Quantum Information and Quantum Computing, Solutions 3

Assistant : sara.alvesdossantos@epfl.ch, clemens.giuliani@epfl.ch

Problem 1 : Elementary quantum circuits

In this problem set, we are going to analyse some elementary quantum circuits and their properties.

1. To see the equivalence between the SWAP gate and the three CNOT, let's see how these gates act on a two-qubit state of the computational basis:

$$\text{SWAP}|x,y\rangle = |y,x\rangle \tag{1}$$
$$\text{CNOT}_{0,1}|x,y\rangle = |x,y\oplus x\rangle \tag{2}$$
$$\text{CNOT}_{1,0}|x,y\rangle = |x\oplus y,y\rangle \tag{3}$$

Therefore, the left-hand side of the equivalence to be proven reads

$$\begin{aligned}\text{CNOT}_{0,1}\left[\text{CNOT}_{1,0}\left(\text{CNOT}_{0,1}|x,y\rangle\right)\right] &= \text{CNOT}_{0,1}\left[\text{CNOT}_{1,0}|x,y\oplus x\rangle\right]\\ &= \text{CNOT}_{0,1}|x\oplus y\oplus x,y\oplus x\rangle\\ &= \text{CNOT}_{0,1}|y,y\oplus x\rangle\\ &= |y,y\oplus x\oplus y\rangle = |y,x\rangle\end{aligned}$$

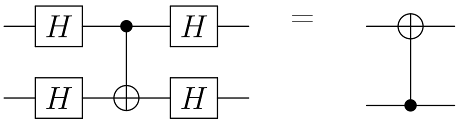
Recalling that $x\oplus x=0\,,\ x\in\{0,1\}$, that proves the equivalence.

2. To prove the equivalence, we can note that it's action in the computational basis is only $\text{CZ}|11\rangle = -|11\rangle$, otherwise it acts as the identity. The matrix representation for both circuits is

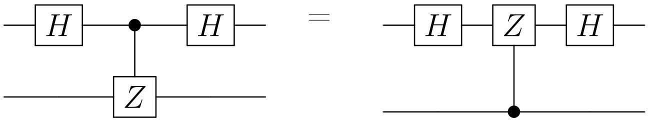
$$\text{CZ} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix} \tag{4}$$

so they are equivalent.

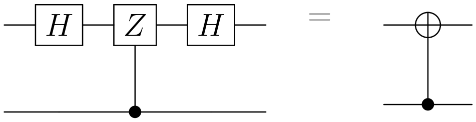
Now we can use this last equivalence to prove



At first, we use the single-qubit gate equivalence $HXH = Z$ to rewrite it as



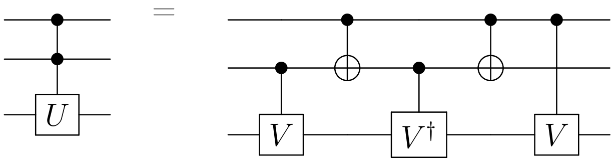
where to invert the control Z we used the equivalence proved in the previous point, and $H^2 = \mathbb{1}$. Now again from the last equivalence, using the inverse $HZH = X$ we have



Notice that the relation $HZH = X$ can be applied even if the Z is a controlled operation. In fact, if Z is not triggered by the control qubit.

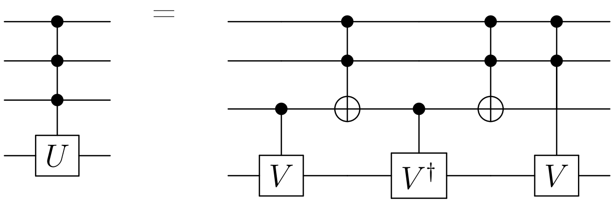
3. Assume we are allowed to use multiple-controlled X (NOT) and V gates (but only up to c^{n-1}) when we want to realise a c^n gate). Then the circuit can be implemented by generalising the identity used to construct the c-c-U.

   Suppose we are able to implement c-V and c-$V^\dagger$, with V such that $V^2 = U$, now we can create a a circuit for the c-c-U in the following way

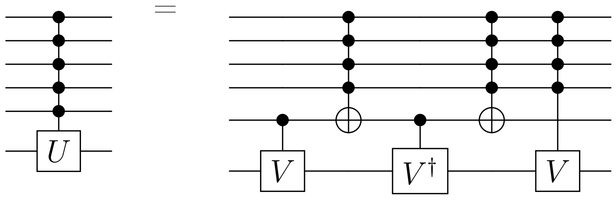


   In this way, we apply V^2 only if both the first and the second qubits are in $|1\rangle$.

   To generalise the circuit above to $c^3(U)$ we replace every controlled gate with a doubly controlled gate.



And finally, to generalise this circuit even more, we replace every controlled gate with a c^n gate. This is possible without ancillae if we have access to $c^{n-1}V$ and NOT . So in particular if we want a c^5-U gate the circuit we have to implement is the following



where the idea of the circuit is the same as before: we apply V^2 only if the first five qubits are in $|1\rangle^{\otimes 5}$.

4. We know that the general circuit to implement a QFT on a n-qubit system is

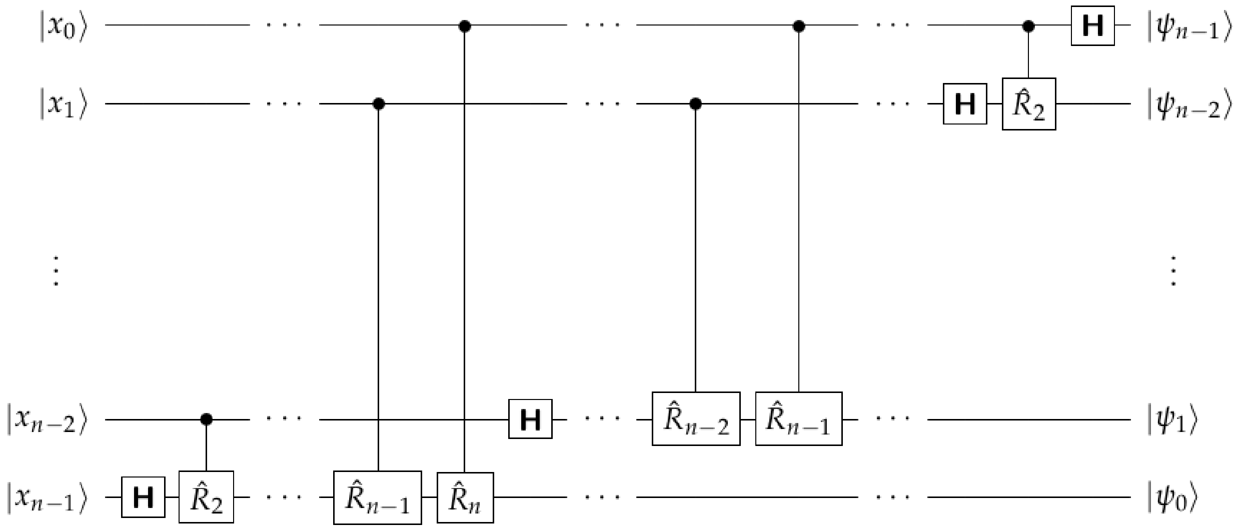


Figure 1: General circuit for the QFT on a n-qubit system

where

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \tag{5}$$

The circuit can be designed also in the reverse qubit order, by applying $\frac{n}{2}$ SWAP gate at the end. Since we are considering a 3-qubits system we have

$$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{2}} \end{bmatrix} = S \quad , \quad R_1 = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{bmatrix} = T \tag{6}$$

therefore the circuit in the problem set is indeed the circuit for the QFT on a $n = 3$ qubit system. Alternatively, you can start from an input state in the computational basis and compute explicitly the quantum state after every stage of the circuit, to show that at the end one gets the corresponding Fourier-transformed state.

The corresponding unitary matrix we want to write has dimension $N \times N = 8 \times 8$, its form can be obtained considering the action of the QFT over a vector of the computational basis $|x\rangle_8$, $x \in \{0, \dots, 7\}$; the general action is:

$$F_Q|x\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i k x/N} |k\rangle \tag{7}$$

considering $N = 8$ and defining $e^{2\pi i/8} = w$

$$F_Q|x\rangle_3 = \frac{1}{\sqrt{8}} \sum_{k=0}^{N-1} w^{kx} |k\rangle_3 \tag{8}$$

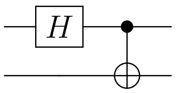
Since $|x\rangle_3$ and $|k\rangle_3$ are basis vectors, the coefficient applied to them are the component of the matrix

$$F_{Q_{xk}} = \frac{1}{\sqrt{8}} w^{xk} \quad x, k \in \{0, \dots, 7\} \tag{9}$$

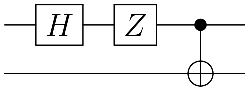
therefore the first column and row are made of 1 and the other matrix elements are powers of w

5. Bell states can be generated using a single-qubit gate H to create the superposition, Z and X to flip values or phases, and finally the two-qubit gate CNOT for the entanglement

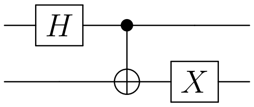
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \tag{10}$$



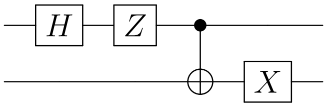
$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} = \tag{11}$$



$$\frac{|01\rangle + |10\rangle}{\sqrt{2}} = \tag{12}$$



$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \tag{13}$$



Problem 2 : Quantum teleportation

In this problem we will see how Bell (i.e. entangled) states can be used to teleport the quantum state of a qubit, by additionally sharing classical information between the two parties.

First, let's rewrite the initial state in a more compact form:

$$|\Psi_0\rangle = |\psi\rangle \otimes |\beta_{00}\rangle = \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |111\rangle) \tag{14}$$

where we dropped all the indices. Now we can start looking at the quantum teleportation protocol.

1. Alice applies to her two qubits a Controlled-NOT gate. Since Alice acts only on her own qubits, the transformation on the whole system of 3 qubits can be written as

$$\text{C-NOT} \otimes \mathbb{I} = |0\rangle\langle 0| \otimes \mathbb{I} \otimes \mathbb{I} + |1\rangle\langle 1| \otimes X \otimes \mathbb{I} \tag{15}$$

and its action on the state of the system $|\Psi_0\rangle$ is

$$[\text{C-NOT} \otimes \mathbb{I}]\,|\Psi_0\rangle = \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle) = |\Psi_1\rangle \tag{16}$$

2. The Hadamard gate is a single-qubit gate and its action on states $|0\rangle$ and $|1\rangle$ is

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{17}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{18}$$

In this case the transformation on the whole system is

$$[H \otimes \mathbb{I} \otimes \mathbb{I}]\,|\Psi_1\rangle = \frac{\alpha}{2}(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + \frac{\beta}{2}(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle) = |\Psi_2\rangle \tag{19}$$

We can rewrite the $|\Psi_2\rangle$ state in a easier to interpret way as a sum of tensor product states between Alice's and Bob's parts

$$|\Psi_2\rangle = \frac{1}{2}[|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + \\ + |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)] \tag{20}$$

3. From the expression of $|\Psi_2\rangle$ it's easy to see that, if Alice measures the qubits 1 and 2 in the computational basis, her qubits state is projected onto one of the four possible outcomes $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, and Bob's qubit is correspondingly projected in one of the four states entering the expression for $|\Psi_2\rangle$.

The probability of each outcome $|xy\rangle$ is

$$P_{xy} = |\langle xy|\Psi_2\rangle|^2 = \frac{1}{4} \qquad \forall x, y \in \{0,1\}^2 \tag{21}$$

so every state is *equally probable* and independent from the quantum states she wants to send. This means that, even knowing the operations Alice is going to perform on her qubits, Bob has no clue about what could be the outcome of her measurement.

After Alice's measurement, we have 4 possible outcomes:

$$\begin{aligned}
A : |00\rangle &\longrightarrow B : \alpha|0\rangle + \beta|1\rangle \\
A : |01\rangle &\longrightarrow B : \alpha|1\rangle + \beta|0\rangle \\
A : |10\rangle &\longrightarrow B : \alpha|0\rangle - \beta|1\rangle \\
A : |11\rangle &\longrightarrow B : \alpha|1\rangle - \beta|0\rangle
\end{aligned}$$

Alice now communicates to Bob the outcome (x, y). From this piece of information, Bob knows which operation to perform on his qubit in order to retrieve the original $|\psi\rangle$ state:

$$\begin{aligned}
&\text{if}(0,0) \longrightarrow \text{Bob applies} \quad \mathbb{I} \\
&\text{if}(0,1) \longrightarrow \text{Bob applies} \quad X \\
&\text{if}(1,0) \longrightarrow \text{Bob applies} \quad Z \\
&\text{if}(1,1) \longrightarrow \text{Bob applies} \quad X \quad \text{and then} \quad Z
\end{aligned}$$

In this way, Bob has the certainty that his qubit will be in the state $|\psi\rangle$, i.e. the state in which Alice's qubit initially was.

4. In the whole process there was no teleportation of matter from Alice to Bob. They shared a pair of maximally entangled qubits and then there was only transmission of classical information.

5. The quantum state $|\psi\rangle$ was not cloned (it would be forbidden because of the no-cloning theorem). The quantum state $|\psi\rangle$ on Alice's side was destroyed by Alice's measurement process. Also, no information about the quantum state was obtained in the process (it would be forbidden by the theorem on the impossibility to know an arbitrary quantum state). The two facts are obviously related. If we could clone a state, then we could clone and measure different observables repeatedly, until we gather arbitrarily precise information about the quantum state (this process is called quantum state tomography). If we could know the quantum state $|\psi\rangle$, then we may conceive a specific quantum circuit to generate it starting from one state of the computational basis, therefore cloning the state.

6. Finally, there was no superluminal transmission of information, and the quantum teleportation protocol obeys the Relativity principle. This happens because all the outcomes of Alice's measure are equally probable, so she has to communicate the results classically to Bob, with signals that can't travel faster than the speed of light.