Exercise 1. Finding a hidden parabola in a function.

Suppose we are given a black-box function $f_{\alpha,\beta} : \mathbb{F}_p^2 \rightarrow \mathbb{F}_p$, where $p$ is a prime, satisfying the promise that $f_{\alpha,\beta}(x, y) = f_{\alpha,\beta}(x', y')$ if and only if

$$\alpha x^2 + \beta x - y = \alpha x'^2 + \beta x' - y'.$$

for some unknown $\alpha \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_p$. In other words, $f_{\alpha,\beta}$ is constant on the parabola

$$P_{\alpha,\beta,\gamma} := \{(x, y) \in \mathbb{F}_p^2 : y = \alpha x^2 + \beta x + \gamma\}$$

for any fixed $\gamma \in \mathbb{F}_p$, and distinct on parabolas corresponding to different values of $\gamma$. We have access to the unitary

$$O_{f_{\alpha,\beta}}(|x\rangle|y\rangle|z\rangle) = |x\rangle|y\rangle|z + f_{\alpha,\beta}(x, y)\rangle.$$

and our goal is to find $\alpha$ and $\beta$. Recall that for all $x \in \mathbb{F}_p$,

$$QFT_p(|x\rangle) = \frac{1}{\sqrt{p}} \sum_{y \in \mathbb{F}_p} \omega^{xy} |y\rangle.$$

where $\omega = e^{2\pi i/p}$. We consider the following procedure

---

**Procedure 1**

1. Start from three registers initialized at $|0\rangle$.
2. Apply $QFT_p$ on each of the two first registers.
3. Apply the unitary operation $O_{f_{\alpha,\beta}}$ on all the registers.
4. Measure the third register in the computational basis i.e. the basis $\{|0\rangle, \ldots, |p-1\rangle\}$.
5. Apply $QFT_p$ on the second register and measure it.
Question 1. Show that after step 4 the above procedure creates the state

$$|\psi_4\rangle = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} |x\rangle|\alpha x^2 + \beta x + \gamma\rangle.$$ 

for an unknown $\gamma \in \mathbb{F}_p$.

Solution: Let’s follow the steps of the procedure

$$|0\rangle|0\rangle|0\rangle \xrightarrow{QFT_p \otimes QFT_p \otimes I} \frac{1}{p} \sum_{x,y \in \mathbb{F}_p} |x\rangle|y\rangle|0\rangle \xrightarrow{O_{f_{\alpha,\beta}}} \frac{1}{p} \sum_{x,y} |x\rangle|y\rangle|f(x,y)\rangle.$$ 

We measure the third register and get some value $v$, the two first register are a uniform superposition over inputs $x,y$ such that $f(x,y) = v$. $v$ is the image of $f$, so there exists $x_0, y_0$ such that $f(x_0, y_0) = v$. By definition of $f$, values $x, y$ such that $f(x,y) = v$ are exactly the elements of $P_{\alpha,\beta,\gamma}$ for an unknown $\gamma$ (because $x_0, y_0$ are not known). The 2 first registers therefore become

$$|\psi_4\rangle = \frac{1}{\sqrt{p}} \sum_{x,y \in P_{\alpha,\beta,\gamma}} |x\rangle|y\rangle = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} |x\rangle|\alpha x^2 + \beta x + \gamma\rangle.$$ 

\[\square\]

Question 2. Show that after step 5 the above procedure creates (up to a global phase) the state

$$|\psi_u\rangle = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \omega^{(\alpha x^2 + \beta x)u} |x\rangle.$$ 

for a known $u$. Why is $u$ known ?

Solution: We start from $|\psi_4\rangle$. After applying $F_p$, we get the state

$$\frac{1}{p} \sum_{x,u} \omega^{(\alpha x^2 + \beta x + \gamma)u} |x\rangle|u\rangle.$$ 

when we measure $u$ at the second register, we obtain $\frac{\omega^u}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \omega^{(\alpha x^2 + \beta x)u} |x\rangle$. $u$ is measured hence known. \[\square\]

Question 3. We apply the procedure twice and we construct the state $|\Phi\rangle = |\psi_u\rangle \otimes |\psi_{u'}\rangle$ for 2 known values $u, u' \in \mathbb{F}_p$. Write $|\Phi\rangle$. Show (using ancilla qubits), how to construct in time $O(\text{polylog}(p))$ the state

$$|\Omega_{u,u'}\rangle = \frac{1}{p} \sum_{x,x'} \omega^{(ux^2 + u'x'^2) + \beta(ux + u'x')} |x\rangle|x'\rangle|ux^2 + u'x'^2\rangle|ux + u'x'\rangle$$ 

from $|\Phi\rangle$. 

\[2\]
Solution:
\[ |\psi_u \rangle \otimes |\psi_{u'} \rangle = \sum_{x, x'} \omega^{\alpha(ux^2 + u'x'^2) + \beta(ux + u'x')} |x \rangle |x' \rangle. \]

We add 2 ancilla register to obtain
\[ \sum_{x, x'} \omega^{\alpha(ux^2 + u'x'^2) + \beta(ux + u'x')} |x \rangle |x' \rangle |0 \rangle |0 \rangle. \]

The functions \((x, x') \rightarrow ux^2 + u'x'^2\) and \((x, x') \rightarrow ux + u'x'\) can be efficiently computed classically. Applying the quantum circuit version of those functions on registers 1, 2, 3 and 1, 2, 4 gives the state \(|\Omega \rangle\).

