave in the previous trials and conclude that the function must be of the balanced variety. But if the function keeps on evaluating to a constant one has to conduct at least $2^N/2 = 2^{N-1}$ trials to make sure that it is a constant function. So the resources, which in this case is the time taken to do the algorithm, scales exponentially with the problem "size", N and hence we deem it a hard problem classically to do. In "hard" problems, the resources needed to run the best known algorithm scales exponentially with the input size N.

Now consider the following quantum algorithm represented by the following circuit for $N+1$ qubits. The first N qubits form a "register" that holds the input and the last one is the register for the output.



The unitary transformation U_f in the circuit is a reversible "implementation" of the given function. We are assuming that the function is efficiently implementable with a non-exponentially growing

number of elementary gates both on the classical as well as on the quantum circuits. If classically itself the function is not implementable then there is no question of even the comparison with the best classical algorithm because the computational device on which the algorithm can run itself cannot be built. So we exclude those cases. What U_f does is to take in the input bit string x and evaluate the function f on it and write the answer $f(x)$ on to the second register as $u \oplus f(x)$.

Now let us look at each stage of the circuit and see what this algorithm is doing. The initial state is

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle.$$

After the first set of HADAMARD gates, we have the state

$$|\psi_1\rangle = H^{\otimes N}|0\rangle^{\otimes N} \otimes H|1\rangle = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

Here x denotes all the integers from 0 to $2^N - 1$ represented in binary since as a result of the N HADAMARDs we get on the first register the (not normalized) state

$$(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle) = |00\cdots0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle = \sum_x |x\rangle,$$

where x is represented in binary.

As a result of the unitary U_f we get the state

$$|\psi_2\rangle = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle \otimes \frac{1}{\sqrt{2}}\Big(|f(x)\rangle - \Big|\overline{f(x)}\Big\rangle\Big) = |\psi_2\rangle = \frac{1}{\sqrt{2^N}} \sum_x (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

The last step may be viewed as a *phase kickback*, where the relative phases, associated with the second register, between terms of the superposition in $|\psi_2\rangle$ is "re-assigned" to the first register. The function values are now written in the phase of the first register states.

After the HADAMARD on the second register, we reset the second register to the initial state and we get

$$|\psi_3\rangle = \frac{1}{\sqrt{2^N}} \sum_x (-1)^{f(x)}|x\rangle \otimes |1\rangle.$$

The effect of the last set of HADAMARD gates on the first register can be computed using

$$H^{\otimes N}|x\rangle = \frac{1}{\sqrt{2^N}} \sum_y (-1)^{x\cdot y}|y\rangle,$$

where $x \cdot y$ corresponds to the bitwise dot product (mod 2) of the strings x and y. The bitwise dot product to two strings is defined as

$$(a_1, a_2, \ldots, a_N) \cdot (b_1, b_2, \cdots, b_N) = a_1b_1 \oplus a_2b_2 \oplus \cdots \oplus a_Nb_N.$$

We will not be proving that the action of the HADAMARD gates is as above, but verifying (forgetting normalization) it in the simple case of $N = 2$ is easy,

$$\begin{aligned}
|00\rangle &\rightarrow |00\rangle + |01\rangle + |10\rangle + |11\rangle \\
|01\rangle &\rightarrow |00\rangle - |01\rangle + |10\rangle - |11\rangle \\
|10\rangle &\rightarrow |00\rangle + |01\rangle - |10\rangle - |11\rangle \\
|11\rangle &\rightarrow |00\rangle - |01\rangle - |10\rangle + |11\rangle
\end{aligned}$$

So after the second set of HADAMARD gates we get the state

$$|\psi_4\rangle = \left(\frac{1}{2^N}\sum_{x,y}(-1)^{f(x)+x\cdot y}|y\rangle\right)\otimes|1\rangle.$$

If $f(x)$ is a constant then the state of the first register is

$$|\chi\rangle = \pm\frac{1}{2^N}\sum_{y}\Big(\sum_{x}(-1)^{x\cdot y}\Big)|y\rangle.$$

We can show that

$$\sum_{x}(-1)^{x\cdot y} = 2^N\delta(y),$$

so that when $f(x)$ is a constant we have

$$|\chi\rangle = \pm|0\rangle^{\otimes N}.$$

To verify the above, for the two qubit case

$$\begin{aligned}
y = 00 \quad &\Rightarrow \quad (-1)^{00\cdot 00} + (-1)^{01\cdot 00} + (-1)^{10\cdot 00} + (-1)^{11\cdot 00} = 1+1+1+1 = 4\\
y = 01 \quad &\Rightarrow \quad (-1)^{00\cdot 01} + (-1)^{01\cdot 01} + (-1)^{10\cdot 01} + (-1)^{11\cdot 01} = 1-1+1-1 = 0\\
y = 10 \quad &\Rightarrow \quad (-1)^{00\cdot 10} + (-1)^{01\cdot 10} + (-1)^{10\cdot 10} + (-1)^{11\cdot 10} = 1+1-1-1 = 0\\
y = 11 \quad &\Rightarrow \quad (-1)^{00\cdot 11} + (-1)^{01\cdot 11} + (-1)^{10\cdot 11} + (-1)^{11\cdot 11} = 1-1-1+1 = 0
\end{aligned}$$

If $f(x)$ is balanced then we get

$$\langle 0|\chi\rangle = \sum_{x}(-1)^{f(x)} = 0.$$

So if the measurement on the first register yields a 0 on all of the individual qubits, then in on shot one knows that the function is a constant. Any other result means that the function is balanced since that result cannot appear for the case where the function is constant.