Deutsch's Algorithm

Andreas Klappenecker

Deutsch's Problem

Suppose that we are given a Boolean function f: {0,1} -> {0,1}. So it has a single bit input.

The problem is to decide whether f is a constant function or not.

[Apparently, we need to look at both values f(0) and f(1) to answer this question. If we have a black box implementation of f]

The classical solution to this problem requires two calls to the black box, since the function might be constant or not. In the quantum version, you are given an implementation of f as a quantum circuit on two quantum bits,

$$\mathbf{B}: |x_1\rangle \otimes |x_0\rangle \mapsto |x_1\rangle \otimes |x_0 \oplus f(x_1)\rangle, \tag{3.4}$$

with $x_1, x_0 \in \mathbf{F}_2 = \{0, 1\}$. The quantum version can be solved with a single call to the black box. The problem and its solution were suggested by Deutsch in 1985; it is historically one of the first quantum algorithms.

Phase Kickback

Let B denote the unitary map on $\mathbf{C}^4$ determined by (3.4). We will derive the solution in some small steps. It is clear that we have to take advantage of the superposition principle to evaluate the boolean function simultaneously for both possible input arguments. The solution to Deutsch's problem uses an additional trick, which allows us to encode the value of $f(x)$ into a phase factor. Suppose that the least significant bit is in the state $1/\sqrt{2}(|0\rangle - |1\rangle)$, then

$$B\left(|x_1\rangle \otimes (\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle)\right) = |x_1\rangle \otimes (\frac{1}{\sqrt{2}}|f(x_1)\rangle - \frac{1}{\sqrt{2}}|1 \oplus f(x_1)\rangle) =: v_{x_1}$$

for all $x_1 \in \{0, 1\}$. If the value of $f(x_1)$ is zero, then the input state remains invariant; otherwise, B affects a change of sign. Explicitly,

$$v_{x_1} = (-1)^{f(x_1)}|x_1\rangle \otimes (\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle).$$

We can now use the superposition principle. If we choose $1/\sqrt{2}(|0\rangle + |1\rangle)$ for the most significant qubit, then we obtain the result $1/\sqrt{2}(v_0 + v_1)$ since the black box B is linear. To put this in a different way, we get

$$B\left(\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)\right) = \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle).$$

The goal was to discriminate between functions, which satisfy $f(0) \oplus f(1) = 0$, and functions satisfying $f(0) \oplus f(1) = 1$. The previous state is equivalent to

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

If we apply the Hadamard gate on the most significant qubit, then we get

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

We measure the most significant qubit now. If the function in the black box satisfies $f(0) \oplus f(1) = 0$, then we will observe 0 with certainty. If f satisfies $f(0) \oplus f(1) = 1$, then we will observe 1. Note that the algorithm is completely deterministic. We can summarize the algorithm that we have developed as follows: