# Tutorial 5

## Problem 1: SWAP Test

Given the two-qubit SWAP gate:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and the two single-qubit states $|\phi_1\rangle = a\,|0\rangle + b\,|1\rangle$ and $|\phi_2\rangle = c\,|0\rangle + d\,|1\rangle$.

**a.** Show that $U_{\text{SWAP}}\,|\phi_1\rangle \otimes |\phi_2\rangle = |\phi_2\rangle \otimes |\phi_1\rangle$

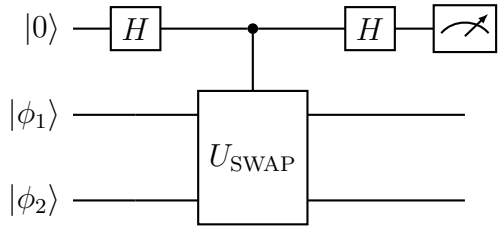
---

**Solution:** We have $|\phi_1\rangle \otimes |\phi_2\rangle = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle$. The action of the SWAP gate is to exchange $|10\rangle$ and $|01\rangle$, leading to

$$\begin{aligned} U_{\text{SWAP}}\,|\phi_1\rangle \otimes |\phi_1\rangle &= ac\,|00\rangle + bc\,|01\rangle + ad\,|10\rangle + bd\,|11\rangle && (1)\\ &= c\,|0\rangle \otimes (a\,|0\rangle + b\,|1\rangle) + d\,|1\rangle \otimes (a\,|0\rangle + b\,|1\rangle) && (2)\\ &= (c\,|0\rangle + d\,|0\rangle) \otimes (a\,|0\rangle + b\,|1\rangle) && (3)\\ &= |\phi_2\rangle \otimes |\phi_1\rangle && (4) \end{aligned}$$

---

**b.** Consider the following SWAP test circuit acting on the two states $|\phi_1\rangle$ and $|\phi_2\rangle$.




Give the quantum state of the three qubit system at each step of the circuit.

---

**Solution:** The input to the circuit reads $|\psi_0\rangle = |0\rangle \otimes |\phi_1\rangle \otimes |\phi_2\rangle$. After the first Hadamard gate, the state reads

$$\begin{aligned} |\psi_1\rangle &= H \otimes I \otimes I\,|0\rangle \otimes |\phi_1\rangle \otimes |\phi_2\rangle && (5)\\ &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\phi_1\rangle \otimes |\phi_2\rangle && (6) \end{aligned}$$

After the controlled SWAP, the state reads

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle \otimes |\phi_1\rangle \otimes |\phi_2\rangle + |1\rangle \otimes |\phi_2\rangle \otimes |\phi_1\rangle\right] \quad (7)$$

After the last Hadamard gate, the state reads

$$\begin{aligned}|\psi_3\rangle &= \frac{1}{2}\left[(|0\rangle+|1\rangle)\otimes|\phi_1\rangle\otimes|\phi_2\rangle+(|0\rangle-|1\rangle)\otimes|\phi_2\rangle\otimes|\phi_1\rangle\right]\\ &= |0\rangle\otimes\frac{1}{2}\left[|\phi_1\rangle\otimes|\phi_2\rangle+|\phi_2\rangle\otimes|\phi_1\rangle\right]+|1\rangle\otimes\frac{1}{2}\left[|\phi_1\rangle\otimes|\phi_2\rangle-|\phi_2\rangle\otimes|\phi_1\rangle\right]\end{aligned}$$

---

**c.** Compute the probability $P(0)$ of obtaining the outcome 0 at the top qubit, the probability $P(1)$ of obtaining the outcome 1, and their bias $P(0)-P(1)$.

