Lecture "Quantum Information" WS 19/20 — Exercise Sheet #6

Problem 1: Grover's algorithm with multiple marked elements.
Consider the Grover search problem of finding x_0 such that $f(x_0) = 1$ for some function $f(x) \in \{0, 1\}$. In the lecture, we derived Grover's algorithm which finds x_0, given that it is unique. Now assume that there are $r > 1$ solutions to the equation $f(x) = 1$. In other words, suppose that we have N states and r of them are marked. The problem is to find one of the marked states with high probability.
Grover's algorithm with multiple solutions is very similar to the unique solution one. First, the oracle is constructed the same way as before, i.e.

$$O_f = \mathbb{I} - 2 \sum_{x \text{ s.t.} f(x)=1} |x\rangle\langle x|$$

Find the action of the oracle on a state $|x\rangle$. The remaining steps of the algorithm remain unchanged (i.e. the definition of O_ω and the alternating application of O_f and O_ω. Perform a step-by-step analysis of this modified Grover's algorithm, and estimate the number of iterations needed to obtain one of the marked elements with high probability. How does the runtime of the algorithm scale in r and N? Compare this to the performance of a classical algorithm.

Problem 2: Phase estimation.
Consider a unitary U with an eigenvector $U|\phi\rangle = e^{2\pi i\phi}|\phi\rangle$. Assume that $\phi = 0.\phi_1\phi_2 \ldots \phi_n = \frac{1}{2}\phi_1 + \frac{1}{4}\phi_2 + \ldots$. Our goal will be to study ways to determine ϕ as accurately as possible, given that we can implement U (and are given $|\phi\rangle$).

1. First, consider that we use controlled-U operations $CU|0\rangle|\phi\rangle = |0\rangle|\phi\rangle$, $CU|1\rangle|\phi\rangle = |1\rangle e^{2\pi i\phi}|\phi\rangle$. Describe a protocol where we apply CU to $|+\rangle|\phi\rangle$, followed by a measurement on the first qubit, to infer information about ϕ.

2. Now consider a refined scheme. To this end, assume we can also apply controlled-$U^{(2^k)} \equiv CU_k$ operations for integer k efficiently.
   a) We start by applying CU_{n-1} to $|+\rangle|\phi\rangle$. Which information can we infer? What measurement do we have to make (we perform measurement again on the first qubit)?
   b) In the next step, we apply CU_{n-2}, *knowing* the result of step a). What information can we infer? What measurement do we have to make? Rephrase the measurement as a unitary rotation followed by a measurement in the $|\pm\rangle$ basis.
   c) Iterating the preceding steps, describe a procedure (circuit) to obtain $|\phi\rangle$ exactly. How many times do we have to evaluate controlled-$U^{(2^k)}$'s?
   (*Note:* This procedure is known as *quantum phase estimation.*)

3. An alternative way to determine ϕ is to use the quantum Fourier transform. To this end, we apply a transformation

$$\sum_{x=1}^{2^n} |x\rangle|\phi\rangle \mapsto \sum_{x=1}^{2^n} |x\rangle U^x|\phi\rangle,$$

   followed by a quantum Fourier transform (applied on the first n qubits) and a measurement. Describe the resulting protocol, its outcome, and the number of $U^{(2^k)}$'s required.