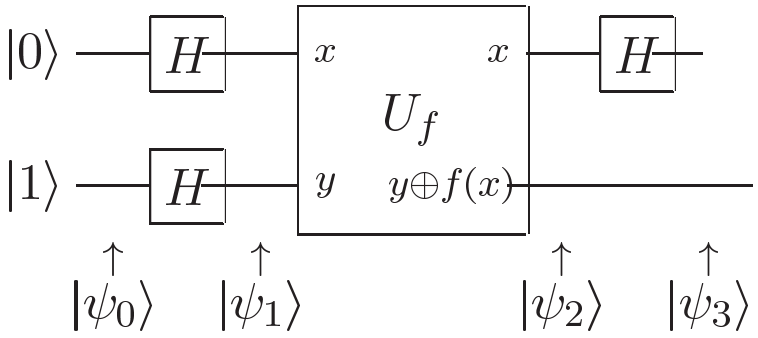

Figure III.22: Quantum circuit for Deutsch algorithm. [fig. from Nielsen & Chuang (2010)]

D Quantum algorithms

D.1 Deutsch-Jozsa

D.1.a Deutsch algorithm

In this section you will encounter your first example of a quantum algorithm that can compute faster than a classical algorithm for the same problem. This is a simplified version of Deutsch's original algorithm, which shows how it is possible to extract global information about a function by using quantum parallelism and interference (Fig. III.22).[8]

Suppose we have a function $f : \mathbf{2} \to \mathbf{2}$, as in Sec. C.5. The goal is to determine whether $f(0) = f(1)$ with a *single* function evaluation. This is not a very interesting problem (since there are only four such functions), but it is a warmup for the Deutsch-Jozsa algorithm. Simple as it is, it could be expensive to decide on a classical computer. For example, suppose $f(0) =$ the billionth bit of π and $f(1) =$ the billionth bit of e. Then the problem is to decide if the billionth bits of π and e are the same. It is mathematically simple, but computationally complex.

To see how we might solve this problem, suppose we have a quantum gate array U_f for f; that is, $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$. In particular, $U_f|x\rangle|0\rangle =$

[8] This is the 1998 improvement by Cleve et al. to Deutsch's 1985 algorithm (Nielsen & Chuang, 2010, p. 59).

$|x\rangle|f(x)\rangle$ and $U_f|x\rangle|1\rangle = |x\rangle|\neg f(x)\rangle$. Usually we set $y = 0$ to get the result $|f(x)\rangle$, but here you will see an application in which we want $y = 1$.

Now consider the result of applying U_f to $|x\rangle$ in the data register and to the superposition $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ in the target register.

$$U_f|x\rangle|-\rangle = \frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|\neg f(x)\rangle = \frac{1}{\sqrt{2}}|x\rangle[|f(x)\rangle - |\neg f(x)\rangle].$$

Now the rightmost square bracket is $|0\rangle - |1\rangle$ if $f(x) = 0$ or $|1\rangle - |0\rangle$ if $f(x) = 1$. Therefore, we can write

$$U_f|x\rangle|-\rangle = \frac{1}{\sqrt{2}}|x\rangle(-)^{f(x)}(|0\rangle - |1\rangle) = (-)^{f(x)}|x\rangle|-\rangle. \tag{III.21}$$

[Here, $(-)^x$ is an abbreviation for $(-1)^x$ when we want to emphasize that the sign is all that matters.] Since $U_f|x\rangle|-\rangle = (-)^{f(x)}|x\rangle|-\rangle$, the result of applying it to an equal superposition of $x = 0$ and $x = 1$ is:

$$\frac{1}{\sqrt{2}}\sum_{x\in\mathbf{2}} U_f|x\rangle|-\rangle = \frac{1}{\sqrt{2}}\sum_{x\in\mathbf{2}}(-)^{f(x)}|x\rangle|-\rangle.$$

If f is a constant function, then $f(0) = f(1)$, and the summation is $\pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle = \pm|+\rangle|-\rangle$ because both components have the same sign.. On the other hand, if $f(0) \neq f(1)$, then the summation is $\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|-\rangle = \pm|-\rangle|-\rangle$ because the components have opposite signs. That is, a constant function gives the $|0\rangle$ and $|1\rangle$ components of the data qubit the same phase, and otherwise gives them the opposite phase. Therefore, we can determine whether the function is constant or not by measuring the first qubit in the sign basis; we get $|+\rangle$ if $f(0) = f(1)$ and $|-\rangle$ otherwise. With this background, we can state Deutsch's algorithm.

algorithm Deutsch:

Initial state: Begin with the qubits $|\psi_0\rangle \stackrel{\text{def}}{=} |01\rangle$.

Superposition: Transform it to a pair of superpositions

$$|\psi_1\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+-\rangle. \tag{III.22}$$

by a pair of Hadamard gates. Recall that $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$.

Function application: Next apply U_f to $|\psi_1\rangle = |+-\rangle$. As we've seen, $U_f|x\rangle|0\rangle = |x\rangle|0 \oplus f(x)\rangle = |x\rangle|f(x)\rangle$, and $U_f|x\rangle|1\rangle = |x\rangle|1 \oplus f(x)\rangle = |x\rangle|\neg f(x)\rangle$. Therefore, expand Eq. III.22 and apply U_f:

$$\begin{aligned}
|\psi_2\rangle &\stackrel{\text{def}}{=} U_f|\psi_1\rangle \\
&= U_f\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \\
&= \frac{1}{2}[U_f|00\rangle - U_f|01\rangle + U_f|10\rangle - U_f|11\rangle] \\
&= \frac{1}{2}[|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle]
\end{aligned}$$

There are two cases: $f(0) = f(1)$ and $f(0) \neq f(1)$.

Equal (constant function): If $f(0) = f(1)$, then

$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}[|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(0)\rangle - |1, \neg f(0)\rangle] \\
&= \frac{1}{2}[|0\rangle(|f(0)\rangle - |\neg f(0)\rangle) + |1\rangle(|f(0)\rangle - |\neg f(0)\rangle)] \\
&= \frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) \\
&= \pm\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&= \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle \\
&= |+-\rangle.
\end{aligned}$$

The last line applies because global phase (including $\pm$) doesn't matter.

Unequal (balanced function): If $f(0) \neq f(1)$, then

$$|\psi_2\rangle = \frac{1}{2}[|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, \neg f(0)\rangle - |1, f(0)\rangle]$$

$$
\begin{aligned}
&= \frac{1}{2}[|0\rangle(|f(0)\rangle - |\neg f(0)\rangle) + |1\rangle(|\neg f(0)\rangle - |f(0)\rangle)] \\
&= \frac{1}{2}[|0\rangle(|f(0)\rangle - |\neg f(0)\rangle) - |1\rangle(|f(0)\rangle - |\neg f(0)\rangle)] \\
&= \frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) \\
&= \pm\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \\
&= \pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|-\rangle \\
&= |--\rangle
\end{aligned}
$$

Clearly we can discriminate between the two cases by measuring the first qubit in the sign basis. In particular, note that in the unequal case, the $|1\rangle$ component has the opposite phase from the $|0\rangle$ component.

Measurement: Therefore we can determine whether $f(0) = f(1)$ or not by measuring the first bit of $|\psi_2\rangle$ in the sign basis, which we can do with the Hadamard gate (recall $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$):

$$
\begin{aligned}
|\psi_3\rangle &\stackrel{\text{def}}{=} (H \otimes I)|\psi_2\rangle \\
&= \begin{cases} \pm|0\rangle|-\rangle, & \text{if } f(0) = f(1) \\ \pm|1\rangle|-\rangle, & \text{if } f(0) \neq f(1) \end{cases} \\
&= \pm|f(0) \oplus f(1)\rangle|-\rangle.
\end{aligned}
$$

□

Notice that the information we need is in the *data* register, not the target register. This technique is called *phase kick-back* (i.e., kicked back into the phase of the data register).

In conclusion, we can determine whether or not $f(0) = f(1)$ with a *single evaluation* of f, which is quite remarkable. In effect, we are evaluating f on a superposition of $|0\rangle$ and $|1\rangle$ and determining how the results interfere with each other. As a result we get a definite (not probabilistic) determination of a global property with a single evaluation.

