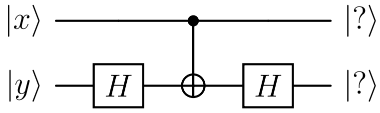
Final exam 2024: Solutions
Quantum Computation

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

Exercise 1 *Analysis of a quantum circuit (14 points)*

Consider the following quantum circuit:



a) Compute the output of the circuit when the input is an element $|x\rangle \otimes |y\rangle$ of the computational basis in $(\mathbb{C}^2)^2$.

Answer: Let us compute the output first for $x = 0$ (this can also be computed more straightforwardly by observing that the CNOT gate does not act in this case and that the two H gates cancel each other):

$$(I \otimes H)\,\mathrm{CNOT}\,(I \otimes H)\,(|0\rangle \otimes |y\rangle) = (I \otimes H)\,\mathrm{CNOT}\left(|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + (-1)^y\,|1\rangle)\right)$$
$$= (I \otimes H)\left(|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + (-1)^y\,|1\rangle)\right) = |0\rangle \otimes \frac{1}{2}(|0\rangle + |1\rangle + (-1)^y(|0\rangle - |1\rangle))$$
$$= |0\rangle \otimes |y\rangle$$

and then for $x = 1$:

$$(I \otimes H)\,\mathrm{CNOT}\,(I \otimes H)\,(|0\rangle \otimes |y\rangle) = (I \otimes H)\,\mathrm{CNOT}\left(|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + (-1)^y\,|1\rangle)\right)$$
$$= (I \otimes H)\left(|1\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle + (-1)^y\,|0\rangle)\right) = |1\rangle \otimes \frac{1}{2}(|0\rangle - |1\rangle + (-1)^y(|0\rangle + |1\rangle))$$
$$= (-1)^y\,|1\rangle \otimes |y\rangle$$

So overall, the output is $(-1)^{xy}\,|x\rangle \otimes |y\rangle$.

b) Assume now the input is in a product state $|\varphi\rangle \otimes |\psi\rangle$, where $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$ and $|\psi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$ with $|\gamma|^2 + |\delta|^2 = 1$. Under what condition(s) on $\alpha, \beta, \gamma, \delta$ is the output of the circuit also in a product state?

Answer: Using part a), let us compute the output:

$$(I \otimes H)\,\text{CNOT}\,(I \otimes H)\,(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) = \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle - \beta\delta\,|11\rangle$$

As

$$\det \begin{pmatrix} \alpha\gamma & \alpha\delta \\ \beta\gamma & -\beta\delta \end{pmatrix} = -\alpha\gamma\beta\delta - \beta\gamma\alpha\delta = -2\alpha\beta\gamma\delta$$

we conclude that the output is in a product state if and only if (at least) one of the coefficients α, β, γ or $\delta = 0$.

c) And if now the input is in an entangled state, is there a possibility that the output is in a product state? If yes, provide an example; if no, explain why this is impossible.

Answer: Yes, it is possible: assume the input state is $\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$ with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$ and

$$\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \alpha\delta - \beta\gamma \neq 0$$

then the output state is

$$\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle - \delta\,|11\rangle$$

and

$$\det \begin{pmatrix} \alpha & \beta \\ -\gamma & -\delta \end{pmatrix} = -\alpha\delta - \beta\gamma$$

which might be equal to 0, even when $\alpha\delta \neq \beta\gamma$. Consider for exemple the case $\alpha = \beta = \gamma = \frac{1}{2} = -\delta$. In this case, the input is in the entangled state

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right)$$

but the output is in the product state

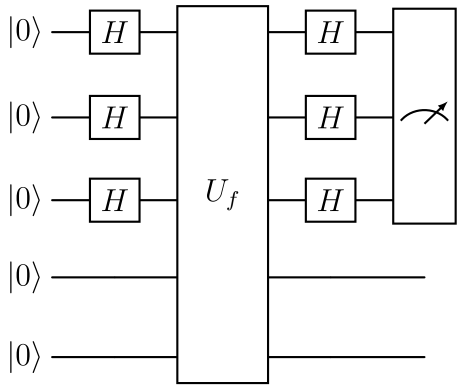
$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) = |+\rangle \otimes |+\rangle$$

Exercise 2 *Period of a function (18 points)*

Let us consider the following circuit: where the 5-qubit gate U_f is the oracle corresponding to the function $f : \{0,1\}^3 \to \{0,1\}^2$ defined as

$$f(x,y,z) = (x \oplus y, y \oplus z) \quad \text{for} \quad (x,y,z) \in \{0,1\}^3$$

a) Compute explicitly the 5-qubit output $|\psi\rangle$ of the circuit before the measurement.



