Raul Garcia-Patron
Petros Wallden
Milos Prokop

IQC 2023-24
November 2, 2023

# Tutorial 4

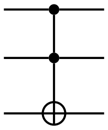
## Problem 1: Grover's Algorithm

Consider a search space of dimension $N = 4$ with its elements encoded in binary $\{00, 01, 10, 11\}$. Suppose you are searching for the element $z = 11$.

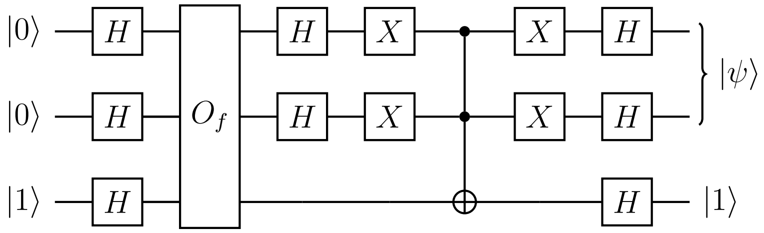
**a.** Construct the circuit implementing the quantum oracle $O_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ for the function:

$$f(x) = \begin{cases} 1 & \text{for } x = z \\ 0 & \text{otherwise} \end{cases}$$

**Solution:** In order to construct the circuit that implements the quantum oracle, we need to see how it acts in the computational basis. We see that the register consists of two qubits. The classical function returns one only if $x_1x_2 =$'11'. If we look carefully on the action of the oracle, we can see that the target qubit is flipped only if both the register qubits are in the $|1\rangle$ state. This is exactly the action of the controlled-controlled-NOT operator. Thus the quantum circuit implementing the oracle is:



**b.** We can now construct the quantum circuit which performs the initial Hadamard transformations and a single Grover iteration $G$:



1. Compute the output state.

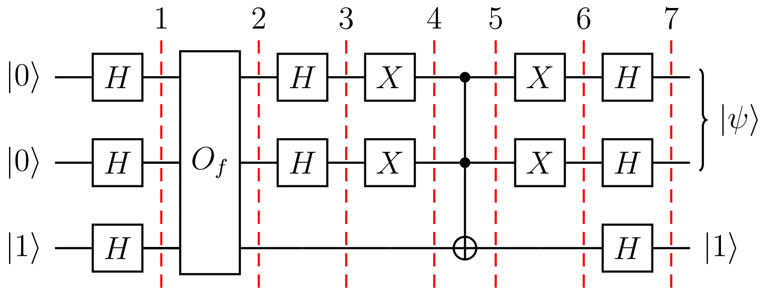
2. What happens after we measure the output in the computational basis?

3. How many times do we have to repeat $G$ to obtain $z$ in this example?

4. In the lecture we saw the scaling of Grover algorithm is $T \approx \frac{\pi}{4}2^{n/2}$, which could have lead us to think that we would need 2 Grover steps to find the solution. What would be wrong with our reasoning?

**Solution:**

1. First of all, we have to divide the quantum circuit into steps and calculate the state of the composite system in every subsequent stage.



The three-qubit state at step 1 is:

$$|\psi\rangle_1 = H^{\otimes 2}|001\rangle = \frac{1}{2}(|00\rangle|-\rangle + |01\rangle|-\rangle + |10\rangle|-\rangle + |11\rangle|-\rangle)$$

We choose to write it in this form in order to use the fact that the action of the oracle on the state $|x\rangle|-\rangle$, where $|x\rangle$ is a computational basis state is:

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

By using the above property, the action of the oracle at step 2 is:

$$\begin{aligned}|\psi\rangle_2 &= \frac{1}{2}\left(|00\rangle|-\rangle + |01\rangle|-\rangle + |10\rangle|-\rangle - |11\rangle|-\rangle\right)\\ &= \frac{1}{2}\left(|0\rangle|+\rangle + |1\rangle|-\rangle\right)|-\rangle\end{aligned}$$

