HW3 (25 points)

Problem 1. *(Points :1+5+1=7)* Consider the unordered search problem, i.e., the task of searching for $x \in \{0,1\}^2$ such that $f(x) = 1$ where $f()$ can be accessed through an oracle $U_f |x, b\rangle \to |x, b \oplus f(x)\rangle$. We can use the amplitude amplification framework on the following algorithm $A|0^3\rangle \to \frac{1}{2}\sum_{x\in\{0,1\}^2} |x, f(x)\rangle$ and the following projector for good states $P_g = I \otimes |1\rangle\langle 1|$.

Consider the following function: $f(00) = f(01) = f(11) = 0$, and $f(10) = 1$. Draw the circuit for performing unordered search using the amplitude amplification framework that uses 1 application of the Grover's iterator. Recall that the iterator was described in the lecture as a sequence of 4 operators. Specify the states before and after each of these operators. What is the probability of success?

Note that the above approach differs slightly from the standard Grover's algorithm, in terms of the low-level gates.

Problem 2. *(Points :5+6=11)* Question 1 shows how to use the amplitude amplification framework to solve the unordered search problem. However, a fundamental requirement of this approach is the knowledge of the initial success probability, or equivalently, the number of solutions. For this question, assume that we do not know the number of solutions. Suppose the total number of items is denoted N, and there are t solutions.

1. Study the algorithm described on page-9 of https://courses.cs.duke.edu/spring06/cps237/Quantum.papers/boyer.search.pdf that can output a solution. The algorithm promises to output a solution, if one exists, using $c\sqrt{N/t}$ queries, with probability at least 0.99, in which c is a fixed constant.

2. (3+2=5 points) Design and analyse the query complexity of an algorithm to output all solutions. Your algorithm will call the above algorithm.

3. Study the QISKIT API `class Grover` on https://qiskit.org/documentation/stubs/qiskit.algorithms.Grover.html. The S_f oracle is same as the $(2P_g - I)$ operator and the S_0 operator is same as the $2|0^n\rangle\langle 0^n| - I$ operator that we used while discussing the Grover's iterator. *You may want to reflect upon the difference between this implementation and that in Q1.*

4. Recall that you implemented a U_f for a Boolean function in HW2. For familiarity with the Grover API, use it to find any solution to $f(x)$. This task is ungraded and need not be submitted.

5. (4+2=6 points) Implement your algorithm above to find all x such that $f(x) = 1$ (assume that you do not know its truth table). The *precision* of one run is the fraction of solutions found relative to total number of output, and the *recall* is the fraction of solutions relative to the actual number of solutions. Run the entire algorithm 20 times, tracking the precision, recall, and the number of queries to U_f each time. Submit the Python code/Jupyter notebook, a table with the precision, recall, queries, and their average values for the 20 runs.

Problem 3. *(Points :3+1+3=7)* This problem involves algebra, in particular inequalities on real and complex numbers, and states and operators.

1. (3 points) Given two quantum states $|\psi\rangle = \sum_i \alpha_i |i\rangle$ and $|\phi\rangle = \sum_i \beta_i |i\rangle$ on the same Hilbert space, consider the following distance measures. The Euclidean distance is defined as $\| |\psi\rangle - |\phi\rangle \| = \sqrt{\sum_i |\alpha_i - \beta_i|^2}$. The total variation distance is defined as $TVD(|\psi\rangle, |\phi\rangle) = \frac{1}{2}\sum_i |\alpha_i^2 - \beta_i^2|$ (it actually denotes the maximum difference in the probability distributions obtained by measuring them in the standard basis). Suppose $\| |\psi\rangle - |\phi\rangle \| = \epsilon$. Show that $TVD(|\psi\rangle, |\phi\rangle) \leq \epsilon$. This implies that states with low Euclidean distance generate almost identical probability distributions upon measurement, and are thus, hard to distinguish. You will probably require the Cauchy-Schwarz inequality: $\sum_i u_i v_i \leq \sqrt{\sum_i u_i^2}\sqrt{\sum_i v_i^2}$ where each variable must be a real number.

2. (1 point) The *operator norm* of an operator is defined as $\|U\| = \max_{|v\rangle} \|U|v\rangle\|$ where the maximum is taken only on normalized states. An alternative definition is the largest singular value of U. The *distance* between two operators is defined as $\|U - V\|$. What is the distance between I and R_{10} (R_k was defined while constructing the circuit for QFT)? You do not have to submit, but you can similarly compute the distance between the controlled-R_{10} gate and identity. These distance will come out to be very small. Observe that operators with a low distance cannot generate states with a large Euclidean norm.

3. (3 points) Let U_1, U_2, U_3 be any three unitary operators. Let U denote the circuit $U_3U_2U_1$ and V denote the circuit U_3U_1 (so, U_2 is left out). Show that $\|U - V\| = \|U_2 - I\|$. This can be generalized to larger sequences of gates as well, and then the result indicates that dropping a gate which is almost similar to identity does not change the overall behaviour of the circuit. Now further using the previous subquestions, we get that it is okay to drop the controlled-R_k gates from the QFT circuit for large k.