Answer: After the first series of Hadamard gates, the state is given by

$$|\psi_1\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z \in \{0,1\}} |x, y, z, 0, 0\rangle$$

After the U_f gate, the state is given by

$$|\psi_2\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z \in \{0,1\}} |x, y, z, x \oplus y, y \oplus z\rangle$$

So right before the measurement, the state is given by

$$|\psi_3\rangle = \frac{1}{8} \sum_{u,v,w,x,y,z \in \{0,1\}} (-1)^{xu+yv+zw} \; |u, v, w, x \oplus y, y \oplus z\rangle$$

As a reminder, the measurement is described by the collection of orthogonal projectors in the computational basis $\{P_{u,v,w}, \; (u, v, w) \in \{0,1\}^3\}$, defined as

$$P_{u,v,w} = |u, v, w\rangle \langle u, v, w| \otimes I_2$$

and the output state $|\psi'\rangle = P_{u,v,w} |\psi\rangle \,/\, \| \, P_{u,v,w} |\psi\rangle \, \|$ occurs with probability

$$\text{prob}(u, v, w) = \langle\psi| \, P_{u,v,w} \, |\psi\rangle$$

b) Compute prob(u, v, w) for every $(u, v, w) \in \{0,1\}^3$.

Answer: The probabilities are given by

$$\text{prob}(u, v, w) = \frac{1}{64} \sum_{x,y,z,x',y,z' \in \{0,1\}} (-1)^{(x \oplus x')u + (y \oplus y')v + (z \oplus z')w} \, \langle x' \oplus y', y' \oplus z' | x \oplus y, y \oplus z\rangle$$

Observing that the braket term is non-zero if and only if $x', y', z' = x, y, z$ or $x', y', z' = \overline{x}, \overline{y}, \overline{z}$, we obtain

$$\begin{aligned}\text{prob}(u, v, w) &= \frac{1}{64} \sum_{x,y,z \in \{0,1\}} \left((-1)^0 + (-1)^{u+v+w}\right) \\ &= \frac{1}{8} \left(1 + (-1)^{u+v+w}\right) = \frac{1}{4} \quad \text{if and only if} \quad u + v + w \quad \text{is even}\end{aligned}$$

c) Deduce from there the period of the function f (that is, the value of $a \in \{0,1\}^3 \backslash \{(0,0,0)\}$ such that $f(x \oplus a) = f(x)$ for all $x \in \{0,1\}^3$).

Answer: Let $H = \text{span}((0,0,0), a)$. From part b) [and the course on Simon's algorithm], we see that the space $H^\perp = \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}$, so we deduce that $a = (1,1,1)$ (= the only vector such that $a \cdot x = 0$ for all $x \in H^\perp$).

Note: You can also check directly that $a = (1,1,1)$ is the period of the function f by checking that $f(x \oplus a) = f(x)$ for all $x \in \{0,1\}^3$.

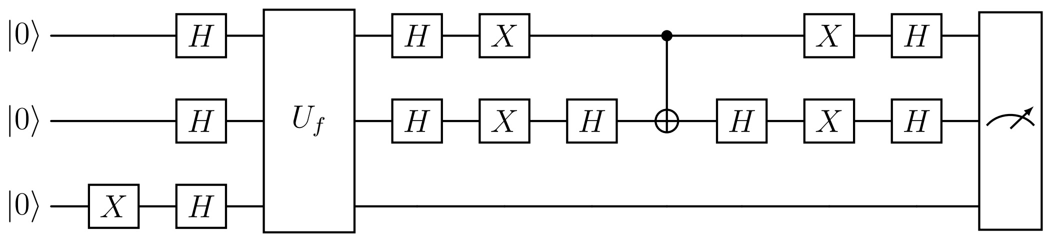
Exercise 3 *Quantum search (18 points)*

Let $f : \{0,1\}^2 \to \{0,1\}$ be a binary function such that there exists a unique value of $(x_0, y_0) \in \{0,1\}^2$ with $f(x_0, y_0) = 1$. Let also U_f be the 3-qubit oracle gate whose action on the states in the computational basis is given by

$$U_f(|x, y, z\rangle) = |x, y, z \oplus f(x,y)\rangle$$

a) Build explicitly a circuit using gates X, H, C-NOT and U_f, taking as input $|0,0,0\rangle$ and whose output is given by $|x_0, y_0\rangle \otimes |\psi\rangle$, where $|\psi\rangle$ is some (irrelevant) state in $\mathbb{C}^2$.

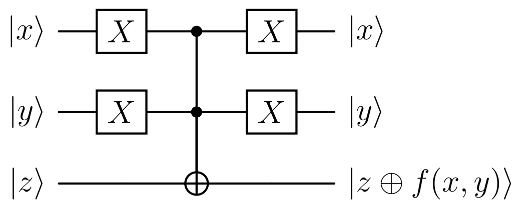
Answer: The circuit is as follows (cf. Grover's algorithm with $k = 1$):



b) Build explicitly the oracle gate U_f in the case where $(x_0, y_0) = (0,0)$.

Note: Here, there is no restriction on the type of elementary gates which can be used.

Answer: The circuit is as follows:



c) Assume now that for the very same function f with $(x_0, y_0) = (0,0)$, we run Deutsch-Josza's circuit with the corresponding gate U_f. After the measurement of the first two qubits of the output of the circuit, what are the probabilities of each output?

Answer: The output of the Deutsch-Josza circuit for a generic function f is given by

$$|\psi\rangle = \frac{1}{4} \sum_{x,y,u,v \in \{0,1\}} (-1)^{f(x,y)+xu+yv} \, |u,v\rangle \otimes |-\rangle$$

So in our case:

$$|\psi\rangle = \frac{1}{4} \sum_{u,v \in \{0,1\}} \left((-1) + (-1)^u + (-1)^v + (-1)^{u+v}\right) |u,v\rangle \otimes |-\rangle$$

Therefore, $\text{prob}(u,v) = \frac{1}{4}$ for every couple $(u,v) \in \{0,1\}^2$.

Exercise 4 *Quantum error correction (18 points)*

a) Two qubits in state $|\varphi\rangle = \sum_{x,y\in\{0,1\}} \alpha_{x,y} \, |x,y\rangle$ in $(\mathbb{C}^2)^2$, with $\sum_{x,y\in\{0,1\}} |\alpha_{x,y}|^2 = 1$, are sent through a channel and the received state is

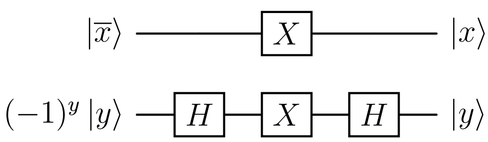
$$|\psi\rangle = \sum_{x,y\in\{0,1\}} (-1)^y \, \alpha_{x,y} \, |\overline{x}, y\rangle$$

Propose a sequence of operations involving exclusively X and H operators allowing to recover the initial state $|\varphi\rangle$ from the received state $|\psi\rangle$, and draw the corresponding circuit.

Answer: To recover $|\varphi\rangle$ from $|\psi\rangle$, it is necessary to perform a bit-flip on x and a phase-flip on y, so

$$|\varphi\rangle = (X \otimes HXH) \, |\psi\rangle$$

which corresponds to the circuit



b) A single qubit in state $|\varphi\rangle \in \mathbb{C}^2$, with $\| \, |\varphi\rangle \, \| = 1$, is sent through a channel and the received state is

$$|\psi\rangle = HXHXHXHX \, |\varphi\rangle$$

What is the *minimum* number of actions needed to recover state $|\varphi\rangle$ from state $|\psi\rangle$ (up to a global phase)? Justify your answer.

Answer: Observe fist that $HXH = Z$. Indeed:

$$HXH = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$

So $HXHXHXHX = ZXZX$ and $XZX = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, so finally, we obtain

$$HXHXHXHX = -I$$

There is therefore *no* action needed in order to recover state $|\varphi\rangle$ from state $|\psi\rangle$ (up to a global phase).

c) Consider the Shor code which, as a reminder, is defined as follows:

$$\begin{cases} |0\rangle_S = \dfrac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \dfrac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \dfrac{|000\rangle + |111\rangle}{\sqrt{2}} \\ \\ |1\rangle_S = \dfrac{|000\rangle - |111\rangle}{\sqrt{2}} \otimes \dfrac{|000\rangle - |111\rangle}{\sqrt{2}} \otimes \dfrac{|000\rangle - |111\rangle}{\sqrt{2}} \end{cases}$$

With this code, is it possible to correct both a bit-flip occuring on a given qubit *and* a phase-flip occuring on another qubit?

If yes, explain the detection and correction procedure in the case where the bit-flip occurs on qubit 1 and the phase-flip occurs on qubit 4.

If no, explain why this is impossible (considering the same example as above).

Answer: Yes, it is possible.

Detection procedure for a bit-flip occuring on qubit 1 and a phase-flip occuring on qubit 4:

Apply Z_1Z_2, Z_2Z_3, as well as $X_1X_2X_3X_4X_5X_6$, $X_4X_5X_6X_7X_8X_9$ to the received state. This will lead to eigenvalues $-1, +1$ and $-1, -1$ respectively, indicating that the bit-flip occured in position 1 and that the phase-flip occured in one of the positions 4,5,6.

Correction procedure for a bit-flip occuring on qubit 1 and a phase-flip occuring on qubit 4:

Apply X_1 to correct the bit-flip on qubit 1 and then $Z_4Z_5Z_6$ to correct the phase-flip on qubit 4.