Problem 1: Projectors and measurement

a. Consider the four Bell quantum states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Write the four matrices of their outer products $\Pi_{\Phi^\pm} = |\Phi^\pm\rangle\langle\Phi^\pm|$ and $\Pi_{\Psi^\pm} = |\Psi^\pm\rangle\langle\Psi^\pm|$ in the two-qubit computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

b. First, show that $\Pi_{\Phi^\pm}$ and $\Pi_{\Psi^\pm}$ are projectors by verifying the condition $\Pi_i^2 = \Pi_i$. Then, show that Π_{Φ^+} and Π_{Φ^-} project onto orthogonal subspaces, as $\Pi_{\Phi^+}\Pi_{\Phi^-} = 0$. Finally, show also that $\Pi_{\Psi^+}\Pi_{\Psi^-} = 0$ and give a simple argument for $\Pi_{\Psi^\pm}\Pi_{\Phi^\pm} = 0$.

c. Check the completeness relation for the measurement in the Bell basis $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$.

d. Compute the probability $\Pr(\Phi^+) = \|\Pi_{\Phi^+}|\psi\rangle\|^2$ for an arbitrary two-qubit state $|\psi\rangle = \psi_{00}|00\rangle + \psi_{01}|01\rangle + \psi_{10}|10\rangle + \psi_{11}|11\rangle$. Then, compute the post-measurement state $|\psi_{\Phi^+}\rangle$ for the same outcome, obtained by dividing the projected vector by its norm:

$$|\psi_{\Phi^+}\rangle = \frac{\Pi_{\Phi^+}|\psi\rangle}{\|\Pi_{\Phi^+}|\psi\rangle\|}.$$

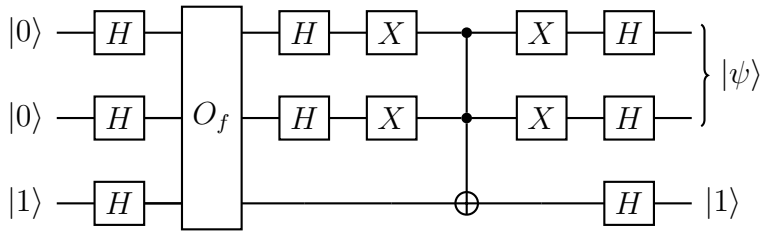
Problem 2: Grover's Algorithm

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

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

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

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 lectures we saw that the scaling of Grover's algorithm is $T \approx \frac{\pi}{4} 2^{n/2}$, which could have led us to think that we would need 2 Grover steps to find the solution. What would be wrong with our reasoning?

Problem 3: Simon's Algorithm

Suppose we run Simon's algorithm on the following function $f : \{0,1\}^3 \to \{0,1\}^3$:

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

where f is two-to-one and satisfies $f(x) = f(x \oplus a)$ for all $x \in \{0,1\}^3$, for some unknown period $a \neq 000$.

a. By inspecting the function given above, find the period a.

b. What is the initial state of the two registers in Simon's algorithm?

c. What will the state be after:

1. the first layer of Hadamard gates applied to the upper three qubits;

2. the oracle query $O_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$?

d. What would the state be after measuring the second register, supposing that the measurement gave the outcome 001?

e. Imagine we now apply the final step, three Hadamard transforms. Using the formula

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle ,$$

write the state after applying this step.

f. Suppose 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 $a = 111$.