Worksheet 6
IQC 2024

1. (a) Is $QFT_{2^2} = (QFT_2)^{\otimes 2}$?

   (b) Show that for any n, $(QFT_2)^{\otimes n} |0^n\rangle = QFT_{2^n} |0^n\rangle$.

2. Given an N such that $N = A^B$, show that it is possible to obtain A in time $O(\log^3(N))$ for any $A > 1$ and $B \geq 2$.

3. Recall that when performing an unordered search in the case when θ is known, the number of times the Grover iterator was applied was $k = \lfloor \frac{\pi}{4\theta} + 1 \rfloor$. Moreover, we showed that using this k would limit the error to at most 1/2. Now, show that even if we set $k = \lceil \frac{\pi}{4\theta} + 1 \rceil$, the error of the algorithm would still be at most 1/2.

4. Prove that any n-qubit state $|\phi\rangle$ that is orthogonal to $H |00 \cdots 0\rangle$ has the sum of its amplitudes equal to 0.

5. Say you are given access to a Boolean input X via an oracle. You are also promised that the Hamming weight of X, denoted $|X|$, is either 0 or some integer t. Given X, you are to distinguish if $|X|$=0 or $|X| = t$.

   - Construct a classical algorithm of complexity $O(N)$ that solves this problem with probability 1.
   - Construct a classical algorithm of complexity $O(N/t)$ that solves this problem with a high probability.
   - Can you construct a quantum algorithm with complexity $O(\sqrt{N/t})$ that success with probability 1? (Hint: Such an algorithm is possible.)

6. Recall that the Grover iterator can be given as a composition of two reflections as $\mathbf{G} = R_{|\psi\rangle} R_{|x\rangle}$ where $|x\rangle$ is the good state and $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_y |y\rangle$. Show, that for any state $|\phi\rangle = \sum_y \alpha_y |y\rangle$, the operator $R_{|\psi\rangle}$ inverts about the mean, i,e., it acts as

$$R_{|\psi\rangle} |\phi\rangle = \sum_y (\mu - \alpha_u) |y\rangle$$

   where $\mu = \frac{1}{N} \sum_y \alpha_y$. (Hint: Decompose $|\phi\rangle$ into $|\psi\rangle$ and $|\psi^\perp\rangle$.)

7. Suppose we have an algorithm A that outputs a good solution with probability $\frac{1}{4} - \epsilon$. Show how one iteration of amplitude amplification gives us an algorithm that succeeds with probability $1 - O(\epsilon^2)$.

8. Let $|\phi_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} |yr + b\rangle$. Suppose you are given a candidate p. Construct an algorithm that outputs 0 always if p is a multiple of r and outputs 1 with probability at least 1/2 if p is not a multiple of r. (Hint: How can you use p and $|\phi_{r-b}\rangle$ to get such an algorithm?)