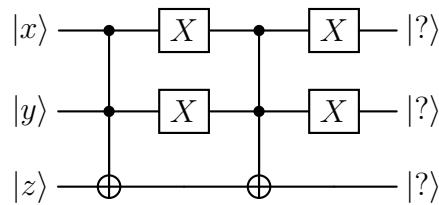


Please pay attention to the presentation of your answers! (2 points)

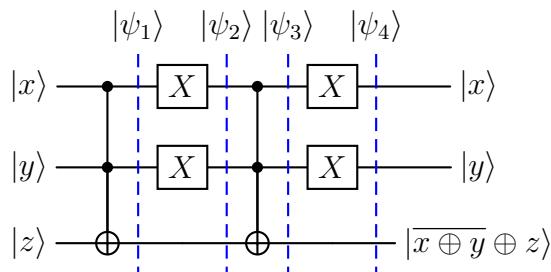
Exercise 1 Outputs of quantum circuits (12 points)

a) Consider the following 3-qubit quantum circuit U :



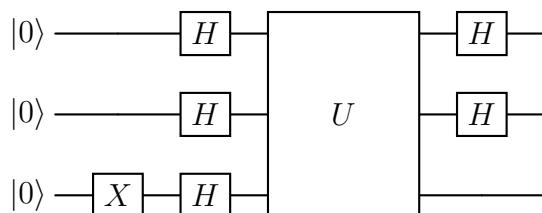
What is the output of the circuit U when the input is an element $|x, y, z\rangle$ of the computational basis?

Solution:



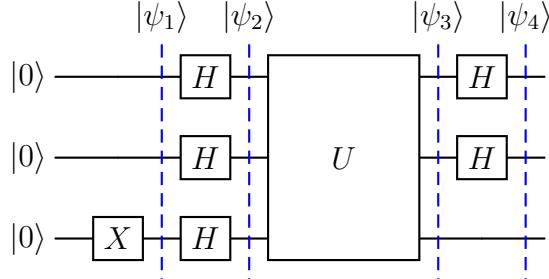
The states at different points in the circuit are $|\psi_1\rangle = |x, y, xy \oplus z\rangle$, $|\psi_2\rangle = |\bar{x}, \bar{y}, xy \oplus z\rangle$, $|\psi_3\rangle = |\bar{x}, \bar{y}, \bar{xy} \oplus xy \oplus z\rangle$ and $|\psi_4\rangle = |x, y, \bar{xy} \oplus xy \oplus z\rangle = |x, y, \bar{x \oplus y} \oplus z\rangle$.

b) Consider now the following circuit:



What is/are the possible output(s) of the first 2 qubits of the circuit (i.e., the ones following the gates H) and their corresponding probabilities?

Solution:



We have $|\psi_1\rangle = |001\rangle$. The subsequent states can be computed as follows:

$$\begin{aligned}
 |\psi_2\rangle &= H^{\otimes 3} |\psi_1\rangle = \left(\frac{1}{2} \sum_{x,y \in \{0,1\}} |x,y\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{2^{3/2}} \sum_{x,y \in \{0,1\}} |x,y\rangle \otimes |0\rangle - |x,y\rangle \otimes |1\rangle \\
 |\psi_3\rangle &= U |\psi_2\rangle = \frac{1}{2^{3/2}} \sum_{x,y \in \{0,1\}} U |x,y\rangle \otimes |0\rangle - U |x,y\rangle \otimes |1\rangle \\
 &= \frac{1}{2^{3/2}} \sum_{x,y \in \{0,1\}} |x,y\rangle \otimes |\overline{x \oplus y}\rangle - |x,y\rangle \otimes |x \oplus y\rangle = \frac{1}{2} \sum_{x,y \in \{0,1\}} (-1)^{\overline{x \oplus y}} |x,y\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
 \end{aligned}$$

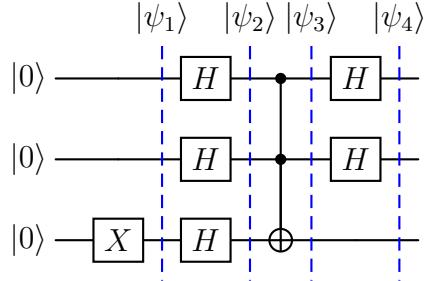
and finally:

