Raul Garcia-Patron
Stuart Ferguson

Tutorial 4

Problem 1: Projectors and measurement

a. Consider the four Bell quantum states:

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

Write the fours matrices of their outer-products $P_{\Phi^\pm} = |\Phi^\pm\rangle\langle\Phi^\pm|$ and $P_{\Psi^\pm} = |\Psi^\pm\rangle\langle\Psi^\pm|$ in the 2-bit computational basis ($\{00, 01, 10, 11\}$).

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

c. Check the completeness relation for the measurement on the $\{\Phi^\pm, \Psi^\pm\}$ basis.

d. Compute $P(\Phi^+) = ||P_{\Phi^+}|\psi\rangle||^2$ for an arbitrary two-qubit state $|\psi\rangle = \psi_{00}|00\rangle + \psi_{01}|01\rangle + \psi_{10}|10\rangle + \psi_{11}|11\rangle$.

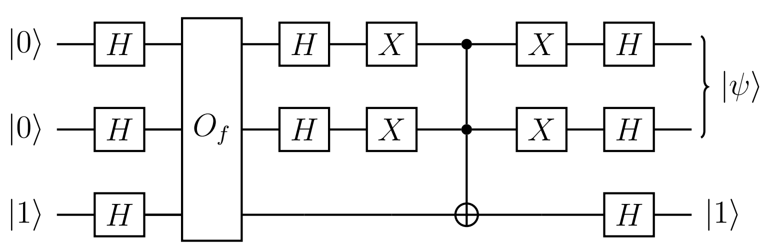
Problem 2: Grover's Algorithm

Consider a search space of dimension $N = 4$ with its elements encoded in binary $\{00, 01, 10, 11\}$. 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 lecture we saw the scaling of Grover algorithm is $T \approx \frac{\pi}{4} 2^{n/2}$, which could have lead 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 $f(x) : \{0,1\}^3 \to \{0,1\}^3$.

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

Where $f(x)$ is $2 - \text{to} - 1$ and $\text{f}(x_i) = f(x_i \oplus 111)$ for all $i \in \{0,1\}^3$; therefore the period is $a = 111$.

a. What is the initial input of Simon's algorithm?

b. What will the state be after:

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

2. the phase kickback unitary generated by the oracle query.

c. What would the state be after measuring the second register, supposing that the measurement gave $|001\rangle$?

d. Imagine we now apply the final step, three Hadamard transforms. Using the formula $H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{xy} |y\rangle$, write the state after applying this step.

e. If 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 $a = 111$.