---

**Solution:** The probability of outcome result correspond to $||\tilde{\Pi}_0|\psi_3\rangle||^2 = \langle\psi_3|\tilde{\Pi}_0|\psi_3\rangle$. It is easy to see that

$$\tilde{\Pi}_0|\psi_3\rangle = |0\rangle\otimes\frac{1}{2}\left[|\phi_1\rangle\otimes|\phi_2\rangle+|\phi_2\rangle\otimes|\phi_1\rangle\right]. \tag{8}$$

Then the probability of its outcome reads

$$\begin{aligned}\langle\psi_3|\tilde{\Pi}_0|\psi_3\rangle &= \frac{1}{4}\left[\langle\phi_1|\otimes\langle\phi_2|+\langle\phi_2|\otimes\langle\phi_1|\right]\left[|\phi_1\rangle\otimes|\phi_2\rangle+|\phi_2\rangle\otimes|\phi_1\rangle\right]\\ &= \frac{1}{4}+\frac{1}{4}\langle\phi_2|\phi_1\rangle\langle\phi_1|\phi_2\rangle+\frac{1}{4}\langle\phi_1|\phi_2\rangle\langle\phi_2|\phi_1\rangle+\frac{1}{4} &(9)\\ &= \frac{1}{2}+\frac{1}{2}\langle\phi_1|\phi_2\rangle\langle\phi_1|\phi_2\rangle^* &(10)\\ &= \frac{1}{2}+\frac{1}{2}|\langle\phi_2|\phi_1\rangle|^2 &(11)\end{aligned}$$

A similar calculation as above leads to:

$$P(1) = \frac{1}{2}-\frac{1}{2}|\langle\phi_2|\phi_1\rangle|^2. \tag{12}$$

Therefore, the bias of probabilities reads $P(0)-P(1) = |\langle\phi_2|\phi_1\rangle|^2$.

---

# Problem 2: Quantum Fourier Transform

As you have seen in the lectures, we can represent any integer $z$ in its binary form as:

$$z = z_1 z_2 \ldots z_n$$

where $z_1, z_2, \ldots, z_n$ are such so that:

$$z = z_1 2^{n-1} + \ldots + z_{n-1}2^1 + z_n$$

**a.** How many qubits at least would we need to encode the integer states $|14\rangle$ and $|9\rangle$? What is their binary representation when using qubits to encode the integers?

---

**Solution:** In order to represent an integer state $|N\rangle$, one would require at least $n = \lceil \log(N+1) \rceil$ qubits. This implies that for both cases we require 4 qubits. The binary representation of these four-qubit integer states is:

$$|14\rangle = |1110\rangle$$
$$|9\rangle = |1001\rangle$$

---

**b.** Recall that:

$$0.z_l z_{l+1} \dots z_m \equiv \frac{z_l}{2} + \frac{z_{l+1}}{2^2} + \cdots + \frac{z_m}{2^{m-l+1}}$$

Calculate:

1. $2^3 \cdot 0.z_1z_2z_3$, $2^2 \cdot 0.z_1z_2z_3$ and $2 \cdot 0.z_1z_2z_3$, where $z_i \in \{0,1\}$.
2. $e^{2\pi i \cdot 2^2 \cdot 0.j_1j_2j_3}$ where $j_i \in \{0,1\}$.

---

**Solution:** We start by writing down the expression for $0.z_1z_2z_3$:

$$0.z_1z_2z_3 = \frac{z_1}{2} + \frac{z_2}{4} + \frac{z_3}{8}$$

Then it is easy to calculate the expressions above. For the first case, we have:

$$2^3 \cdot 0.z_1z_2z_3 = 4z_1 + 2z_2 + z_3$$
$$2^2 \cdot 0.z_1z_2z_3 = 2z_1 + z_2 + \frac{z_3}{2}$$
$$2 \cdot 0.z_1z_2z_3 = z_1 + \frac{z_2}{2} + \frac{z_3}{4}$$

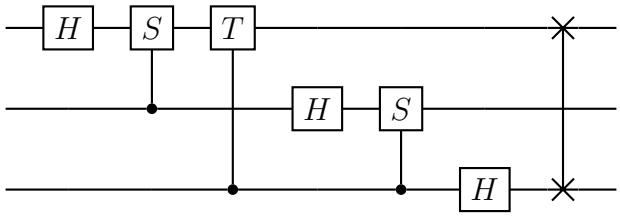
For the second case:

$$e^{2\pi i \cdot 2^2 \cdot 0.j_1j_2j_3} = e^{2\pi i(2j_1 + j_2 + j_3/2)} = e^{2\pi i(2j_1+j_2)} e^{2\pi i j_3/2} = e^{2\pi i 0.j_3},$$

where in the second equality we used the fact that $2j_1 + j_2$ is an integer and therefore $e^{2\pi i(2j_1+j_2)} = 1$.

---

**c.** Now consider the quantum Fourier circuit for three qubits:



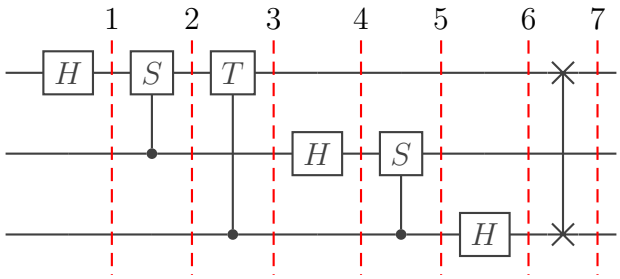

with $S$ and $T$ being the gates:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Suppose that we input the state $|j\rangle = |j_1 j_2 j_3\rangle$. What will be the output state?

---

**Solution:** We start as usual by dividing the quantum circuit into subsequent steps:




Initially, the system is in the state:

$$|\psi\rangle_0 = |j_1 j_2 j_3\rangle$$

Then we act with the Hadamard operator on the first qubit and use the fact that $e^{2\pi i 0.j_1}$ is $+1$ if $j_1 = 0$ and $-1$ if $j_1 = 1$. Thus the state at step 1 is transformed to:

$$|\psi\rangle_1 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2 j_3\rangle$$

Recall that the unitary operator $R_k$ is defined as:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

It's easy to see that both $S$ and $T$ are special cases of the operator $R_k$ for two different choices of $k$. $S$ corresponds to $R_2$ while $T$ corresponds to $R_3$.

On the next step, applying the $S$ operator on the first qubit controlled by the second qubits produces the state:

$$|\psi\rangle_2 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1} e^{2\pi i 0.0 j_2}|1\rangle)|j_2 j_3\rangle = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)|j_2 j_3\rangle$$

Next, we perform the controlled-$T$ operation and so we get:

$$|\psi\rangle_3 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2} e^{2\pi i 0.00 j_3}\,|1\rangle)\,|j_2 j_3\rangle = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}\,|1\rangle)\,|j_2 j_3\rangle$$

If we work with the exact same way for the rest of the steps we will get:

*Step 4:*

$$|\psi\rangle_4 = \frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}\,|1\rangle)(|0\rangle + e^{2\pi i 0.j_2})\,|j_3\rangle$$

*Step 5:*

$$|\psi\rangle_4 = \frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}\,|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3})\,|j_3\rangle$$

*Step 6:*

$$|\psi\rangle_4 = \frac{1}{2^{3/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}\,|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3})(|0\rangle + e^{2\pi i 0.j_3}\,|1\rangle)$$

At the final step, we swap the state of the first and third qubit and recover the *quantum Fourier transformation*:

$$|\psi\rangle_4 = \frac{1}{2^{3/2}}(|0\rangle + e^{2\pi i 0.j_3}\,|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3})(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}\,|1\rangle)$$

---

# Problem 3: Order-Finding

For two positive integers $x$ and $N$ with $x < N$ the *order* of $x$ modulo $N$ is defined to be the *least positive integer* such that:

$$x^r = 1 \mod N$$

**a.** Show that for $x = 2$ and $N = 5$ we have $r = 4$.

---

**Solution:** It's easy to see that for $r = 4$:

$$2^4 = 3 \times 5 + 1,$$

which implies $2^4 = 1 \mod 5$. Similarly, one can show that $2^3 = 3 \mod 5$ and $2^2 = 4 \mod 5$. Therefore, $r = 4$ is the least integer such that $2^4 = 1 \mod 5$.

**Note:** Remark that modular exponentiation is a periodic function of period $r$. You can check that for $x = 3$ we also obtain $r = 4$, but for $x = 4$ we have $r = 2$, the latest can be easily derived from the case of $x = 2$.

---

**b.** Now consider the transformation $U_x$ which acts on the computational basis states as follows:

$$U_x |y\rangle \equiv |xy \mod N\rangle$$

Prove that:

1. $U_x U_{x'} = U_{xx'}$
2. $U_{x^{-1}} = U_x^{-1} = U_x^\dagger$.
3. $U_x U_x^\dagger = U_x^\dagger U_x = I$, which proves it is an unitary transformation.
4. $U_x^r = I$ where $r$ is the period of $x$ modulo $N$.

---

**Solution:** We start with the first property, which result from the associativity of the multiplication of integer $\mod N$. We have:

$$U_x U_{x'} |y\rangle = U_x |x'y \mod N\rangle = |xx'y \mod N\rangle$$
$$U_{xx'} |y\rangle = |xx'y \mod N\rangle$$

and thus:

$$U_x U_{x'} = U_{xx'} = U_{x'} U_x$$

We continue with the second property:

$$U_{x^{-1}} U_x |y\rangle = U_{x^{-1}} |xy \mod N\rangle = |y\rangle$$

and thus:

$$U_{x^{-1}} = U_x^{-1}$$

Now for the second part of the second property:

$$\langle y| U_x^\dagger U_x |y\rangle = \langle yx \mod N | yx \mod N\rangle = 1$$

and thus $U_x^\dagger U_x = I$ and so the inverse of $U_x$ is $U_x^\dagger$, i.e.:

$$U_{x^{-1}} = U_x^{-1} = U_x^\dagger$$

The third property follows immediately from the previous property as $U_x U_x^\dagger = U_x U_x^{-1} = I = U_x^\dagger U_x$ and thus $U_x$ is a unitary operator.
Then for the final property we have:

$$\underbrace{U_x U_x \dots U_x}_{r} |y\rangle = |x^r y \mod N\rangle = |y\rangle$$

and so we proved that:

$$U_x^r = I$$

---

**c.** Show that the states:

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^k \mod N\rangle$$

for integer $0 \leq s \leq r-1$ are eigenstates of $U_x$. What is their corresponding eigenvalues?

---

**Solution:** If we act with $U_x$ on the states $|u_s\rangle$ we get:

$$U_x |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} U_x |x^k \mod N\rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^{k+1} \mod N\rangle = \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} e^{-\frac{2\pi i s (k'-1)}{r}} |x^{k'} \mod N\rangle$$

where in the last step we switched the variable $k$ with the variable $k' = k+1$. If we continue with the calculation we have:

$$U_x |u_s\rangle = e^{2\pi i s/r} \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} e^{-\frac{2\pi i s k'}{r}} |x^{k'} \mod N\rangle$$

But recall that $r$ is the order of $x$ modulo $N$ and so $x^r = 1 \mod N$. It's easy to see then that the sum in the expression can be replaced to:

$$\sum_{k'=1}^{r} \to \sum_{k=0}^{r-1},$$

as it correspond only to a reordering of the same sum (a shift to the left of a closed cycle). Thus, we can conclude that $|u_s\rangle$ is an eigenstate of the operator $U_x$ with eigenvalue $e^{2\pi i s/r}$:

$$U_x |u_s\rangle = e^{2\pi i s/r} |u_s\rangle$$

---

**d.** As you can see preparing the state $|u_s\rangle$ requires that we know $r$ in advance. Fortunately there is clever observation which circumvents the problems of preparing $|u_s\rangle$. Show that:

1.
$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = r\delta_{k,0}$$

2.
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle = |x^k \mod N\rangle$$

which has as special case when $k = 0$:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle ,$$

which is a trivial state to generate. This opens the door to applying quantum phase-estimation to sample from $\varphi = s/r$, which later leads to a guess of $r$ as explained in the lecture on Shor's algorithm.

---

**Solution:** Consider the first expression and let $k = 0$. It's easy to see that we have a sum of $r$ terms, all equal to the identity and thus:

$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = r \text{ if } k = 0$$

Now consider $k \neq 0$. The sum then corresponds to a geometric series which is equal to:

$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = \frac{1 - e^{-2\pi ik}}{1 - e^{-2\pi ik/r}} = 0$$

for every $k \in \mathbb{Z}$ with $k \neq 0$. Thus we can conclude that:

$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = r\delta_{k,0}$$

For the second expression we have:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left[ e^{2\pi isk/r} \frac{1}{\sqrt{r}} \sum_{k'=0}^{r-1} e^{-\frac{2\pi isk'}{r}} |x^{k'} \mod N\rangle \right]$$
$$= \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k'=0}^{r-1} e^{2\pi is(k-k')/r} |x^k \mod N\rangle = \frac{1}{r} \sum_{k'=0}^{r-1} r\delta_{0,k-k'} |x^{k'} \mod N\rangle$$

where in the last equality we used the result from expression 1. It's trivial to see that $\delta_{0,k-k'} = \delta_{k,k'}$ and the sum over $k'$ contributes only when $k' = k$. Thus:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k/r} |u_s\rangle = |x^k \mod N\rangle .$$

The case $k = 1$ is only a corollary of this last result, leading to the input state $|1\rangle$ used in the order finding algorithm.

---

**e.** If we wanted to apply a phase estimation procedure we must have efficient procedures to implement a controlled-$U^{2^j}$ operation for any integer $j$. Given an integer number $x$, propose a technique to compute $x^{2^k}$ that scales linearly in $k$.

---

**Solution:** if we want to compute $x^{2^k}$ an inefficient approach is to multiply $2^k$ times $x$. A more efficient approach is to square iteratively, i.e., we apply the function $y^2 \mod N$ $k$ times to the input $x$. It is easy to see then that we get the series $x^2$, $x^4$, $x^{2^3}$,..., $x^{2^k}$. Because the multiplication is $\mod N$, the memory register does not need to increase, as it will never be larger than $N$.

---

**f.** Assuming that we are given an unitary $S$ such that implements $S|x\rangle = |x^2 \mod N\rangle$ that needs $O(L^2)$ gates, where $L = \lceil \log N \rceil$, i.e., the size of the register. How many gates we will be needed to implement $|x\rangle \to |x^{2^k} \mod N\rangle$?

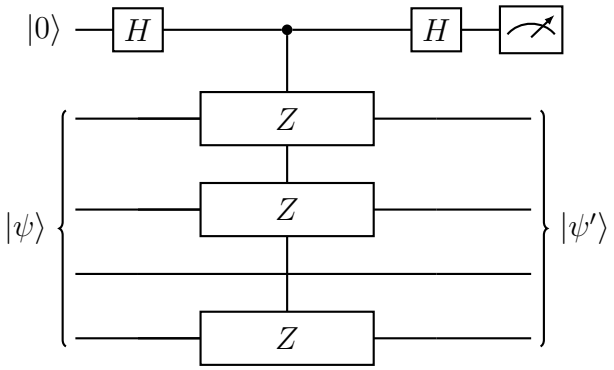
---

**Solution:** We are given that the unitary $S$ is such that implements $S|x\rangle = |x^2 \mod N\rangle$ using $O(L^2)$ gates. Clearly if we want to implement $|x\rangle \to |x^{2^k} \mod N\rangle$ we need to apply $S$ $k$ times, which lead to an asymptotic scaling $O(kL^2)$ of number of gates. Because in phase estimation we need to implement up to $U^{2^k}$ where $k \in \{0, 2L+1\}$, it is easy to see that need $O(L^3)$ gates.

---

# Extra problem: Three-Qubit Parity Check

We want to perform an even/odd parity check on qubits $1, 2, 4$. It's easy to see that the parity operator $P = Z \otimes Z \otimes I \otimes Z$ is both Hermitian and Unitary, so that it can both be regarded as an observable and a quantum gate. Suppose we wish to measure the observable $P$. That is, we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving an updated state after the measurement that is projected to its corresponding eigenspace. We are going to show that the following circuit implements a measurement of $P$:




**a.** Derive the action of the three-qubit parity operator $P = Z \otimes Z \otimes I \otimes Z$ on the computational basis state $|x_1 x_2 x_3 x_4\rangle$. What are the eigenvalues of the operator $P$?

---

**Solution:** Recall that the state $|x_1 x_2 x_3 x_4\rangle$ corresponds to the tensor product:

$$|x_1 x_2 x_3 x_4\rangle \equiv |x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes |x_4\rangle$$

We can use the property:

$$\begin{gathered} P\,|x_1 x_2 x_3 x_4\rangle = (Z \otimes Z \otimes I \otimes Z)\,(|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes |x_4\rangle) \\ = Z\,|x_1\rangle \otimes Z\,|x_2\rangle \otimes I\,|x_3\rangle \otimes Z\,|x_4\rangle = (-1)^{x_1}\,|x_1\rangle \otimes (-1)^{x_2}\,|x_2\rangle \otimes |x_3\rangle \otimes (-1)^{x_4}\,|x_4\rangle \\ \implies P\,|x_1 x_2 x_3 x_4\rangle = (-1)^{x_1+x_2+x_4}\,|x_1 x_2 x_3 x_4\rangle \end{gathered}$$

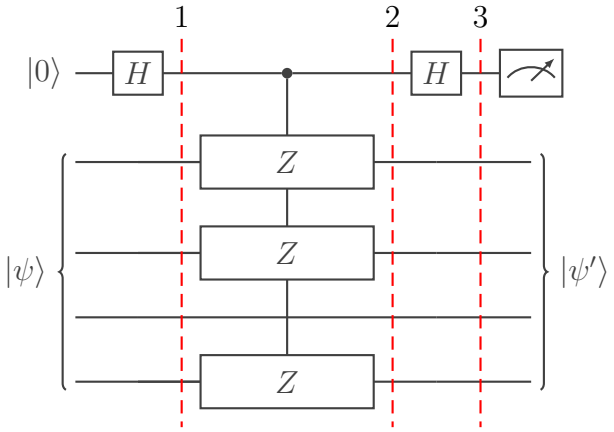
We can see that when $P$ acts on a computational basis, it is scaled by a factor of $-1$ or $+1$ depending on the bits $x_i$. This means that the computational basis states are the eigenvectors of $P$ with eigenvalues $\pm 1$.

---

**b.** Derive the global state right before the measurement of the upper-qubit when the input state reads $|0\rangle \otimes |\psi\rangle$, where $|\psi\rangle = \sum_{x \in \{0,1\}^4} \gamma_x |x\rangle$ is a four qubit arbitrary input state and $x$ is a four bit string.

---

**Solution:** First of all, we are going to divide the quantum circuits into subsequent steps and calculate the composite state in each one of them.




The initial state of the composite system of 5 qubits is:

$$|\psi\rangle_0 = |0\rangle \otimes |\psi\rangle = \sum_{x\in\{0,1\}^4} \gamma_x |0\rangle |x\rangle$$

*Step 1:* On the first step, we act with the Hadamard operator on the first qubit and get:

$$(H\otimes I)|\psi\rangle_0 = \sum_{x\in\{0,1\}^4} \gamma_x H|0\rangle|x\rangle = \sum_{x\in\{0,1\}^4} \gamma_x \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|x\rangle$$
$$\sum_{x\in\{0,1\}^4} \frac{\gamma_x}{\sqrt{2}}|0\rangle|x\rangle + \sum_{x\in\{0,1\}^4} \frac{\gamma_x}{\sqrt{2}}|1\rangle|x\rangle$$

and so the state $|\psi\rangle_1$ at step 1 is:

$$|\psi\rangle_1 = \sum_{x\in\{0,1\}^4} \frac{\gamma_x}{\sqrt{2}}|0\rangle|x\rangle + \sum_{x\in\{0,1\}^4} \frac{\gamma_x}{\sqrt{2}}|1\rangle|x\rangle$$

*Step 2:* On the second step, we act with the controlled-$P$ operator and get:

$$CP|\psi\rangle_1 = \sum_{x\in\{0,1\}^4} \frac{\gamma_x}{\sqrt{2}}|0\rangle|x\rangle + \sum_{x\in\{0,1\}^4} \frac{\gamma_x}{\sqrt{2}}|1\rangle P|x\rangle$$

Note that $x$ is the bitstring $x_1x_2x_3x_4$. Thus, by using the answer of question (a.) we get that the state $|\psi\rangle_2$ at step 2 is:

$$|\psi\rangle_2 = \sum_{x\in\{0,1\}^4} \frac{\gamma_x}{\sqrt{2}}|0\rangle|x\rangle + \sum_{x\in\{0,1\}^4} \frac{\gamma_x}{\sqrt{2}}|1\rangle(-1)^{x_1+x_2+x_4}|x\rangle$$
$$= \sum_{x_1+x_2+x_4=even} \gamma_x|+\rangle|x\rangle + \sum_{x_1+x_2+x_4=odd} \gamma_x|-\rangle|x\rangle$$

*Step 3:* On the third step, we act again with the Hadamard operator on the first qubit and get:

$$|\psi\rangle_3 = \sum_{x_1+x_2+x_4=even} \gamma_x |0\rangle |x\rangle + \sum_{x_1+x_2+x_4=odd} \gamma_x |1\rangle |x\rangle$$

$$|\psi\rangle_3 = |0\rangle \otimes \left( \sum_{x_1+x_2+x_4=even} \gamma_x |x\rangle \right) + |1\rangle \otimes \left( \sum_{x_1+x_2+x_4=odd} \gamma_x |x\rangle \right)$$

---

**c.** Using the rules of partial measurement, show that the measurement of the upper-qubit projects the state of the lower four qubits to its odd or even parity subspaces, depending on the outcome being 0 or 1.

---

**Solution:** The partial measurement of the first qubit can be described as the linear operator $P_i \otimes I = |i\rangle\langle i| \otimes I$ with $i \in \{0, 1\}$. If we perform the measurement on the first qubit and find it in the $|0\rangle$ state, then the system after the measurement will be in the state:

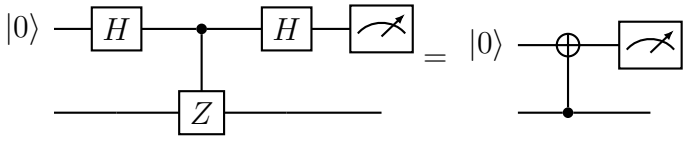
$$|\psi\rangle = \frac{P_0 \otimes I |\psi\rangle_3}{||P_0 \otimes I |\psi\rangle_3||} = |0\rangle \otimes \frac{1}{(\sum_{x_1+x_2+x_4=even} |\gamma_x|^2)^{1/2}} \left( \sum_{x_1+x_2+x_4=even} \gamma_x |x\rangle \right)$$

On the other hand, if we measure it to be in the state $|1\rangle$ then the state of the system after the measurement will be:

$$|\psi\rangle = \frac{P_1 \otimes I |\psi\rangle_3}{||P_1 \otimes I |\psi\rangle_3||} = |1\rangle \otimes \frac{1}{(\sum_{x_1+x_2+x_4=odd} |\gamma_x|^2)^{1/2}} \left( \sum_{x_1+x_2+x_4=odd} \gamma_x |x\rangle \right)$$

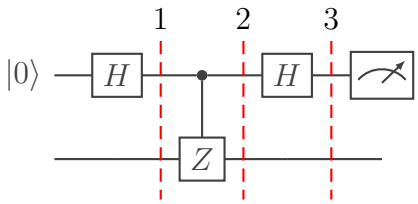
---

**d.** Prove that the two circuits below are equivalent:




---

**Solution:** Consider the second qubit to be in the general state $|\psi\rangle = a|0\rangle + b|1\rangle$. We split the first circuit into three parts.



The initial state of the composite system is:

$$|\psi\rangle_0 = a\,|00\rangle + b\,|01\rangle$$

*Step 1:*

$$|\psi\rangle_1 = (H \otimes I)\,|\psi\rangle_0 = \frac{a}{\sqrt{2}}(|00\rangle + |10\rangle) + \frac{b}{\sqrt{2}}(|01\rangle + |11\rangle)$$

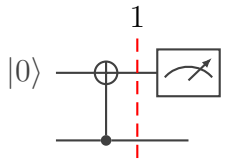
*Step 2:*

$$\begin{aligned}|\psi\rangle_2 = CZ\,|\psi\rangle_1 &= \frac{a}{\sqrt{2}}(|00\rangle + |10\rangle) + \frac{b}{\sqrt{2}}(|01\rangle - |11\rangle) \\ &= a\,|+\rangle\,|0\rangle + b\,|-\rangle\,|1\rangle\end{aligned}$$

*Step 3:*

$$|\psi\rangle_3 = (H \otimes I)\,|\psi\rangle_2 = a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|1\rangle$$

We consider again the same input on the second circuit:




We can see that if we start with the same input:

$$|\psi\rangle_0 = a\,|00\rangle + b\,|01\rangle$$

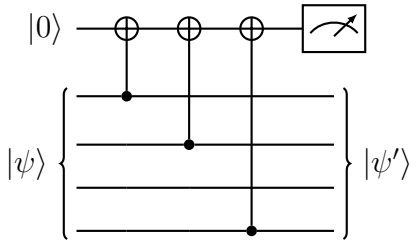
then after the action of the controlled-NOT with the control being the second qubit we have:

$$|\psi\rangle_1 = a\,|00\rangle + b\,|11\rangle$$

We can thus conclude that the two circuits are equivalent.

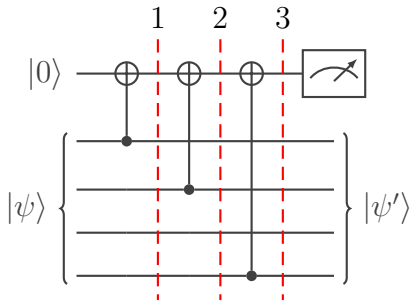
---

**e.** Prove that we can achieve the same result with the circuit:



---

**Solution:** In the same manner, we break the circuit into subsequent steps:




The initial state of the system is:

$$|\psi\rangle_0 = |0\rangle \otimes |\psi\rangle = \sum_{x\in\{0,1\}^4} \gamma_x |0\rangle |x\rangle$$

*Step 1:*

$$|\psi\rangle_1 = \sum_{x\in\{0,1\}^4} \gamma_x |0 \oplus x_1\rangle |x\rangle$$

*Step 2:*

$$|\psi\rangle_2 = \sum_{x\in\{0,1\}^4} \gamma_x |0 \oplus x_1 \oplus x_2\rangle |x\rangle$$

*Step 3:*

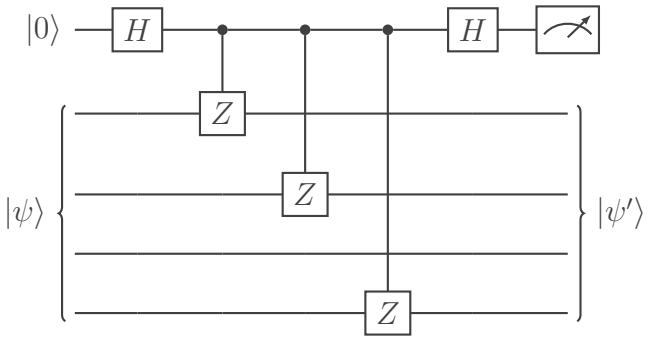
$$|\psi\rangle_3 = \sum_{x\in\{0,1\}^4} \gamma_x |0 \oplus x_1 \oplus x_2 \oplus x_4\rangle |x\rangle$$

$$\implies |\psi\rangle_3 = |0\rangle \otimes \left( \sum_{x_1+x_2+x_4=even} \gamma_x |x\rangle \right) + |1\rangle \otimes \left( \sum_{x_1+x_2+x_4=odd} \gamma_x |x\rangle \right)$$

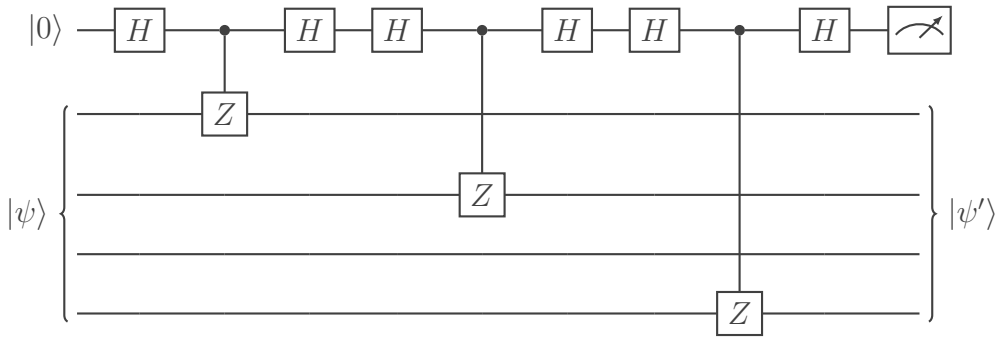
We can see that in both cases the output state is the same. We can thus conclude that the two circuits are equivalent.

**Alternative solution:**

We can rewrite the original circuit by splitting the controlled-multi-Z gate into individual gates (as they are independent of each other, and have the same control qubit):




Now we can insert double Hadamard gates in between controlled-Z gates, as they are equivalent to identity:




Using the results from **d**, this is equivalent to: