Assignment: CS 682 (Fall 2022)

1. (5+5) The following steps show, how to implement a Toffoli gate using standard two and one qubit gates.
   - What is the square root of X gate (assume positive square roots). How can you implement controlled version of it using C-S gate (S is the phase gate).
   - Show that a CC-U gate (for any unitary U) can be implemented using CNOT,C-V and C-V^* gates, where V is the square root of U. Hint: If a, b represent the boolean value at the control wires, we need to apply $V^b(V^*)^{b\oplus a}V^a$.
2. (5+5) Suppose we want to factor 15 on a quantum computer. We will do it by finding the order of 2 on the quantum computer.
   - Show all the classical steps needed after we get the order of 2.
   - Simulate the quantum algorithm to get the order of 2. Assume that you have continued fraction as a subroutine and it gives $1, r$ (for fraction $1/r$) as the answer in the first chance. Describe the oracle and the intermediate states.
3. (10) Given n, a, b, we are interested in finding s for which $a^s = b \mod n$. Show that this problem can be converted to an HSP with function $f(x_1, x_2) = b^{x_1}a^{x_2}$. State clearly, what is the group and what is the hidden subgroup.
4. (5+5+5) Given a positive integer m, let $n = 2^{\lceil \log m \rceil}$. Let F_m be Fourier transform over $\mathbb{Z}_m$ defined on an n-dimensional space.

$$F_m(|x\rangle) = \begin{cases} |\tilde{x}\rangle = \frac{1}{\sqrt{m}}\sum_{y=0}^{m-1} e^{2\pi i xy/m}|y\rangle & \text{for } 0 \le x < m \\ |x\rangle & m \le x < n \end{cases}$$

   - Let U be the operator: $U|y\rangle = |y-1 \mod m\rangle$ if $0 \le y < m$, otherwise $U|y\rangle = |y\rangle$. Show that $|\tilde{x}\rangle$ is an eigenvector of U with eigenvalue $e^{2\pi i x/m}$.
   - Give a quantum algorithm to convert $|0\rangle|\tilde{x}\rangle$ to $|x\rangle|\tilde{x}\rangle$. Assume x/m requires small precision to be specified completely.
   - Show that you can convert $|x\rangle|\tilde{x}\rangle$ to $|0\rangle|\tilde{x}\rangle$.
5. (5+5+5) Element distinctness is a problem where given a function $f : [n] \to S$, we need to find if it is a one-to-one mapping. That means, does there exist two elements $x, y \in [n]$ such that $f(x) = f(y)$. The function is given as an oracle. Your task is to design an algorithm for this problem with query complexity $O(n^{3/4})$.
   - Let l be a parameter, we pick l random elements and query them all. Next, we search in the remaining $n - l$ elements, if there is a value which collides with one of these l values using Grover search. With proper justification, show that the query complexity of the algorithm is $l + O(\sqrt{n})$.

- What is the success probability of the previous algorithm. How many iterations do we need to make it constant?
- Show that there exists an l such that the above algorithm succeeds with constant probability and does $O(n^{3/4})$ queries.