**QCLG Exercise sheet 8**

# Part 1. Quantum algorithm for the discrete logarithm problem

Let $p$ be a prime number, $(\mathbb{Z}/p\mathbb{Z})^*$ the multiplicative group with elements in $\{1,\ldots,p-1\}$. Let $g$ be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. As a consequence, we have $g^{p-1}=1 \mod p$ and $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*,\ \exists!\ y \in \{0,\ldots,p-2\}, x = g^y \mod p$.

The discrete log problem is the following: let $x \in (\mathbb{Z}/p\mathbb{Z})^*$, find $y \in \{0,\ldots,p-2\}$ such that $x = g^y \mod p$.

For any number $N \in \mathbb{N}$, we assume we have a perfect quantum unitary operation that performs the quantum Fourier transform $QFT_N$ satisfying that $\forall k \in \{0,\ldots,N-1\}$,

$$QFT_N(|k\rangle) = \frac{1}{\sqrt{N}}\sum_{a=0}^{N-1}\omega_N^{ak}|a\rangle .$$

where $\omega_N := e^{\frac{2i\pi}{N}}$.

Let $V$ be the quantum unitary operator satisfying $V(|a\rangle|b\rangle|0\rangle = |a\rangle|b\rangle\left|g^a x^{-b} \mod p\right\rangle$. The goal of this exercise is to analyze the following quantum algorithm for the discrete logarithm problem.

Quantum algorithm for discrete logarithm.

We start with an input $x \in (\mathbb{Z}/p\mathbb{Z})^*$. We want to find $y \in \{0,\ldots,p-2\}$ such that $x = g^y \mod p$.

1. Start from three registers initialized at $|0\rangle$.
2. Apply $QFT_{p-1}$ on each of the two first registers.
3. Apply the unitary operation $V$ on all the registers.
4. Measure the third register in the computational basis *i.e.* the basis $\{|0\rangle,\ldots,|p-1\rangle\}$. Let $k$ be the output.
5. Apply the Fourier transform $QFT_{p-1}$ on the first register and second register.
6. Measure both registers in the computational (standard) basis to get some outcome $(l_1,l_2)$.
7. Conclude

Let $|\phi_i\rangle$ the state of the algorithm after step $i$.

**Exercise 1.** *Write $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle$. Let $Z_c$ be the following set*

$$Z_c := \{(a,b) \in \{0,\dots,p-2\} \times \{0,\dots,p-2\} : (a - by \mod (p-1)) = c\}.$$

*Show that $|\phi_3\rangle$ can be written*

$$|\phi_3\rangle = \frac{1}{\sqrt{p-1}} \sum_{c\in\{0,\dots,p-2\}} \frac{1}{\sqrt{p-1}} \sum_{a,b\in Z_c} |a\rangle |b\rangle |g^c \mod p\rangle .$$

*Write therefore $|\phi_4\rangle$ as a function of $c$ depending on the measured outcome $g^c$.*

**Exercise 2.** *For a fixed $k$ (and hence $c$), write the state $|\phi_5\rangle$. Show that after step 6, we obtain a random couple $(l_1, l_2)$ satisfying*

$$l_1 y + l_2 = 0 \mod (p-1).$$

*Conclude when $l_1$ is invertible in the ring $\mathbb{Z}/(p-1)\mathbb{Z}$. What would you do if this is not the case?*

# Part 2. Finding a hidden parabola in a function.

Suppose we are given a black-box function $f_{\alpha,\beta} : \mathbb{F}_p^2 \to \mathbb{F}_p$, 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 $\omega = e^{\frac{2i\pi}{p}}$. 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.

**Exercise 1.** *Show that after step 4 the above procedure creates the state*

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

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

**Exercise 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?*

**Exercise 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 $O(polylog(p))$ the state*

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

*from $|\Phi\rangle$.*

**Exercise 4.** *We **assume** that, from $|\Omega_{u,u'}\rangle$, we know how to construct the state*

$$|\xi\rangle = \frac{1}{p} \sum_{w_1, w_2 \in \mathbb{F}_p} \omega^{\alpha w_1 + \beta w_2} |w_1\rangle |w_2\rangle .$$

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