2.111J/18.435J/ESD.79 Quantum Computation | Due: Oct 25, in class

Problem Set 5 (Corrected)

Problem 1

Define an unitary transformation G_s to be

$$G_s = 2\left|s\right\rangle\left\langle s\right| - I \ . \tag{1}$$

It has the eigenvectors $\left|s\right\rangle$ and $\left|s_\perp\right\rangle$, which are orthogonal to each other, such that $G_s\left|s\right\rangle = \left|s\right\rangle$ and $G_s\left|s_\perp\right\rangle = -\left|s_\perp\right\rangle$. Now, construct G_s with the following

$$\begin{aligned} V\left|0\dots0\right\rangle &= \left|s\right\rangle \\ G_0\left|0\dots0\right\rangle &= \left|0\dots0\right\rangle \\ G_0\left|a\right\rangle &= -\left|a\right\rangle, a \neq 0 \ . \end{aligned}$$

You are allowed to use G_0 and V more than once. Note that each ket vector represents n qubits.

Problem 2

Devise an algorithm that identifies one of the M winners in the following function

$$f(x) = \begin{cases} 0 & \text{if } x \notin w \\ 1 & \text{if } x \in w, |w| = M, \end{cases} \tag{2}$$

where you can assume $M \ll N$.

Problem 3

Show that classically, any algorithm that solves Simon's problem with a probability of at least $\frac{2}{3}$ for any function f must evaluate f at least $O(2^{\frac{n}{3}})$ times. Note: Many people have not been able to obtain this bound, if you have found a looser bound, you are allowed to present it.

Problem 4

In Simon's problem, where s is the hidden period, show that a measurement in the computational basis would yield result $w^{(i)}$, $i = 1, 2, \dots (n-1)$, such that the set $\{w^{(i)}\}$ is uniformly distributed over the dim $(n-1)$ space that is orthogonal to s.