QCLG Exercise sheet 5

Exercise 1. *Consider a function $f : \{0,1\}^2 \to \{0,1\}$ st. there exists a unique x_1 st. $f(x_1) = 1$. Apply one step of Grover's algorithm (i.e. construct the original state $|\psi_1\rangle$ and then perform a reflexion over $|\psi_{Bad}\rangle$ and then over $|\psi_1\rangle$). More precisely:*

1. *Write the different states $|\psi_{Good}\rangle, |\psi_{Bad}\rangle, |\psi_1\rangle$ as defined in the lecture in this setting.*
2. *Write $|\psi_1\rangle = \cos(\theta)|\psi_{Bad}\rangle + \sin(\theta)|\psi_{Good}\rangle$. What is the value of θ?*
3. *Show the different steps of the computation - you don't need to reprove how to perform the reflexions - and show the algorithm succeeds wp. 1 after 1 step of Grover's algorithm in this case.*

Assume now we have the following generalization of Grover's algorithm:

Theorem 1. *Let $f : T \to \{0,1\}$ be an efficiently computable function. Let $S = \{x \in S : f(x) = 1\}$. Grover's algorithm finds a random element of S in time $O(\sqrt{\frac{|T|}{|S|}})$.*

We can use this theorem for the next exercice.

Exercise 2. *We consider a graph $G = (V, E)$ with V being the set of vertices and E being the set of edges. Let $|V| = n$ and $|E| = m$. The graph is undirected so $(i,j) \in E \Leftrightarrow (j,i) \in E$ and without self-loops so $(i,i) \notin E$ for each $i \in V$. We have access to an efficient classical circuit that computes f_E where*

$$f_E(i,j) = 1 \textit{ if } (i,j) \in E \textit{ and } f_E(i,j) = 0 \textit{ otherwise.}$$

A triangle is a triplet (i,j,k) st. $(i,j), (j,k), (i,k) \in E$.

1. *Use Grover's algorithm to find a quantum algorithm that finds a triangle in time $O(n^{3/2})$ if a triangle exists.*
2. *Find a quantum algorithm that finds an edge in time $O(\sqrt{\frac{n^2}{m}})$. Argue that the edge found is a random edge from the set of all edges.*
3. *Given an edge (i,j), find an algorithm that determines whether there exists k st. (i,j,k) is a triangle in time $O(\sqrt{n})$.*

4. *From there, constructs an algorithm that finds a triangle* (i, j, k) *(if it exists) in time* $O(\sqrt{\frac{n^2}{m}} + \sqrt{n})$ *and that succeeds wp. at least* $\frac{1}{m}$.

5. *In the next lecture, we will present the notion of amplitude amplification saying that if you have an algorithm running in time* T *that finds a solution to a problem wp.* p *then you can construct an algorithm finding a solution in expected time* $O(T\sqrt{\frac{1}{p}})$. *Use this result to find a quantum algorithm for finding a triangle in time* $O(n + \sqrt{mn})$.

6. *Compare this complexity with the one from Question* 1. *When is it better? Can it be worse?*

Extra exercice.

Let $x = x_0 \dots x_{N-1}$, where $N = 2^n$ and $x_i \in \{0,1\}^n$, be an input that we can query in the usual way. We are promised that this input is 2-to-1: for each i there is exactly one other j such that $x_i = x_j$.[3] Such an (i, j)-pair is called a *collision*.

(a) Suppose S is a uniformly randomly chosen set of $s \leq N/2$ elements of $\{0, \dots, N-1\}$. What is the probability that there exists a collision in S?

(b) (H) Give a classical randomized algorithm that finds a collision (with probability $\geq 2/3$) using $O(\sqrt{N})$ queries to x.

(c) (H) Give a quantum algorithm that finds a collision (with probability $\geq 2/3$) using $O(N^{1/3})$ queries.