At step 3, we act with the Hadamard operator on the register qubits, i.e:

$$|\psi\rangle_3 = (H \otimes H \otimes I)|\psi\rangle_2 = \frac{1}{2}\left(|+\rangle|0\rangle + |-\rangle|1\rangle\right)|-\rangle,$$

where the action of the gates left the state invariant. At step 4, we apply NOT gates on the address qubits, which using $X|-\rangle = |-\rangle$ leads to:

$$|\psi\rangle_4 = \frac{1}{2}\left(|+\rangle|1\rangle - |-\rangle|0\rangle\right)|-\rangle,$$

which can be written as:

$$|\psi\rangle_4 = \frac{1}{2}(|01\rangle + |11\rangle - |00\rangle + |10\rangle)|-\rangle$$

Then we act with the controlled-controlled-NOT operator on $|\psi\rangle_4$ and the state becomes:

$$|\psi\rangle_5 = \frac{1}{2}(|01\rangle - |11\rangle - |00\rangle + |10\rangle)|-\rangle$$

On step 6, we flip again the first two qubits:

$$|\psi\rangle_6 = \frac{1}{2}(|10\rangle - |00\rangle - |11\rangle + |01\rangle)\,|-\rangle = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\,|-\rangle = -\,|-\rangle\,|-\rangle\,|-\rangle\,.$$

Thus the final action of the Hadamard operator is trivial. Since the global phase has no physical consequence we can neglect it and see that all qubits at the end of the circuit will be in the $|1\rangle$ state and thus the output state will be:

$$|\psi\rangle_f = |11\rangle\,|1\rangle$$

2. If we measure the output in the computation basis we always obtain the output 11, the output 11 has probability one.

3. We can see that in this example we have to repeat $G$ only once.

4. There relation $T \approx \frac{\pi}{4}2^{n/2}$, which is almost 2 for $n = 2$, was using two approximation, firstly $T >> 1$, $\theta_0 << 1$ such that $\theta_0 = \sin\theta_0$, that are not necessarily true in our example with so restricted number of qubits. On the other hand, if we revisit the relation $(2T + 1)\theta_0 = \pi/2$ and using the fact that for $n = 2$ we have $\sin\theta_0 = 1/2$ and therefore $\theta_0 = \pi/6$ we obtain $T = 1$ as we have observed before.

   Remark that for large $n$ we will rarely achieve exactly $\pi/2$ (full rotation) after the $T$ Grover iterations, but rather $\pi/2-\delta$. This will lead to an error on guessing the solution with small probability $\delta$ (assuming $\delta << 1$ as expected if $N >> 1$), which can be made further small by repeating the algorithm few times.

# Problem 2: Simon's Algorithm

Suppose we run Simon's algorithm on the following function $f(x) : \{0,1\}^3 \rightarrow \{0,1\}^3$.

$$\begin{aligned} f(000) = f(111) = 000 \\ f(001) = f(110) = 001 \\ f(010) = f(101) = 010 \\ f(011) = f(100) = 011 \end{aligned}$$

Where $f(x)$ is $2 - \text{to} - 1$ and f$(x_i) = f(x_i \oplus 111)$ for all $i \in \{0,1\}^3$; therefore the period is $a = 111$.

**a.** What is the initial input of Simon's algorithm?

**Solution:** The input of Simon's algorithm is:

1. A function of the form (as described above) $f(x) : \{0,1\}^3 \rightarrow \{0,1\}^3$, with the function *promised* to obey the property: there exists a string $a \in \{0,1\}^3$ such that $[f(x) = f(y)] \iff [x \oplus y \in \{0^3, a\}]$ for all $x, y \in \{0,1\}^3$.

2. Access to this function restricted to queries of a quantum oracle.

3. The function is also determined by its domain, and the initial input state of Simon's algorithm is: $|0^n\rangle \otimes |0^n\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$. So in this case, we would have for $n = 3$: $|\psi_{\text{initial}}\rangle = |0^3\rangle \otimes |0^3\rangle = |000\rangle \otimes |000\rangle = |000000\rangle$.

**b.** What will the state be after:

1. the first layer of Hadamard gates applied to the the upper three qubits.
2. the phase kickback unitary generated by the oracle query.

**Solution:**

i) After the first Hadamard transform on the first three qubits $|\psi\rangle' = (H^{\otimes 3}|0^3\rangle) \otimes |0^3\rangle$, we have:
$|\psi\rangle' = (\sum_{x\in\{0,1\}^3} \frac{1}{\sqrt{2^3}}|x\rangle) \otimes |0^3\rangle = \frac{1}{\sqrt{2^3}} \sum_{x\in\{0,1\}^3} (|x\rangle \otimes |0^3\rangle)$

ii) After the Oracle query, we have:
$|\psi\rangle'' = \frac{1}{\sqrt{2^3}} \sum_{x\in\{0,1\}^3} |x\rangle |f(x)\rangle$
$= \frac{1}{\sqrt{2^3}}(|000\rangle|f(000)\rangle + |001\rangle|f(001)\rangle + |010\rangle|f(010)\rangle + |011\rangle|f(011)\rangle + |100\rangle|f(100)\rangle + |101\rangle|f(101)\rangle + |110\rangle|f(110)\rangle + |111\rangle|f(111)\rangle)$
$= \frac{1}{\sqrt{2^3}}((|000\rangle + |111\rangle)|000\rangle + (|001\rangle + |110\rangle)|001\rangle + (|010\rangle + |101\rangle)|010\rangle + (|011\rangle + |100\rangle)|011\rangle)$
$= \frac{1}{2}(\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)|000\rangle + \frac{1}{\sqrt{2}}(|001\rangle+|110\rangle)|001\rangle + \frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)|010\rangle + \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle)|011\rangle)$.

**c.** What would the state be after measuring the second register, supposing that the measurement gave $|001\rangle$?

**Solution:** To answer this question we need to apply the projector $I \otimes |001\rangle\langle 001|$ to $|\psi''\rangle$. Because $|x\rangle\langle x||y\rangle \neq 0$ if and only if $x = y$, we obtain

$$I \otimes P_{001}|\psi''\rangle = I \otimes |001\rangle\langle 001||\psi''\rangle = \frac{1}{2}\frac{1}{\sqrt{2}}(|001\rangle + |110\rangle) = \tag{1}$$

We can see that the only term that will remain if we measure the second register and get the state $|001\rangle$ with probability 1/4, as it correspond to the square of the norm of the result of the projection, while the upper-register after the outcome measurement reads $|\psi\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle) = \frac{1}{\sqrt{2}}(|001\rangle + |001 \oplus a\rangle)$.

**d.** Imagine we now apply the final step, three Hadamard transforms. Using the formula $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle$, write the state after applying this step.

**Solution:** Applying $H^{\otimes 3}$ on the state $\frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)$ gives us

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{2^3}}\frac{1}{\sqrt{2}}\left(\sum_{z_1,z_2,z_3\in\{0,1\}}(-1)^{z_3}|z_1z_2z_3\rangle + \sum_{z_1,z_2,z_3\in\{0,1\}}(-1)^{z_1+z_2}|z_1z_2z_3\rangle\right) \tag{2}$$

which after some re-arrangement reads:

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{2^3}}\frac{1}{\sqrt{2}}\left(\sum_{z_1,z_2,z_3\in\{0,1\}}(-1)^{z_3}\left(1+(-1)^{z_1+z_2}\right)|z_1z_2z_3\rangle\right). \tag{3}$$

We see an interference where the amplitude of outcomes satisfying the equation $y_1 \oplus y_2 \oplus y_3 = a \cdot y = 0$ is amplified to 2, while the amplitude of those satisfying $y_1 \oplus y_2 \oplus y_3 = a \cdot y = 1$ are cancel to 0, i.e.,

$$|\tilde{\psi}\rangle = \frac{1}{2}\left(\sum_{z_1,z_2,z_3\in\{0,1\}:a\cdot z=0}(-1)^{z_3}|z_1z_2z_3\rangle\right). \tag{4}$$

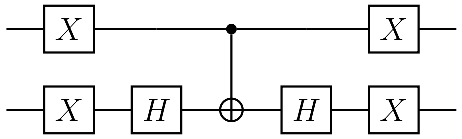
Remark that the normalization is correct as there are 4 potential equiprobable outcomes satisfying $y_1 \oplus y_2 \oplus y_3 = 0$. We see that the probability of events satisfying $y_1 \oplus y_2 \oplus y_3 = a \cdot y = 0$ is amplified, while those satisfying $y_1 \oplus y_2 \oplus y_3 = a \cdot y = 1$ do not occur at all, where the sum runs over the 4 existing combinations of $z_1z_2z_3$ that satisfy the condition $a \cdot z = 0$.

