Problem 1

Define an unitary transformation $G_s$ to be

$$G_s = 2 |s⟩⟨s| - I.$$  \hspace{1cm} (1)

It has the eigenvectors $|s⟩$ and $|s⊥⟩$, which are orthogonal to each other, such that $G_s |s⟩ = |s⟩$ and $G_s |s⊥⟩ = - |s⊥⟩$. Now, construct $G_s$ with the following

$$V |0\ldots0⟩ = |s⟩$$

$$G_0 |0\ldots0⟩ = |0\ldots0⟩$$

$$G_0 |a⟩ = - |a⟩, a \neq 0.$$ 

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

$$f(x) = \begin{cases} 
0 & \text{if } x \notin w \\
1 & \text{if } x \in w, |w| = M,
\end{cases}$$  \hspace{1cm} (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 $O(2^n)$ 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 $w^{(i)}$, $i = 1,2,\ldots(n-1)$, such that the set $\{w^{(i)}\}$ is uniformly distributed over the dim $(n-1)$ space that is orthogonal to $s$. 