## Deutsch algorithm

*Deutsch's algorithm* is the simplest example of quantum computers being capable of computations that go beyond the capabilities of classical computers. Suppose that the function $f : \{0,1\} \mapsto \{0,1\}$ is given by some oracle (that is, a "black box", which returns the value $f(x)$ at the input $x$ without revealing anything about how to calculate this value). The task is to decide whether $f$ is constant or not. In the classical case, it is obvious that we have to perform two queries, i.e. to find out both values of the function $f$. On the other hand, notice that the question is about a single bit of information: "constant yes or no"? However, there is no way to ask the oracle just this question. This is exactly the point at which the quantum computer has the upper hand.

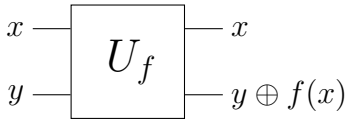
The situation becomes somewhat complicated by the question of what a quantum oracle should look like. It follows from the postulates of quantum mechanics that it should be some unitary transformation. The problem, however, is that the function $f$ need not be injective, i.e. not regular, let alone unitary. The standard solution to this problem is to introduce an auxiliary cubit that represents the input value. The function $f$ will therefore correspond to the two-bit operator $U_f$, which is defined for $x, y \in \{0,1\}$ by the relation

$$|x\rangle \otimes |y\rangle \overset{U_f}{\longmapsto} |x\rangle \otimes |y \oplus f(x)\rangle,$$

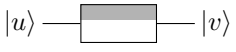
where the symbol $\oplus$ denotes a binary sum (sum in $\mathbb{Z}_2$). Note that the matrix $U_f$ permutes the four basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, and is therefore obviously unitary (moreover, $U_f \circ U_f = \mathrm{Id}$).

The construction of the quantum oracle above is the basis of the extended capabilities of the quantum algorithm. It is therefore easy to get the impression that the quantum algorithm is more successful due to the more relaxed definition of the oracle. This impression is only partially justified. The quantum oracle has no advantage over the classical one in terms of the **basis states** $|0\rangle$ and $|1\rangle$, on which the function is defined. Extended capabilities are not so much given by the construction of the oracle as by the typically quantum fact that the oracle can also process **superpositions**. This involves some kind of "illegal" information about the inner workings of the oracle, namely that it behaves **linearly** with respect to state superpositions.

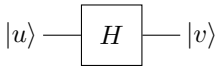
Following the example of algorithmic schemes, we can display $U_f$ as a logical gate:




This notation should not be confused with the scheme we used for the beamsplitter in the description of the Mach-Zehnder interferometer. It was a single-cubic operator, which should be drawn as a gate as




where $|v\rangle = H|u\rangle$, or better yet

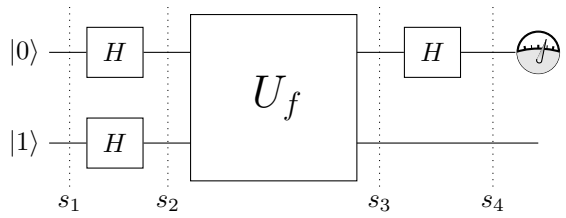


to make it clear that we don't care whether operator

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

is realized by a beamsplitter, or otherwise. As we have already pointed out, this $H$ operator plays an important role in quantum computers and is called the *Hadamard gate*.

The quantum circuit implementing the Deutsch algorithm is relatively simple. It consists, in addition to the oracle $U_f$, of three Hadamard gates:




In the figure, the vertical lines indicate the four phases of the calculation. At the beginning, the two-bit register is in the state

$$s_1 = |01\rangle.$$

In the second phase we get

$$s_2 = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

The result of the oracle, of course, depends on the $f$ function. The simplest case is $f(0) = f(1) = 0$, where $U_f$ is the identity. Then we have

$$s_3 = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

If $f(0) = f(1) = 1$, the action $U_f$ is given by the relation

$$|00\rangle \mapsto |01\rangle \qquad |01\rangle \mapsto |00\rangle \qquad |10\rangle \mapsto |11\rangle \qquad |11\rangle \mapsto |10\rangle.$$

