QCLG Exercise sheet 6

Exercise 1. *Consider an efficiently computable function $f : \{0, \ldots, 2^n-1\} \to \{0,1\}$. We also consider a string $s = s_0, \ldots, s_{S-1} \in \{0,1\}^S$. The goal is to find S consecutive values of $f(x)$ that are equal s. More formally, we want to find $x \in \{0, \ldots, 2^n - S\}$ st. $f(x) = s_0$, $f(x+1) = s_1, \ldots, f(x+S-1) = s_{S-1}$. We assume there exists a single x_0 that satisfies this property*

1. *Find a quantum algorithm that finds x_0 in time $O(S2^{n/2})$.*
2. *Assume now we have an efficiently computable function $g : \{0, \ldots, S-1\} \to \{0,1\}$ st. $g(i) = s_i$.*
   (a) *Assume you have access to a version of Grover's algorithm, that outputs a solution to a search problem for a function $l : I \to \{0,1\}$ if there is a solution and $\perp$ if there is no solution. Assume also that this routine works wp. 1 and takes time $O(\sqrt{|I|})$. Construct an algorithm A that for any input x, outputs 1 if $x = x_0$ and 0 otherwise in time $O(\sqrt{S})$.*
   (b) *Construct a quantum algorithm that finds x_0 in time $O(\sqrt{S}2^{n/2})$.*

Exercise 2.

1. *We are given 2 efficiently computable functions $f, g : \{0,1\}^n \to \{1, \ldots, N\}$. We say that f dominates g iff. $\forall x \in \{0,1\}^n,\ f(x) \geq g(x)$. Give a quantum algorithm that determines whether f dominates g in time $O(\sqrt{2^n})$. One can use $\sin(\theta) \approx \theta$ for $0 \leq \theta \ll 1$.*
2. *We are given an efficiently computable function $f : \{0,1\}^n \to \{0,1\}$ with $T = \{x : f(x) = 1\}$. We are given the promise that $T = 1$ or $T = 2^{n/2}$. Construct an algorithm that determines in which case we are in time $O(2^{n/4})$ and succeeds with high probability.*

Exercise 3 (Grover's algorithm that succeeds wp. 1)**.** *Consider an efficiently computable function $f : \{0,1\}^8 \to \{0,1\}$ such that $\exists!\ x_1 \in \{0,1\}^8,\ f(x_1) = 1$. We run Grover's algorithm to find this solution. We call the iteration 0 of Grover's algorithm the construction of $|\psi_0\rangle = \frac{1}{16}\sum_{x\in\{0,1\}^8} |x\rangle |f(x)\rangle$ and each iteration is the reflexion $R_{|\psi_{Bad}\rangle}$ over $|\psi_{Bad}\rangle = \sqrt{\frac{1}{255}}\sum_{x:f(x)=0} |x\rangle |0\rangle$ and then the reflexion $R_{|\psi_0\rangle}$ over $|\psi_0\rangle$. Our goal is to perfectly construct $|\psi_{Good}\rangle = |x_1\rangle |1\rangle$.*

1. *Write $|\psi_0\rangle$ in the $\{|\psi_{Bad}\rangle, |\psi_{Good}\rangle\}$ basis. Show how to construct $|\psi_0\rangle$ efficiently.*

2. *What is the state of Grover's algorithm after C steps. One can write the solution as a function of $\alpha = \arcsin(\frac{1}{16})$.*

3. *Let $|\psi_C\rangle$ be the quantum state after C iterations. What is the smallest value of C for which we are just before the crossing point of $|\psi_{Good}\rangle$, meaning that $\langle\psi_C|\psi_{Bad}\rangle > 0$ and $\langle\psi_C|\psi_{Bad}\rangle < 0$. We can use $\alpha \in [\frac{\pi}{50.2}, \frac{\pi}{50.3}]$. Draw a picture of this "crossing" of $|\psi_{Good}\rangle$.*

4. *Perform C iterations of Grover's algorithm where C is the smallest value just before the crossing point. Assume we could make a counter-clockwise rotation of angle β in the $\{|\psi_{Bad}\rangle, |\psi_{Good}\rangle\}$ basis for any $\beta \in [0, 2\alpha]$. Show how to transform $|\psi_C\rangle$ into $|\psi_{Good}\rangle$ with a single β-rotation.*