**e.** If the first run of the algorithm gives $y = 011$ and the second run gives $y = 101$. Show that, assuming $a \neq 000$, these two runs of the algorithm already determine that $a = 111$.

**Solution:** As discussed in the lecture it must hold for the period $a$ that $a \cdot 011 = 0$ and that $a \cdot 101 = 0$. For $a \in \{000, 100, 011, 111\}$ the first equation is fulfilled and for $a \in \{000, 010, 101, 111\}$ the second equation is fulfilled. This means that for $a \in \{000, 111\}$ both equations are fulfilled and since it is assumed that $a \neq 000$ it follows that $a = 111$. An alternative explanation could be that $a \cdot 011 = 0$ implies $a_2 \oplus a_3 = 0$ and $a \cdot 101 = 0$ implies $a_1 \oplus a_3 = 0$. This is equivalent to $a_2 = a_3$ and $a_1 = a_3$, which implies that $a_1 = a_2 = a_3$ leading to $a = 111$ as the only non-zero solution.

# Problem 3: Phase kick-back without ancillary qubit

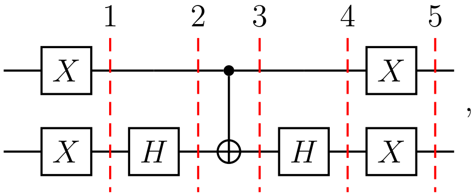
**a.** The target (lower) qubit is a catalytic qubit used to implement a phase-kickback unitary on the address (top) qubits. Show that the circuit below implements the *conditional phase shift transformation* $2|00\rangle\langle 00| - I$,



,

up to a global phase. This allows to replace the circuit on the right of the oracle $O_f$ by a 2-qubit circuit that uses a single CNOT instead of a control-control-NOT

**Solution:** There are two ways to prove that the above circuit it the conditional phase shift transformation. The first is to use the matrix representation of each gate and do the gate concatenation. The other is to see what this action of the circuit is on each computational basis state. We will use the latter. Like always, we break the circuit into steps.



A compact proof of this result uses the notation of $4x4$ matrices a blocs of $2x2$ matrices and the use of the rules of tensor product of matrices. So the circuit can be written as a unitary:

$$U = \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix} \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix}.$$

This leads to

$$U = \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix} \begin{pmatrix} H^2 & 0 \\ 0 & HXH \end{pmatrix} \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix},$$

where using $H^2 = I$ and $HXH = Z$ we obtain

$$U = \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & Z \end{pmatrix} \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix} = \begin{pmatrix} XZX & 0 \\ 0 & X^2 \end{pmatrix} = \begin{pmatrix} -Z & 0 \\ 0 & I \end{pmatrix}, \tag{5}$$

where we used $XZX = -Z$ and $X^2 = I$. Therefore,

$$U = \begin{pmatrix} -Z & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = -(2\left|00\right\rangle\left\langle 00\right| - I)$$

We can see that up to a negligible phase, the above circuit is equivalent to the *conditional phase shift transformation.*

**b.** Taking inspiration from the results from the previous subquestion and subquestion a. construct a 2-qubit quantum circuit which performs the phase kickback unitary corresponding to the oracle $O_f$.

**Solution:** We need to construct a 2-qubit quantum circuit which performs the phase kickback unitary corresponding to the oracle $O_f$. Recall from the previous tutotial that when the ancilla qubit is initialised in the $|-\rangle$ then the action of the oracle on the register plus the ancilla is:

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

we can thus neglect the ancilla qubit and think of the transformation as a unitary gate $U_f$ acting only on the register qubits.

For a given input $|x_1x_2\rangle$ the unitary $U_f$ will output $U_f|x_1x_2\rangle = (-1)^{x_1x_2}|x_1x_2\rangle$, or equivalently and so the matrix form of $U_f$ is:

$$U_f = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

and we can conclude that the unitary $U_f$ is actually a controlled-Z operation, which itself can be implemented using a CNOT preceded and followed by Hadamard gates on the target qubit (but not on the control qubit).

Remark that the difference with respect to the question before is that the $-1$ act on $|11\rangle$ instead of $|00\rangle$. The roles of the $X$ gates in the previous circuit is to exchange the roles of the two.