So

$$s_3 = \frac{1}{2} U_f(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}(|01\rangle - |00\rangle + |11\rangle - |10\rangle) =$$
$$= -\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

We can proceed similarly in other cases and get the overall expression

$$s_3 = \begin{cases} \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{if } f(0) = f(1), \\ \\ \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{if } f(0) \neq f(1). \end{cases}$$

Finally

$$s_4 = \begin{cases} \pm|0\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{if } f(0) = f(1), \\ \\ \pm|1\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{if } f(0) \neq f(1). \end{cases}$$

Now is the right time to **measure the first cubit**. The eigenvalue corresponding to $|0\rangle$ will mean that $f$ is constant, the eigenvalue of $|1\rangle$ the opposite answer.

Deutch's algorithm, in its simplicity, shows the basic idea of all quantum algorithms: the superposition of states allows, in a sense, to compute many values simultaneously. Note that the Hadamard transform brings about the evaluation the balanced superposition of both values. This, on the other hand, does not mean that we have direct access to any functional value. For example, if we measure the first cubite in the phase $s_3$, we get a worthless random result, independent of the function $f$.

## Deutsch-Jozsa algorithm

A more general form of the algorithm is called the *Deutsch-Jozsa algorithm*. There is a Boolean function $f : \{0,1\}^n \to \{0,1\}$, which is either constant or balanced (i.e. exactly half of the arguments take the value 1 and the other half the value 0). The task is again to find out which of the options applies.

The circuit looks the same as in Deutsch's algorithm, only at the input there is a register $|0\rangle^{\otimes n}$ instead of $|0\rangle$ and also the corresponding Hadamard transformation of this register is the tensor product: $H^{\otimes n}$ . We get a somewhat more complicated description of the individual phases. At the beginning we have the state

$$s_1 = |0^n 1\rangle.$$

and in the second phase

$$s_2 = \left(\frac{1}{\sqrt{2}}\right)^n \bigotimes_{i=1}^{n}(|0\rangle + |1\rangle)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)^n \left(\sum_{x\in\{0,1\}^n} |x\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

The case analysis from the Deutsch algorithm can be written succinctly. Note that

$$U_f\left(|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |x\rangle\frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

So after the application of the oracle we get

$$s_3 = \left(\frac{1}{\sqrt{2}}\right)^n \left(\sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Recall that

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

where $x \cdot z = x_1x_2 \ldots x_n \cdot z_1z_2 \ldots z_n$ denotes the dot product of the vectors of the binary development digits, i.e.

$$\sum_{i=1}^{n} x_i z_i.$$

So for the final phase of the algorithm we get

$$s_4 = \frac{1}{2^n}\left(\sum_{x\in\{0,1\}^n}\sum_{z\in\{0,1\}^n} (-1)^{x\cdot z+f(x)}|z\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

What are the possible results of the measurement of the first register? Note that each basis state appears $2^n$ times in the sum, with different signs. However, the signs for the state $|0^n\rangle$ depend only on $f(x)$. Thus, if $f$ is constant, the amplitude of the state $|0^n\rangle$ is equal to 1 or $-1$. Conversely, if $f$ is balanced, the number of

positive terms is the same as the number of negative ones and the amplitude of the probability is 0. Therefore, the measurement result will correspond to the state $|0^n\rangle$ if and only if $f$ is constant.

Note that a more general rule applies, which roughly states that the probability of measuring zero increases as the function $f$ gets closer to a constant.

The Deutsch-Jozsa algorithm allows a correct answer after a single oracle query. This means an exponential speed up compared to the deterministic classical algorithm, which needs $2^{n-1}+1$ queries for a (certain) answer. However, there is a classical probabilistic algorithm with probability of error $\frac{1}{2^k}$, for which $k$ queries are enough: after $k$ random queries we answer "constant" just when all the results are the same. The possibility of error only exists for balanced functions and is obviously less than the required error bound. From this point of view, especially when we consider the susceptibility of quantum phenomena to errors, the acceleration of the quantum computer is only constant.