Raul Garcia-Patron
Petros Wallden
Milos Prokop

Tutorial 4

IQC 2023-24
October 27, 2023

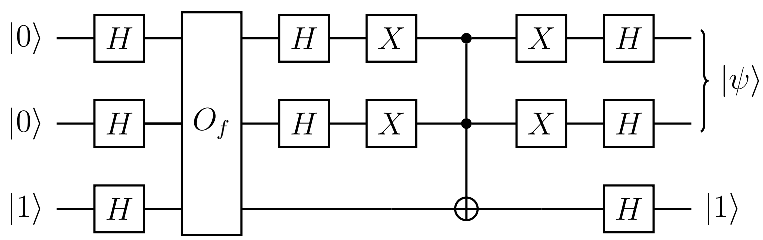
Problem 1: Grover's Algorithm

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 2: Simon's Algorithm

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

$$f(000) = f(111) = 000$$
$$f(001) = f(110) = 001$$
$$f(010) = f(101) = 010$$
$$f(011) = f(100) = 011$$

Where $f(x)$ is $2 - \text{to} - 1$ and 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 $|001\rangle$?

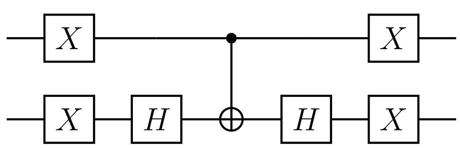
d. Imagine we now apply the final step, three Hadamard transforms. Using the formula $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{xy}|y\rangle$, write the state after applying this step.

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 $a = 111$.

Problem 3: Phase kick-back without ancillary qubit

In the course we have seen that the existence of a quantum oracle implementing $|x\rangle \otimes |0\rangle \xrightarrow{O_f} |x\rangle \otimes |f(x)\rangle$ guarantees the existance of the phase kickback unitary $U_f|x\rangle \to (-1)^{f(x)}|x\rangle$. If this provides an easy way of implementing U_f from O_f, in some situation the agent providing the oracle could have given us directly a quatum oracle implementing U_f directly in a more compact way.

a. In problem 1 above, the target (lower) qubit is a catalytic qubit used to implement a phase-kickback unitary on the address (top) qubits. Show that the circuit below also implements the *conditional phase shift transformation* $2|00\rangle\langle 00| - I$,



,

up to a global phase. This allows to replace the circuit on the right of the oracle O_f by a 2-qubit circuit that uses a single CNOT instead of a control-control-NOT.

b. Taking inspiration from the results from the previous subquestion construct a 2-qubit quantum circuit which performs the phase kickback unitary U_f.