$$\begin{aligned}
 |\psi_4\rangle &= (H^{\otimes 2} \otimes I) |\psi_3\rangle = \frac{1}{2} \sum_{x,y \in \{0,1\}} (-1)^{\overline{x \oplus y}} H^{\otimes 2} |x,y\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
 &= \frac{1}{2} \sum_{x,y \in \{0,1\}} (-1)^{\overline{x \oplus y}} \left(\frac{1}{2} \sum_{u,v \in \{0,1\}} (-1)^{ux \oplus vy} |u,v\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
 &= \left(\frac{1}{4} \sum_{x,y,u,v \in \{0,1\}} (-1)^{\overline{x \oplus y} \oplus ux \oplus vy} |u,v\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
 &= \left(-\frac{1}{4} \sum_{x,y,u,v \in \{0,1\}} (-1)^{x \oplus y \oplus ux \oplus vy} |u,v\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
 &= \left(-\frac{1}{4} \sum_{x,y,u,v \in \{0,1\}} (-1)^{\bar{u}x \oplus \bar{v}y} |u,v\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
 \end{aligned}$$

We see that the probability of $|\psi_4\rangle = |1,1\rangle$ equals 1. Therefore the only possible output state is $|1,1\rangle$.

c) How would these output probabilities be modified if the circuit U were replaced by a single Toffoli gate?

Solution:



The states $|\psi_1\rangle$ and $|\psi_2\rangle$ remain the same as in part (b). The subsequent states can be computed as follows:

$$\begin{aligned}
 |\psi_3\rangle &= \text{CCNOT } |\psi_2\rangle = \frac{1}{2^{3/2}} \sum_{x,y \in \{0,1\}} \text{CCNOT } |x,y\rangle \otimes |0\rangle - \text{CCNOT } |x,y\rangle \otimes |1\rangle \\
 &= \frac{1}{2^{3/2}} \sum_{x,y \in \{0,1\}} |x,y\rangle \otimes |xy\rangle - |x,y\rangle \otimes |\overline{xy}\rangle = \frac{1}{2} \sum_{x,y \in \{0,1\}} (-1)^{xy} |x,y\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
 \end{aligned}$$

and

$$\begin{aligned}
 |\psi_4\rangle &= (H^{\otimes 2} \otimes I) |\psi_3\rangle = \frac{1}{2} \sum_{x,y \in \{0,1\}} (-1)^{xy} H^{\otimes 2} |x,y\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 &= \frac{1}{2} \sum_{x,y \in \{0,1\}} (-1)^{xy} \left(\frac{1}{2} \sum_{u,v \in \{0,1\}} (-1)^{ux \oplus vy} |u,v\rangle \right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 &= \left(\frac{1}{4} \sum_{x,y,u,v \in \{0,1\}} (-1)^{xy \oplus ux \oplus vy} |u,v\rangle \right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
 \end{aligned}$$

We can compute the probabilities as $\mathbb{P}(|00\rangle) = \frac{1}{4}$, $\mathbb{P}(|01\rangle) = \frac{1}{4}$, $\mathbb{P}(|10\rangle) = \frac{1}{4}$, and $\mathbb{P}(|11\rangle) = \frac{1}{4}$.

Exercise 2 *True or false? (16 points)*

For each question, 1 pt for the correct answer, 3 pts for the justification. If you think the statement is correct, then prove it; otherwise, provide a counter-example.

a) Let $|\varphi\rangle$ be a single qubit state and $|\varphi\rangle \otimes |\varphi\rangle$ be the (product) state of two qubits. A measurement in the computational basis is performed on the two qubits. Then the probability of observing the two qubits in the same state is necessarily greater than or equal to the probability of observing them in different states.

Solution: True. Let $|\varphi\rangle = a|0\rangle + b|1\rangle$. Then $|\varphi\rangle \otimes |\varphi\rangle = a^2|00\rangle + ab|01\rangle + ba|10\rangle + b^2|11\rangle$, so

$$\mathbb{P}(|00\rangle \text{ or } |11\rangle) = |a|^4 + |b|^4 \stackrel{(a)}{\geq} 2|a|^2|b|^2 = \mathbb{P}(|01\rangle \text{ or } |10\rangle)$$

where (a) follows from the inequality $(|a|^2 - |b|^2)^2 \geq 0$.

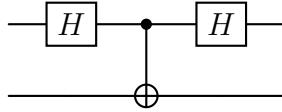
b) Classically, the output of a XOR gate is always equal to 0 if its two inputs are identical. It is also the case that the output target qubit of a CNOT gate is always $|0\rangle$ if its two input qubits are in a product state $|\varphi\rangle \otimes |\varphi\rangle$.

Solution: False. Consider $|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We have

$$\text{CNOT } (|\varphi\rangle \otimes |\varphi\rangle) = \text{CNOT } \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |11\rangle + |10\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

In this case, the target qubit is $|1\rangle$ with probability $\frac{1}{2}$ if measured.

c) If the input to the following circuit:



is in an entangled state, then so is its output.

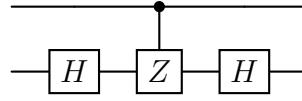
Solution: False. Let us compute the unitary matrix U corresponding to the circuit. We have

$$\begin{aligned} U &= (H \otimes I) \text{CNOT} (H \otimes I) \\ &= \frac{1}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix} \end{aligned}$$

Since U is unitary, an input state corresponding to any of the rows of U will lead to an element in the computational basis. We can verify that a states corresponding to the rows of U are entangled. For example, the first row of U leads to the state $|\psi\rangle = \frac{1}{2}(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle)$ with $(a, b, c, d) = (1, 1, 1, -1)$. However, $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$. Hence $|\psi\rangle$ is an entangled state that gives the output state $|00\rangle$ which is a product state.

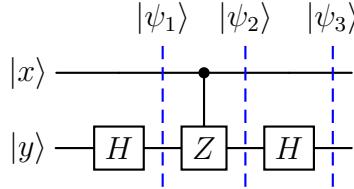
Another simpler solution is the following: as all the considered gates are their own inverses ($H^\dagger = H$ and $\text{CNOT}^\dagger = \text{CNOT}$), one can show that the proposition is false by showing that for an input product state $|00\rangle$, the output is entangled.

d) The following circuit:



is equivalent to a CNOT gate.

Solution: True.



For an input state $|x, y\rangle$ in the computational basis, we can compute the output of the circuit as follows:

$$\begin{aligned} |\psi_1\rangle &= (I \otimes H) |x, y\rangle = \frac{1}{\sqrt{2}} (|x, 0\rangle + (-1)^y |x, 1\rangle) \\ |\psi_2\rangle &= CZ |\psi_1\rangle = \frac{1}{\sqrt{2}} (CZ |x, 0\rangle + (-1)^y CZ |x, 1\rangle) \\ &= \frac{1}{\sqrt{2}} (|x, 0\rangle + (-1)^{x \oplus y} |x, 1\rangle) = |x\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x \oplus y} |1\rangle) \end{aligned}$$

and

$$\begin{aligned} |\psi_3\rangle &= (I \otimes H) |\psi_2\rangle = |x\rangle \otimes \frac{1}{\sqrt{2}} (H|0\rangle + (-1)^{x \oplus y} H|1\rangle) \\ &= |x\rangle \otimes \frac{1}{2} ((1 + (-1)^{x \oplus y}) |0\rangle + (1 - (-1)^{x \oplus y}) |1\rangle) = |x, x \oplus y\rangle \end{aligned}$$

Another simpler solution is the following: let $|x, y\rangle$ be the input (basis) state:

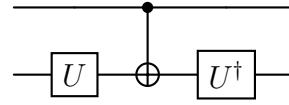
- if $x = 0$, then the controlled Z gate is inactive, and two H gates cancel, so the output is $|0, y\rangle$
- if $x = 1$, then the controlled Z gate is active, so the second qubit $|y\rangle$ goes through the gates HZH which are equivalent to an X gate, so the output is $|1, \bar{y}\rangle$ in this case.

Therefore the above circuit is equivalent to a CNOT gate.

Exercise 3 *Matrix representation (5 points)*

Let $U = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & \sqrt{2} \\ -\sqrt{2} & 1 \end{pmatrix}$ be the matrix representation of the 1-qubit gate U .

What is the matrix representation of the following 2-qubit gate? (in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$)



Solution: The matrix representation V of the circuit can be written as:

$$V = (I \otimes U^\dagger) CNOT (I \otimes U) = \begin{pmatrix} U^\dagger & 0 \\ 0 & U^\dagger \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & U \end{pmatrix} = \begin{pmatrix} U^\dagger U & 0 \\ 0 & U^\dagger X U \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & U^\dagger X U \end{pmatrix}$$

and

$$U^\dagger X U = \frac{1}{3} \begin{pmatrix} 1 & -\sqrt{2} \\ \sqrt{2} & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \sqrt{2} \\ -\sqrt{2} & 1 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} -\sqrt{2} & 1 \\ 1 & \sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & \sqrt{2} \\ -\sqrt{2} & 1 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} -2\sqrt{2} & -1 \\ -1 & 2\sqrt{2} \end{pmatrix}$$

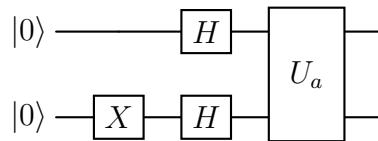
Hence,

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -2\sqrt{2}/3 & -1/3 \\ 0 & 0 & -1/3 & 2\sqrt{2}/3 \end{pmatrix}$$

Exercise 4 *Communication with quantum bits (15 points)*

Consider the following problem: Alice is in possession of a 2-bit vector $a = (a_0, a_1) \in \{0, 1\}^2$ and Bob is in possession of another 2-bit vector $b = (b_0, b_1) \in \{0, 1\}^2$. They would like to exchange information about the vectors a and b .

To this end, Alice builds the following 2-qubit circuit:



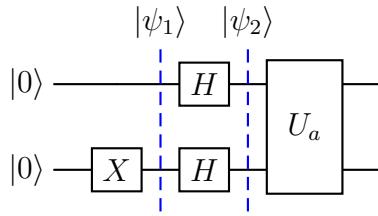
where the action of the gate U_a on a basis state $|x\rangle \otimes |y\rangle$ is described as:

$$U_a (|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus a_x\rangle$$

Alice then sends the 2-qubit output state $|\psi\rangle$ of the above circuit to Bob.

a) Compute the state $|\psi\rangle$.

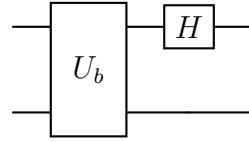
Solution:



The states can be computed successively as follows:

$$\begin{aligned}
 |\psi_1\rangle &= |01\rangle, \\
 |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 |\psi\rangle &= U_a |\psi_2\rangle = \frac{1}{2}(|0, a_0\rangle - |0, \bar{a}_0\rangle + |1, a_1\rangle - |1, \bar{a}_1\rangle) \\
 &= \frac{1}{2}\left((-1)^{a_0} |0\rangle \otimes (|0\rangle - |1\rangle) + (-1)^{a_1} |1\rangle \otimes (|0\rangle - |1\rangle)\right) \\
 &= \frac{1}{\sqrt{2}}\left((-1)^{a_0} |0\rangle + (-1)^{a_1} |1\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
 \end{aligned}$$

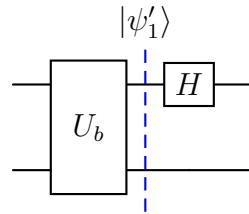
Bob then uses the state $|\psi\rangle$ as input to the following circuit:



where the action of the gate U_b is similar to the action of the gate U_a described above.

b) Compute the 2-qubit output state $|\psi'\rangle$ of the above circuit.

Solution:



We can compute the states $|\psi'_1\rangle$ and $|\psi'\rangle$ as follows:

$$\begin{aligned}
|\psi'_1\rangle &= U_b |\psi\rangle = \frac{1}{2}((-1)^{a_0}(U_b|00\rangle - U_b|01\rangle) + (-1)^{a_1}(U_b|10\rangle - U_b|11\rangle)) \\
&= \frac{1}{2}((-1)^{a_0}(|0, b_0\rangle - |0, \bar{b}_0\rangle) + (-1)^{a_1}(|1, b_1\rangle - |1, \bar{b}_1\rangle)) \\
&= \frac{1}{2}((-1)^{a_0 \oplus b_0} |0\rangle \otimes (|0\rangle - |1\rangle) + (-1)^{a_1 \oplus b_1} |1\rangle \otimes (|0\rangle - |1\rangle)) \\
&= \frac{1}{\sqrt{2}}((-1)^{a_0 \oplus b_0} |0\rangle + (-1)^{a_1 \oplus b_1} |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}$$

and

$$\begin{aligned}
|\psi'\rangle &= (H \otimes I) |\psi'_1\rangle = \frac{1}{\sqrt{2}}((-1)^{a_0 \oplus b_0} H|0\rangle + (-1)^{a_1 \oplus b_1} H|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= \frac{1}{2}(\{(-1)^{a_0 \oplus b_0} + (-1)^{a_1 \oplus b_1}\}|0\rangle + \{(-1)^{a_0 \oplus b_0} - (-1)^{a_1 \oplus b_1}\}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}$$

Bob then measures the first qubit (that is, the top qubit) of the output state $|\psi'\rangle$.

c1) What can he deduce on the relation between the 2-bit vectors a and b if the measured state is $|0\rangle$?

Solution: If the measured state is $|0\rangle$, then we have either $a_0 = b_0, a_1 = b_1$ or $a_0 = \bar{b}_0, a_1 = \bar{b}_1$. So, either a and b are equal or they are complements of each other.

c2) And likewise, what can he deduce on the relation between a and b if the measured state is $|1\rangle$?

Solution: In this case, we deduce that $a_0 = b_0, a_1 \neq b_1$ or $a_0 \neq b_0, a_1 = b_1$. Therefore, only one of the bits of a and b are equal.