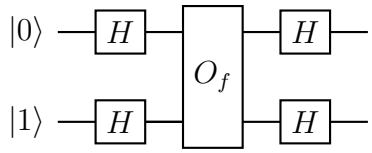
Problem 1: Deutsch's Algorithm

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 $f(0) = 0 \neq f(1) = 1$, we can conclude that f is not constant. Moreover, there is a single input that gives 0 and a single input that gives 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 $x, y \in \{0, 1\}$:

$$|0\rangle|0\rangle \to |0\rangle|0 \oplus 0\rangle = |0\rangle|0\rangle\,, \quad |1\rangle|0\rangle \to |1\rangle|0 \oplus 1\rangle = |1\rangle|1\rangle\,,$$
$$|0\rangle|1\rangle \to |0\rangle|1 \oplus 0\rangle = |0\rangle|1\rangle\,, \quad |1\rangle|1\rangle \to |1\rangle|1 \oplus 1\rangle = |1\rangle|0\rangle\,.$$

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 $O_f = \text{CNOT} = \wedge X$.

---

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

Solution: We can use the solution of Problem 2 of Tutorial 2, which showed that the circuit of our example is equivalent to a CNOT acting on the upper qubit and controlled by the lower qubit. Since the lower qubit is in $|1\rangle$, the upper qubit is flipped and the output is $|1\rangle \otimes |1\rangle$.

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

After layer 1:

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

After layer 2:

$$\frac{1}{2}|0\rangle \otimes \big(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle\big) + \frac{1}{2}|1\rangle \otimes \big(|0\oplus f(1)\rangle - |1\oplus f(1)\rangle\big)$$

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 $|0\oplus f(x)\rangle - |1\oplus f(x)\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$ (this is the phase kick-back studied in Problem 2). The state after layer 2 can then be written as:

$$\begin{aligned}&\frac{1}{2}(-1)^{f(0)}|0\rangle \otimes (|0\rangle - |1\rangle) + \frac{1}{2}(-1)^{f(1)}|1\rangle \otimes (|0\rangle - |1\rangle)\\ &= \frac{(-1)^{f(0)}}{\sqrt{2}}\big(|0\rangle + (-1)^{f(1)-f(0)}|1\rangle\big) \otimes |-\rangle\end{aligned}$$

After layer 3: using $H|-\rangle = |1\rangle$,

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

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 our output state is $|\psi_{\text{output}}\rangle = |1\rangle \otimes |1\rangle$, and the probability of getting 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: From part c, the final state of the algorithm for a general f is

$$(-1)^{f(0)}|f(0)\oplus f(1)\rangle \otimes |1\rangle,$$

so measuring the upper qubit gives, with certainty, the outcome $f(0)\oplus f(1)$. Outcome 0 means $f(0) = f(1)$ (constant), and outcome 1 means $f(0) \neq f(1)$ (balanced). Since we found $\Pr(0) = 0$, we always obtain outcome 1, so $f(0)\oplus f(1) = 1$ and the function is **balanced**. This conclusion, of course, agrees with the answer of part a. The quantum algorithm recovers the correct answer (balanced function) with a single oracle call.

Problem 2: Phase kick-back and the phase oracle

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

$$\begin{aligned}f(0,0) = 0, \quad f(0,1) = 1,\\ f(1,0) = 1, \quad f(1,1) = 0.\end{aligned}$$

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

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

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 $|x\rangle$ 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:

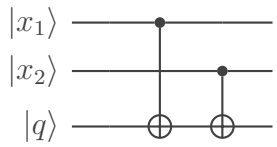
$$\begin{aligned}
O_f |00\rangle |0\rangle &= |00\rangle |0 \oplus f(0,0)\rangle = |00\rangle |0\rangle \\
O_f |01\rangle |0\rangle &= |01\rangle |0 \oplus f(0,1)\rangle = |01\rangle |1\rangle \\
O_f |10\rangle |0\rangle &= |10\rangle |0 \oplus f(1,0)\rangle = |10\rangle |1\rangle \\
O_f |11\rangle |0\rangle &= |11\rangle |0 \oplus f(1,1)\rangle = |11\rangle |0\rangle
\end{aligned}$$