Question 4. We assume that, from \(|\Omega_{u, u'} \rangle\), we know how to construct the state
\[ |\xi \rangle = \frac{1}{p} \sum_{w_1, w_2 \in \mathbb{F}_p} \omega^{|w_1 + w_2|} |w_1 \rangle |w_2 \rangle. \]

Think of a way to recover \((\alpha, \beta)\) from the state \(|\xi \rangle\).

Solution: Apply \(QFT_p^\dagger\) on each register of \(|\xi \rangle\), the result is
\[ \frac{1}{p^2} \sum_{a, b, w_1, w_2} \omega^{w_1(a-\alpha)a} \omega^{w_2(b-\beta)b} |a \rangle |b \rangle = |\alpha \rangle |\beta \rangle. \]

BONUS Question 1 (Hard). Find a way to go from \(|\Omega \rangle\) to a state \(|\tilde{\xi} \rangle\) which is at a constant (non zero) distance in euclidian distance from \(|\xi \rangle\). Don’t go through all the details but show the main ideas to achieve this. You can start by rewriting
\[ |\Omega_{u, u'} \rangle = \sum_{w_1, w_2 \in \mathbb{F}_p} \sum_{(x, x') \in T_{w_1, w_2}} \nu_{x, x', w_1, w_2} \omega^{\alpha w_1 + \beta w_2} |x \rangle |x' \rangle |w_1 \rangle |w_2 \rangle, \]

where \(T_{w, w'} = \{(x, x') : (ux^2 + u'x'^2 = w_1) \land (ux + u'x' = w_2)\} \) and \(\nu_{x, x', w_1, w_2} \in \mathbb{C}\).
Exercise 2. Finding triangles in a graph

Consider an undirected graph $G$ on $n$ vertices $[n] = \{1, 2, \ldots, n\}$ whose access is given by a black-box function $f$ on $I = \{(i, j) : i, j \in [n] \text{ and } i \neq j\}$ such that $f(i, j) = 1$ if $(i, j)$ is an edge of $G$, and $f(i, j) = 0$ otherwise.

Let $m$ be the number of edges of $G$. We assume that $m \geq 1$.

Both $n$ and $m$ are given as input.

For simplicity, we will only consider the number of black-box accesses to $f$, that we call queries, and we will disregard any other complexity measures. If you apply Grover’s algorithm, define properly the classical functions on which you apply the algorithm.

Let $i, j, k \in [n]$ be pairwise distincts. We say that $(i, j, k)$ is a triangle of $G$ if $(i, j), (j, k)$ and $(k, i)$ are all edges of $G$.

**Question 5.** Give a simple quantum algorithm that outputs a triangle $(i, j, k)$ of $G$ with probability at least $9/10$ if there is any, and otherwise aborts, using $O(n^{3/2})$ queries to $f$.

**Solution:** Simply perform a Grover search on all possible triples $(i, j, k)$. There are $n^3$ of them, and checking one requires $3$ queries to $f$.

**Question 6.** Give a quantum algorithm that outputs an edge $(i, j)$ of $G$ with probability at least $9/10$, and otherwise aborts, using $O(n/\sqrt{m})$ queries to $f$.

**Solution:** Consider the following simple algorithm: Take at random a pair $(i, j)$ and check that it is an edge by querying $f$. Then the algorithm has query complexity $1$, and success probability $m/n^2$. Using amplitude amplification we get the required algorithm.

**Question 7.** Let $(i, j)$ be an edge of $G$. Give a quantum algorithm that outputs $k$ such that $(i, j, k)$ is a triangle of $G$ with probability at least $9/10$ if there is any, and otherwise aborts, using $O(\sqrt{n})$ queries to $f$.

**Solution:** Do a Grover search over the $n - 2$ possible values of $k$. Checking a $k$ requires $2$ queries to $f$.

**Question 8.** Give a quantum algorithm that outputs a triangle $(i, j, k)$ of $G$ with probability at least $1/m$ if there is any, and otherwise aborts, using $O(n/\sqrt{m} + \sqrt{n})$ queries to $f$.

**Solution:** Consider the following algorithm: (1) Search for an edge $(i, j)$; (2) Find for $k$ such that $(i, j, k)$ is a triangle of $G$, if there is any. The overall query complexity is $O(n/\sqrt{m} + \sqrt{n})$, and the success probability is at least $1/m$ when $G$ has at least one triangle.