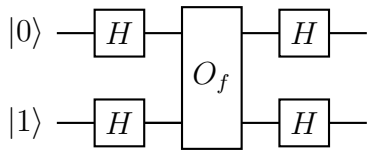
Raul Garcia-Patron
Jakub Adamski

Tutorial 3

IQC 2024-25
October 21, 2024

Problem 1: Deutsch Algorithm

Consider the following circuit:



a. The oracle O_f is a two-qubit gate that maps $|x\rangle\,|y\rangle \to |x\rangle\,|y \oplus x\rangle$. By comparing to what we have seen in the lectures, what is the classical function implemented by the oracle O_f, i.e. $f(x)$? Do you think $f(x)$ will be balanced or constant?

Solution: In the lectures, we have seen that the Quantum Oracle in Deutsch's Algorithm maps $|x\rangle\,|y\rangle \to |x\rangle\,|y \oplus f(x)\rangle$. Comparing this to the oracle O_f defined above, we can see that $f(x) = x$. Since this means that $f(0) = 0 \neq f(1) = 1$, we can conclude that $f(x)$ is not constant since $f(0) \neq f(1)$. Moreover, we can see that there is a single input that gives 0, i.e. $|f^{-1}(0)| = 1$, and a single input that gives 1, i.e. $|f^{-1}(1)| = 1$. This means that the function is **balanced**, as the number of inputs giving 0 is the same as the number of inputs giving 1.

---

b. What is the circuit of O_f?

Solution: In order to determine the two-qubit gate O_f, let us find the output for all possible combinations of $x, y \in \{0, 1\}$:

For $x = 0, y = 0$: $|0\rangle\,|0\rangle \to |0\rangle\,|0 \oplus 0\rangle = |0\rangle\,|0\rangle$,
For $x = 1, y = 0$: $|1\rangle\,|0\rangle \to |1\rangle\,|0 \oplus 1\rangle = |1\rangle\,|1\rangle$

For $x = 0, y = 1$: $|0\rangle\,|1\rangle \to |0\rangle\,|1 \oplus 0\rangle = |0\rangle\,|1\rangle$,
For $x = 1, y = 1$: $|1\rangle\,|1\rangle \to |1\rangle\,|1 \oplus 1\rangle = |1\rangle\,|0\rangle$

It can clearly be seen that if the first qubit is in state $|0\rangle$ the state of the second qubit is unchanged, but if the first qubit is in state $|1\rangle$ the second qubit undergoes a bit-flip, which is exactly the effect of the $CNOT$ gate. Therefore $O_f = CNOT = \wedge X$.

---

c. Compute the two-qubit output state of this circuit and the probability of getting an outcome 0 when measuring the upper qubit.

Solution: We can use the solution of Problem 2 of Tutorial 2 that shown that the circuit of our example is equivalent to a CNOT acting on the upper qubit and controlled by the lower qubit. It is easy to see that the output is then $|1\rangle \otimes |1\rangle$.

For completeness, we give below the general proof for arbitrary O_f. If we think of the circuit in layers, where the first layer is $H^{\otimes 2}$; the second, $O_f = CNOT$; and the third, again $H^{\otimes 2}$ we can write the state after each layer:

After layer 1: $|0\rangle|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = \frac{1}{2}(|0\rangle\otimes(|0\rangle-|1\rangle)+|1\rangle\otimes(|0\rangle-|1\rangle))$

After layer 2: $\frac{1}{2}(|0\rangle\otimes(|0\rangle-|1\rangle)+|1\rangle\otimes(|0\rangle-|1\rangle)) \to \frac{1}{2}|0\rangle\otimes(|0\oplus f(0)\rangle-|1\oplus f(0)\rangle)+\frac{1}{2}|1\rangle\otimes(|0\oplus f(1)\rangle-|1\oplus f(1)\rangle)$

Remark that when $f(x)=0$ we have $|0\oplus f(x)\rangle - |1\oplus f(x)\rangle = |0\rangle - |1\rangle$ and when $f(x)=1$ we have $|0\oplus f(x)\rangle - |1\oplus f(x)\rangle = (-1)(|0\rangle - |1\rangle)$, or equivalently $|0\oplus f(x)\rangle - |1\oplus f(x)\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$. Thus:

$$O_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle.$$

The state $|-\rangle$ is decoupled from the upper register at the beginning and the end of the circuit, so we can write in a more compact form:

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$

The state after *the action of layer 2* can then be written as:
$\frac{1}{2}(-1)^{f(0)}|0\rangle\otimes(|0\rangle-|1\rangle)+\frac{1}{2}(-1)^{f(1)}|1\rangle\otimes(|0\rangle-|1\rangle) = \frac{1}{\sqrt{2}}(-1)^{f(0)}\left(|0\rangle+(-1)^{f(1)-f(0)}|1\rangle\right)\otimes|-\rangle$

Finally, after *layer 3* we have:

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

Now, we can use the fact that $f(0)=0$ and $f(1)=1$ and so *after layer 3* we have the state $|1\rangle\otimes|1\rangle$.

So now, our output state is $|\psi_{\text{output}}\rangle = |1\rangle\otimes|1\rangle$ and we can clearly see that the probability of getting the outcome 0 on the upper qubit is 0.

---

d. Having found the probability of getting outcome 0 on the upper qubit, conclude whether the function is balanced or constant. Justify your answer.

Solution: Since we have that $P(0)=0$ we can therefore conclude that our function $f(x)$ is balanced, the final state of the algorithm is equivalent to:

$$|1\rangle\otimes|1\rangle = |f(0)\oplus f(1)\rangle\otimes|1\rangle$$

and we can therefore see that the function is balanced. This conclusion, of course, agrees with the answer of part A). The quantum algorithm recovers the correct solution (balanced function) with a single oracle call.

Problem 2: Phase kick-back

Suppose you have the balanced function $f : \{0,1\}^2 \to \{0,1\}$ such that:

$$f(0,0) = 0, f(0,1) = 1$$
$$f(1,0) = 1, f(1,1) = 0$$

a. A classical oracle C_f returns for a given query input $\bar{x}$ the value $f(\bar{x})$ of the Boolean function $f : \{0,1\}^n \to \{0,1\}$. We have seen that for every classical oracle there exist a quantum oracle O_f satisfying

$$O_f |\bar{x}\rangle |q\rangle = |\bar{x}\rangle |q \oplus f(\bar{x})\rangle .$$

Provide a circuit of 3 qubits implementing O_f for the function given above.

Solution: In order to construct the quantum circuit, we have to see what the action of the oracle is on the computational basis states. The register $|\bar{x}\rangle$ describes a two-qubit state. Let the third qubit be in the state $|q\rangle = |0\rangle$. The action of the oracle O_f on the four possible states is:

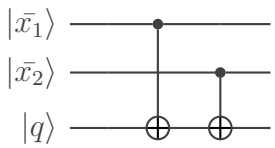
$$O_f |00\rangle |0\rangle = |00\rangle |0 \oplus f(0,0)\rangle = |00\rangle |0\rangle$$
$$O_f |01\rangle |0\rangle = |01\rangle |0 \oplus f(0,1)\rangle = |01\rangle |1\rangle$$
$$O_f |10\rangle |0\rangle = |10\rangle |0 \oplus f(1,0)\rangle = |10\rangle |1\rangle$$
$$O_f |11\rangle |0\rangle = |11\rangle |0 \oplus f(1,1)\rangle = |11\rangle |0\rangle$$

If the third qubit is in the state $|q\rangle = |1\rangle$, then the action of the oracle O_f on the four possible states is:

$$O_f |00\rangle |1\rangle = |00\rangle |1 \oplus f(0,0)\rangle = |00\rangle |1\rangle$$
$$O_f |01\rangle |1\rangle = |01\rangle |1 \oplus f(0,1)\rangle = |01\rangle |0\rangle$$
$$O_f |10\rangle |1\rangle = |10\rangle |1 \oplus f(1,0)\rangle = |10\rangle |0\rangle$$
$$O_f |11\rangle |1\rangle = |11\rangle |1 \oplus f(1,1)\rangle = |11\rangle |1\rangle$$

One can see that O_f can be implemented with two controlled-NOT gates. The first CNOT with the control qubit being the first qubit and the target being the last and the second CNOT with the control qubit being the second qubits and the target being again the last.

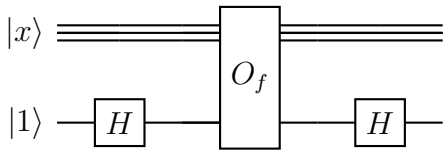
The circuit that implements O_f can be visualised below:



Additional information: Remark that the output of the lower qubit, when it starts as $|0\rangle$, encodes the parity of the two upper-qubits, i.e., $|x_3\rangle = |x_1 \oplus x_2\rangle$. One can see that measuring the third qubit will be equivalent to measuring the parity of the first two qubits, projecting their state to one of the two subspaces of the 2 qubits Hilbert space.

---

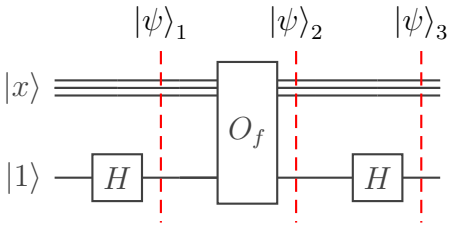
b. In the lecture, we have seen that the Oracle O_f can be used to implement a phase-kickback unitary U_f acting on the address qubits. Show that the circuit below



is equivalent to applying the phase kick-back U_f to the address register:

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle$$

Solution: We begin as usual by dividing the quantum circuit in subsequent steps:



The state of the composite system is:

$$|x\rangle |1\rangle \equiv |x\rangle \otimes |1\rangle$$

Step 1: On the first step, the register is left untouched while we act with the Hadamard operator on the second qubit. Thus, the state at step 1 is:

$$|\psi\rangle_1 = (I \otimes H)\,|x\rangle\,|1\rangle = |x\rangle\,\frac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle) = |x\rangle\,|-\rangle$$

where $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Step 2: At step 2 we act with the unitary U_f on the state $|\psi\rangle_1$ and get:

$$|\psi\rangle_2 = O_f\,|\psi\rangle_1 = O_f\,|x\rangle\,|-\rangle$$
$$\Rightarrow |x\rangle\,\frac{1}{\sqrt{2}}(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)$$

Remark that when $f(x) = 0$ we have $|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = |0\rangle - |1\rangle$ and when $f(x) = 1$ we have $|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = (-1)(|0\rangle - |1\rangle)$, or equivalently $|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$. We finally obtain:

$$O_f\,|x\rangle\,|-\rangle = (-1)^{f(x)}\,|x\rangle\,|-\rangle\,.$$

The state $|-\rangle$ is decoupled from the upper register at the beginning and the end of the circuit, so we can write in a more compact form:

$$U_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle$$

Step 3: It's easy to see that by acting once more with the Hadamard operator on the second qubit, the state $|-\rangle$ transforms back to $|1\rangle$ and thus the output state $|\psi\rangle_3$ is:

$$|\psi\rangle_3 = (-1)^{f(x)}\,|x\rangle\,|1\rangle$$

Since the state of the ancilla qubit $|1\rangle$ did not change after the action of the circuit, it can be omitted from further discussion. We can thus use the convention:

$$U_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle$$

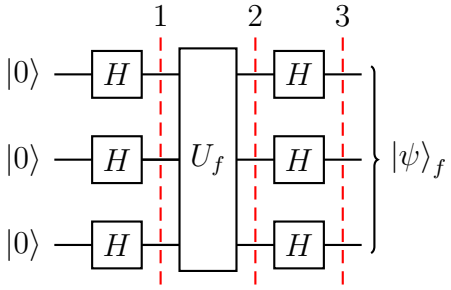
---

c. What is the size of the address register in the Deutsch algorithm in Problem 1?

Solution: On problem 1, the size of the register is just a single qubit, compared to problem 2 where the register consists of two qubits. Note that the size of the register is the same with the number of inputs of the boolean function.

Problem 3: Bernstein-Vazirani Algorithm

Consider the function $f(x) = ax \mod 2$ with the string a being $a =$'111'. The goal is to find a with a single call to the phase kick-back U_f. Consider the quantum circuit implementing the Bernstein-Vazirani algorithm:



a. Write the quantum state at stage 1 of the figure above, i.e. after the first layer of parallel Hadamard gates.

Solution: The initial 3-qubit state of the register and the target qubit is:

$$|000\rangle$$

Recall that the *Walsh-Hadamard* transformation of an n-dimensional computational basis $|x\rangle$ is:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{xy}|y\rangle$$

where:

$$xy \equiv \sum_{i=1}^{n} x_i y_i \tag{1}$$

In our case, the computational basis $|x\rangle$ is the 3-qubit state $|000\rangle$. Thus, the state of the composite system $|\psi\rangle_1$ after step Hence

$$|\psi\rangle_1 = \frac{1}{\sqrt{8}} \sum_{y\in\{0,1\}^3} |y_1 y_2 y_3\rangle$$

---

b. What transformation does the oracle U_f perform on the state $|x\rangle$, where x is a string of 3 bits encoding the computational basis of 3 qubits?

Solution: The action of the phase kick-back U_f on the computational basis states $|x\rangle = |x_1x_2x_3\rangle$ is:

$$\begin{aligned} U_f|x\rangle &= (-1)^{f(x)}|x\rangle \\ &= (-1)^{ax \mod 2}|x\rangle \\ &= (-1)^{ax}|x\rangle \end{aligned}$$

---

c. Calculate the state of the composite system at stage 2 of the circuit.