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:

$$\begin{aligned}
O_f |00\rangle |1\rangle &= |00\rangle |1 \oplus f(0,0)\rangle = |00\rangle |1\rangle \\
O_f |01\rangle |1\rangle &= |01\rangle |1 \oplus f(0,1)\rangle = |01\rangle |0\rangle \\
O_f |10\rangle |1\rangle &= |10\rangle |1 \oplus f(1,0)\rangle = |10\rangle |0\rangle \\
O_f |11\rangle |1\rangle &= |11\rangle |1 \oplus f(1,1)\rangle = |11\rangle |1\rangle
\end{aligned}$$

Since $f(x_1, x_2) = x_1 \oplus x_2$, one can see that O_f can be implemented with two CNOT gates: the first with the first qubit as control and the last qubit as target, and the second with the second qubit as control and again the last qubit as target.

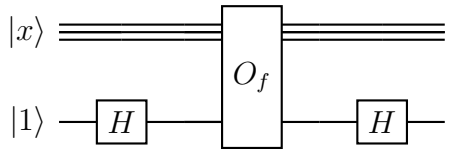
The circuit that implements O_f can be visualised below:



Additional information: Remark that when the lower qubit starts as $|0\rangle$, its output encodes the parity of the two upper qubits, i.e. it ends in the state $|x_1 \oplus x_2\rangle$. Measuring the third qubit is therefore equivalent to measuring the parity of the first two qubits, which projects their state onto one of the two parity subspaces of the two-qubit Hilbert space: the even subspace span$\{|00\rangle, |11\rangle\}$ or the odd subspace span$\{|01\rangle, |10\rangle\}$.

---

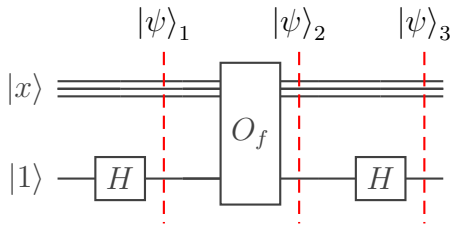
b. In the lectures, we have seen that the oracle O_f can be used to implement a phase oracle U_f acting on the address qubits. Show that the circuit below



is equivalent to applying the phase oracle 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 into steps:



The initial state of the composite system is:

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

Step 1: In the first step, the register is left untouched while we act with the Hadamard operator on the last 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 oracle O_f on the state $|\psi\rangle_1$ and get:

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

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:

$$|\psi\rangle_2 = O_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle .$$

The phase $(-1)^{f(x)}$ has been "kicked back" from the target qubit onto the address register.

Step 3: By acting once more with the Hadamard operator on the last qubit, the state $|-\rangle$ transforms back to $|1\rangle$ and thus the output state $|\psi\rangle_3$ is:

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

The state of the ancilla qubit, $|1\rangle$, did not change after the action of the circuit. Moreover, the ancilla is decoupled from the upper register: the output is a tensor product

$\big((-1)^{f(x)}|x\rangle\big)\otimes|1\rangle$, and the ancilla is in the same state $|1\rangle$ for any input $|x\rangle$ of the upper register. It therefore carries no information about x and can be omitted from further discussion. Furthermore, any subsequent operation acting solely on the upper register, i.e. of the form $U\otimes I$, leaves the lower register unchanged, since $(U\otimes I)\big(|\phi\rangle\otimes|1\rangle\big)=U|\phi\rangle\otimes|1\rangle$. The ancilla can therefore be effectively removed from the circuit, provided the remainder of the circuit does not act on it. The circuit therefore acts on the address register as the phase oracle

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

and, by linearity, it acts in the same way on any superposition of computational basis states.

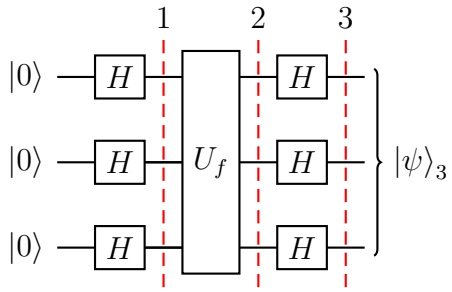
---

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

Solution: In Problem 1, the address register is just a single qubit, compared to Problem 2 where the register consists of two qubits. Note that the size of the address register equals the number of input bits n of the Boolean function $f:\{0,1\}^n\to\{0,1\}$.

Problem 3: Bernstein-Vazirani Algorithm

Consider the function $f(x)=a\cdot x \bmod 2$, where $a\cdot x=\sum_i a_i x_i$, with the string $a=111$. The goal is to find a with a single call to the phase oracle 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 is $|000\rangle$. Each Hadamard gate maps $|0\rangle$ to $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, so the state at stage 1 is

$$|\psi\rangle_1=H^{\otimes 3}|000\rangle=|+\rangle|+\rangle|+\rangle=\frac{1}{\sqrt{8}}\sum_{y\in\{0,1\}^3}|y_1y_2y_3\rangle\,,$$

i.e. the equal superposition of all eight computational basis states.

---

b. What transformation does the phase 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 oracle U_f on the computational basis states $|x\rangle = |x_1x_2x_3\rangle$ is:

$$\begin{aligned} U_f|x\rangle &= (-1)^{f(x)}|x\rangle \\ &= (-1)^{a\cdot x \bmod 2}|x\rangle \\ &= (-1)^{a\cdot x}|x\rangle, \end{aligned}$$

where in the last step we used that $(-1)^k$ only depends on the parity of k.

---

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

Solution: Using the results from the previous two questions and linearity:

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

---

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

Solution: For a single qubit, $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which can be written compactly as

$$H|x_i\rangle = \frac{1}{\sqrt{2}}\sum_{y_i\in\{0,1\}}(-1)^{x_iy_i}|y_i\rangle, \qquad x_i\in\{0,1\}.$$

Since $H^{\otimes 3}|x_1x_2x_3\rangle = H|x_1\rangle\otimes H|x_2\rangle\otimes H|x_3\rangle$, we obtain

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

where $x\cdot y = \sum_i x_iy_i$. The same argument gives, for n qubits,

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

---

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:

$$|\psi\rangle_2 = \frac{1}{\sqrt{8}} \sum_{y\in\{0,1\}^3} (-1)^{a\cdot y} |y_1 y_2 y_3\rangle$$

We now act again with a Hadamard operator on each qubit. Using the result of part d, the state $|\psi\rangle_3$ at stage 3 is:

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

The sum in brackets factorises as $\prod_{i=1}^{3} (1 + (-1)^{a_i+z_i})$. Each factor equals 2 if $z_i = a_i$ and 0 otherwise, so the sum equals 8 if $z = a$ and 0 otherwise. Hence

$$|\psi\rangle_3 = |a\rangle = |111\rangle \,.$$

---

f. Suppose that we perform a measurement in the computational basis. What is the probability of the outcome being the $|000\rangle$ state? What would be the probability of obtaining $|111\rangle$?

Solution: The probability of an outcome is the squared modulus of its amplitude. Using the expression for $|\psi\rangle_3$ from part e (before simplifying), the amplitude of the $|000\rangle$ state is

$$\begin{aligned}
\langle 000|\psi_3\rangle &= \frac{1}{8} \sum_{y\in\{0,1\}^3} (-1)^{(1+0)y_1 + (1+0)y_2 + (1+0)y_3} \\
&= \frac{1}{8} \sum_{y\in\{0,1\}^3} (-1)^{y_1+y_2+y_3} \\
&= 0,
\end{aligned}$$

since four of the eight terms are $+1$ and four are -1. The amplitude of the $|111\rangle$ state is

$$\begin{aligned}\langle 111|\psi_3\rangle &= \frac{1}{8}\sum_{y\in\{0,1\}^3}(-1)^{(1+1)y_1+(1+1)y_2+(1+1)y_3}\\ &= \frac{1}{8}\sum_{y\in\{0,1\}^3}\left((-1)^2\right)^{y_1+y_2+y_3}\\ &= \frac{1}{8}\cdot 8 = 1.\end{aligned}$$

Hence the probabilities of measuring $|000\rangle$ and $|111\rangle$ are $|\langle 000|\psi_3\rangle|^2 = 0$ and $|\langle 111|\psi_3\rangle|^2 = 1$, respectively. In fact, since the probability of measuring $|111\rangle$ is 1, the probability of any other outcome must be zero, in agreement with $|\psi\rangle_3 = |111\rangle$ from part e. Hence, we have recovered the bitstring $a = 111$ with just one query to the phase oracle.