5. *We now show how to construct such β-rotations.*

   (a) *Show that if we write $R_{|\psi_0\rangle}$ and $R_{|\psi_{Bad}\rangle}$ in matrix form in the $\{|\psi_{Bad}\rangle, |\psi_{Good}\rangle\}$ basis, we get*

   $$R_{|\psi_{Bad}\rangle} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } R_{|\psi_1\rangle} = \begin{pmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{pmatrix}. \quad (1)$$

   (b) *We now define for $\gamma \in [0, 2\pi)$ the unitaries $R^{\gamma}_{|\psi_{Bad}\rangle}$ and $R^{\gamma}_{|\psi_1\rangle}$ satisfying*

   $$R^{\gamma}_{|\psi_{Bad}\rangle}(|\psi_{Bad}\rangle) = |\psi_{Bad}\rangle \;;\; R^{\gamma}_{|\psi_{Bad}\rangle}(|\psi_{Good}\rangle) = e^{i\gamma}|\psi_{Good}\rangle$$
   $$R^{\gamma}_{|\psi_0\rangle}(|\psi_0\rangle) = |\psi_0\rangle \;;\; R^{\gamma}_{|\psi_0\rangle}(|\psi_0^{\perp}\rangle) = e^{i\gamma}|\psi_0^{\perp}\rangle$$

   where $|\psi_0^{\perp}\rangle = \sin(\alpha)|\psi_{Bad}\rangle - \cos(\alpha)|\psi_{Good}\rangle$. We obtain the usual reflexions by taking $\gamma = \pi$. We will use without proof that we can construct efficiently these operations and that in the $\{|\psi_{Bad}\rangle, |\psi_{Good}\rangle\}$ basis, these unitaries can be written as

   $$R^{\gamma}_{|\psi_{Bad}\rangle} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\gamma} \end{pmatrix} \text{ and } R^{\gamma}_{|\psi_0\rangle} = \begin{pmatrix} \cos^2(\alpha) + e^{i\gamma}\sin^2(\alpha) & \cos(\alpha)\sin(\alpha)(1-e^{i\gamma}) \\ \cos(\alpha)\sin(\alpha)(1-e^{i\gamma}) & \sin^2(\alpha) + e^{i\gamma}\cos^2(\alpha) \end{pmatrix}.$$

   Show that these matrices are consistent with the ones in Equation 1 for $\gamma = \pi$.

   (c) *For an angle $\beta \in [0, 2\alpha]$, show that $\exists\gamma \in [0, \pi]$ st. $|\cos^2(\alpha) + e^{i\gamma}\sin^2(\alpha)| = \cos(\beta)$. Show that in this case $R^{\gamma}_{|\psi_0\rangle}$ can be written as*

   $$R^{\gamma}_{|\psi_0\rangle} = \begin{pmatrix} e^{i\rho_1}cos(\beta) & e^{i\rho_2}\sin(\beta) \\ e^{i\rho_2}\sin(\beta) & e^{i\rho_3}cos(\beta) \end{pmatrix}.$$

for some angles $\rho_1, \rho_2, \rho_3 \in [0, 2\pi)$. *You can use the fact that* $R^{\gamma}_{|\psi_0\rangle}$ *is a unitary matrix.*

(d) *Using the fact that* $R^{\gamma}_{|\psi_1\rangle}$ *is a unitary matrix, show that the* $\rho_1+\rho_3 = \pi+2\rho_2 \mod (2\pi)$.

(e) *Find* ξ *and* ξ' *st.*

$$R^{\xi}_{|\psi_{Bad}\rangle} R^{\gamma}_{|\psi_0\rangle} R^{\xi'}_{|\psi_{Bad}\rangle} = e^{i\rho_1} \begin{pmatrix} \cos(\beta) & -\sin(\beta) \\ \sin(\beta) & \cos(\beta) \end{pmatrix}.$$

(f) *With the above, we constructed, up to a global phase, the counter-clockwise rotation of angle* β *in the* $\{|\psi_{Bad}\rangle, |\psi_{Good}\rangle\}$. *Conclude.*