Solution: Using the results from the previous two questions:

$$\begin{aligned} |\psi\rangle_2 &= U_f|\psi\rangle_1 \\ &= U_f\frac{1}{\sqrt{8}}\sum_{y\in\{0,1\}^3}|y_1y_2y_3\rangle \\ &= \frac{1}{\sqrt{8}}\sum_{y\in\{0,1\}^3}U_f|y_1y_2y_3\rangle \\ &= \frac{1}{\sqrt{8}}\sum_{y\in\{0,1\}^3}(-1)^{ay}|y_1y_2y_3\rangle \end{aligned}$$

---

d. Derive the action of a layer of three Hadamard gates (Walsh-Hadamard transform) on a computational state $|x_1x_2x_3\rangle$ of three qubits.

Solution: We already showed that the Walsh-Hadamard transformation on n qubits is:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{xy}|y\rangle$$

It's trivial to see that if we restrict ourselves to a computational basis state of just three qubits $|x_1x_2x_3\rangle$ then the action of Walsh-Hadamard transformation is:

$$H^{\otimes 3}|x_1x_2x_3\rangle = \frac{1}{\sqrt{8}}\sum_{y_1\in\{0,1\}}\sum_{y_2\in\{0,1\}}\sum_{y_3\in\{0,1\}}(-1)^{x_1y_1+x_2y_2+x_3y_3}|y_1y_2y_3\rangle$$

---

e. Provide the quantum state at stage 3 of the computation.

Solution: Recall that the state of the composite system at stage 2 of the computation is:

$$|\psi\rangle_2 = \frac{1}{\sqrt{8}}\sum_{y\in\{0,1\}^3}(-1)^{ay}|y_1y_2y_3\rangle$$

We now act again with a Hadamard operator on each qubit. The state of the system $|\psi\rangle_3$ at stage 3 is thus:

$$\begin{aligned}
|\psi\rangle_3 = H^{\otimes 3}|\psi\rangle_2 &= H^{\otimes 3}\frac{1}{\sqrt{8}}\sum_{y\in\{0,1\}^3}(-1)^{ay}|y_1y_2y_3\rangle \\
&= \frac{1}{\sqrt{8}}\sum_{y\in\{0,1\}^3}(-1)^{ay}H^{\otimes 3}|y_1y_2y_3\rangle \\
&= \frac{1}{\sqrt{8}}\sum_{y\in\{0,1\}^3}(-1)^{ay}\left(\frac{1}{\sqrt{8}}\sum_{z\in\{0,1\}^3}(-1)^{yz}|z_1z_2z_3\rangle\right) \\
&= \frac{1}{8}\sum_{y\in\{0,1\}^3}(-1)^{ay}\left(\sum_{z\in\{0,1\}^3}(-1)^{yz}|z_1z_2z_3\rangle\right) \\
&= \frac{1}{8}\sum_{y\in\{0,1\}^3}\sum_{z\in\{0,1\}^3}(-1)^{(a_1+z_1)y_1+(a_2+z_2)y_2+(a_3+z_3)y_3}|z_1z_2z_3\rangle
\end{aligned}$$

---

f. Suppose that we perform a measurement on the first three qubits. What is the probability of the address qubits being $|000\rangle$ state? What would be the probability of obtaining $|111\rangle$?

Solution: The coefficient of the $|000\rangle$ state is

$$\begin{aligned}
&\frac{1}{8}\sum_{y\in\{0,1\}^3}(-1)^{(1+0)y_1+(1+0)y_2+(1+0)y_3} \\
&= \frac{1}{8}\sum_{y\in\{0,1\}^3}(-1)^{y_1+y_2+y_3} \\
&= 0
\end{aligned}$$

The coefficient of the $|111\rangle$ state is

$$\begin{aligned}
&\frac{1}{8}\sum_{y\in\{0,1\}^3}(-1)^{(1+1)y_1+(1+1)y_2+(1+1)y_3} \\
&= \frac{1}{8}\sum_{y\in\{0,1\}^3}(-1)^{2(y_1+y_2+y_3)} \\
&= \frac{1}{8}\sum_{y\in\{0,1\}^3}((-1)^2)^{(y_1+y_2+y_3)} \\
&= 1
\end{aligned}$$

Hence the probabilities of measuring $|000\rangle$ and $|111\rangle$ are 0 and 1 respectively. In fact, since the probability of measuring $|111\rangle$ is 1, it must be the case that the probability of any other outcome is zero. Hence, we have recovered the bitstring $a =' 111'$ in just one quantum query.