This is a clear example where a quantum computer can do something faster than a classical computer. However, note that U_f has to uncompute

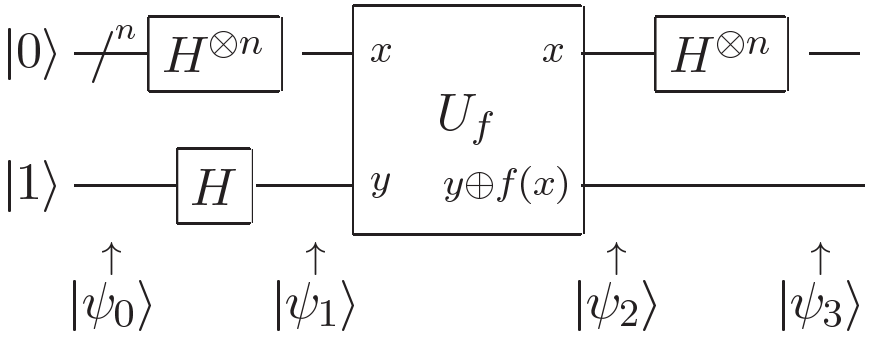

Figure III.23: Quantum circuit for Deutsch-Jozsa algorithm. [fig. from NC]

f, which takes as much time as computing it, but we will see other cases (Deutsch-Jozsa) where the speedup is much more than $2\times$.

D.1.b Deutsch-Jozsa algorithm

The Deutsch-Jozsa algorithm is a generalization of the Deutsch algorithm to n bits, which they published it in 1992; here we present the improved version of Nielsen & Chuang (2010, p. 59).

This is the problem: Suppose we are given an unknown function $f : \mathbf{2}^n \to \mathbf{2}$ in the form of a unitary transform $U_f \in \mathcal{L}(\mathcal{H}^{n+1}, \mathcal{H})$ (Fig. III.23). We are told only that f is either constant or *balanced*, which means that it is 0 on half its domain and 1 on the other half. Our task is to determine into which class the given f falls.

Consider first the classical situation. We can try different input bit strings $\mathbf{x}$. We might (if we're lucky) discover after the second query of f that it is not constant. But we might require as many as $2^n/2 + 1$ queries to answer the question. So we're facing $\mathcal{O}(2^{n-1})$ function evaluations.

algorithm Deutsch-Jozsa:

Initial state: As in the Deutsch algorithm, prepare the initial state $|\psi_0\rangle \stackrel{\text{def}}{=} |0\rangle^{\otimes n}|1\rangle$.

Superposition: Use the Walsh-Hadamard transformation to create a superposition of all possible inputs:

$$|\psi_1\rangle \stackrel{\text{def}}{=} (H^{\otimes n} \otimes H)|\psi_0\rangle = \sum_{\mathbf{x}\in\mathbf{2}^n} \frac{1}{\sqrt{2^n}}|\mathbf{x}, -\rangle.$$

Claim: Similarly to the single qubit case (Eq. III.21), we can see that $U_f|\mathbf{x}, -\rangle = (-)^{f(\mathbf{x})}|\mathbf{x}\rangle|-\rangle$, where $(-)^n$ is an abbreviation for $(-1)^n$. From the definition of $|-\rangle$ and U_f, $U_f|\mathbf{x}, -\rangle = |\mathbf{x}\rangle\frac{1}{\sqrt{2}}(|f(\mathbf{x})\rangle - |\neg f(\mathbf{x})\rangle)$. Since $f(\mathbf{x}) \in \mathbf{2}$, $\frac{1}{\sqrt{2}}(|f(\mathbf{x})\rangle - |\neg f(\mathbf{x})\rangle) = |-\rangle$ if $f(\mathbf{x}) = 0$, and it $= -|-\rangle$ if $f(\mathbf{x}) = 1$. This establishes the claim.

Function application: Therefore, you can see that:

$$|\psi_2\rangle \stackrel{\text{def}}{=} U_f|\psi_1\rangle = \sum_{\mathbf{x}\in\mathbf{2}^n} \frac{1}{\sqrt{2^n}}(-)^{f(\mathbf{x})}|\mathbf{x}, -\rangle. \tag{III.23}$$

In the case of a constant function, all the components of the data state have the same phase, otherwise they do not.

To see how we can make use of this information, let's consider the state in more detail. For a *single* bit you can show (Exer. III.42):

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{z\in\mathbf{2}}(-)^{xz}|z\rangle = \sum_{z\in\mathbf{2}}\frac{1}{\sqrt{2}}(-)^{xz}|z\rangle.$$

(This is just another way of writing $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.) Therefore, the general formula for the Walsh transform of n bits is:

$$\begin{aligned} H^{\otimes n}|x_1, x_2, \ldots, x_n\rangle &= \frac{1}{\sqrt{2^n}}\sum_{z_1,\ldots,z_n\in\mathbf{2}}(-)^{x_1z_1+\cdots+x_nz_n}|z_1, z_2, \ldots, z_n\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{\mathbf{z}\in\mathbf{2}^n}(-)^{\mathbf{x}\cdot\mathbf{z}}|\mathbf{z}\rangle, \end{aligned} \tag{III.24}$$

where $\mathbf{x}\cdot\mathbf{z}$ is the bitwise inner product. (It doesn't matter if you do addition or $\oplus$ since only the parity of the result is significant.) *Remember this formula!* Combining this and the result in Eq. III.23,

$$|\psi_3\rangle \stackrel{\text{def}}{=} (H^{\otimes n} \otimes I)|\psi_2\rangle = \sum_{\mathbf{z}\in\mathbf{2}^n}\sum_{\mathbf{x}\in\mathbf{2}^n}\frac{1}{2^n}(-)^{\mathbf{x}\cdot\mathbf{z}+f(\mathbf{x})}|\mathbf{z}\rangle|-\rangle.$$

Measurement: Consider the first n qubits and the amplitude of one particular basis state, $\mathbf{z} = |\mathbf{0}\rangle = |0\rangle^{\otimes n}$, which we separate from the rest of the summation:

$$|\psi_3\rangle = \sum_{\mathbf{x}\in\mathbf{2}^n} \frac{1}{2^n}(-)^{f(\mathbf{x})}|\mathbf{0}\rangle|-\rangle + \sum_{\mathbf{z}\in\mathbf{2}^n-\{\mathbf{0}\}} \sum_{\mathbf{x}\in\mathbf{2}^n} \frac{1}{2^n}(-)^{\mathbf{x}\cdot\mathbf{z}+f(\mathbf{x})}|\mathbf{z}\rangle|-\rangle$$

Hence, the amplitude of $|0\rangle^{\otimes n}$, the all-$|0\rangle$ qubit string, is $\sum_{\mathbf{x}\in\mathbf{2}^n} \frac{1}{2^n}(-)^{f(\mathbf{x})}$. Recall how in the basic Deutsch algorithm we got a sum of signs (either all the same or not) for all the function evaluations. The result is similar here, but we have 2^n values rather than just two. We now have two cases:

Constant function: If the function is constant, then all the exponents of -1 will be the same (either all 0 or all 1), and so the amplitude will be ± 1. Therefore all the other amplitudes are 0 and any measurement must yield 0 for all the qubits (since only $|0\rangle^{\otimes n}$ has nonzero amplitude).

Balanced function: If the function is not constant then (*ex hypothesi*) it is balanced, but more specifically, if it is balanced, then there must be an equal number of $+1$ and -1 contributions to the amplitude of $|0\rangle^{\otimes n}$, so its amplitude is 0. Therefore, when we measure the state, at least one qubit must be nonzero (since the all-0s state has amplitude 0).
□

The *good news* about the Deutsch-Jozsa algorithm is that with one quantum function evaluation we have got a result that would require between 2 and $\mathcal{O}(2^{n-1})$ classical function evaluations (exponential speedup!). The *bad news* is that the algorithm has no known applications! Even if it were useful, however, the problem could be solved probabilistically on a classical computer with only a few evaluations of f: for an error probability of ϵ, it takes $\mathcal{O}(\log \epsilon^{-1})$ function evaluations. However, it illustrates principles of quantum computing that can be used in more useful algorithms.