INF587 Exercise sheet 6

Exercise 1 (Probability of good approximation in phase estimation)**.** *Recall that before measuring the first t qubits in phase estimation we have the following quantum state*

$$|\psi\rangle \overset{def}{=} \frac{1}{\sqrt{2^t}} \sum_{k,\ell=0}^{2^{t-1}} e^{2i\pi\ell\left(\varphi-\frac{k}{2^t}\right)} |k\rangle |u\rangle$$

Let $b \in [\![0, 2^t - 1]\!]$ be the best t bits approximation of φ, namely

$$\delta \overset{def}{=} \varphi - \frac{b}{2^t} \in [0, 2^{-t}]$$

1. *Let α_j be the amplitude of $(b + j \textbf{ mod } 2^t)$ in the first register. Show that*

$$|\alpha_j| \leq \frac{2}{2^t \left|1 - e^{2i\pi(\delta - j/2^t)}\right|}$$

2. *Using that $|1 - e^{i\theta}| \geq 2|\theta|/\pi$ when $-\pi \leq \theta \leq \pi$, deduce that when $-2^{t-1} < j \leq 2^{t-1}$*

$$|\alpha_j| \leq \frac{1}{2\left(2^t\delta - j\right)}$$

3. *Let m be the outcome when measuring the first register of $|\psi\rangle$. Deduce that*

$$\mathbb{P}\left(|m - b| > \alpha\right) \leq \frac{1}{2(\alpha - 1)}$$

Hint: *you can use the inequality* $\sum_{\ell=A}^{B} \frac{1}{\ell^2} \leq \int_A^B \frac{dx}{x^2} \leq \frac{1}{2A}$ *where* $A, B > 0$.

Exercise 2 (Computing the eigenvector in the phase estimation for order finding)**.** *Recall that we work in the space of $\lceil \log N \rceil$ qubits. Let $x \in [\![0, N - 1]\!]$ where* $\gcd(x, N) = 1$ *and r be the (multiplicative) order of x. Let,*

$$|u_s\rangle \overset{def}{=} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2i\pi sk}{r}} \left|x^k \bmod N\right\rangle$$

Show that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$$

where $|1\rangle$ denotes the quantum state which represents the integer 1 *(recall that we naturally identify integers $y \in [\![0, 2^{\lceil \log N \rceil} - 1]\!]$ with $\lceil \log N \rceil$ qubits via their binary decomposition).*

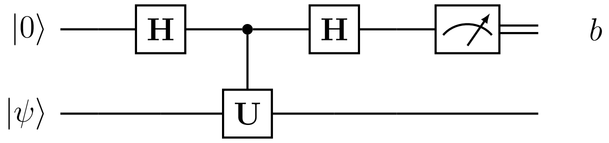
Exercise 3 (Phase estimation with a superposition of eigenvectors)**.**

1. *Recall the quantum circuit of phase estimation before applying* $\mathbf{QFT}^{-1}_{\mathbb{Z}/2^t\mathbb{Z}}$*.*

2. *Suppose that you feed as input the following quantum state to the above quantum circuits*
$$\left|0^t\right\rangle \otimes \sum_u c_u \left|u\right\rangle$$
where $|u\rangle$ *is an eigenvector associated to the eigenvalue* φ_u *and then you apply* $\mathbf{QFT}^{-1}_{\mathbb{Z}/2^t\mathbb{Z}} \otimes \mathbf{I}$*. What is the resulting quantum state?*

3. *Suppose that,*
$$t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right)\right\rceil$$
Deduce that performing a measurement of the first register gives with probability at least $(1-\varepsilon)$ *the first* n *bits of* φ_u *where* u *has been picked according to* $|c_u|^2$*.*

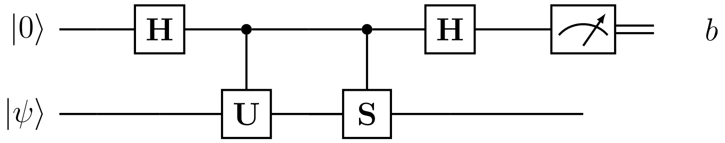
Exercise 4 (The original algorithm for phase estimation: Kitaev's algorithm)**.** *The goal of this exercise is to describe an algorithm for phase estimation that doesn't use the* $\mathbf{QFT}_{\mathbb{Z}/2^t\mathbb{Z}}$*. You are given a unitary* $\mathbf{U}$ *and a quantum state* $|\psi\rangle$ *which is an eigenstate of* $\mathbf{U}$ *of eigenvalue* $e^{i\theta}$ *for* $\theta \in [0, 2\pi)$*. This means we have the guarantee that* $\mathbf{U}|\psi\rangle = e^{i\theta}|\psi\rangle$*. The goal is to find* θ*. Consider the following circuit:*



1. *What is the probability* P_0 *of outputting* $b = 0$*, as a function of* θ*?*

2. *Argue that whatever is the measurement outcome, the state* $|\psi\rangle$ *remains unchanged. Show how by repeating the circuit, you can obtain an approximation of* P_0*. Show that knowing* P_0 *will still give 2 possible solutions for* θ*.*

3. *Find a way to distinguish between these two cases. One can study the circuit*



where $\mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

Exercise 5 (More about the *Abelian* Hidden Subgroup Problem)**.** *The following problem, known as discrete logarithm, is fundamental in public-key cryptography. The security of many cryptosystems that are currently deployed relies on its hardness.*

- **Input:** *a prime number* p *and a generator* g *of the group* $(\mathbb{Z}/p\mathbb{Z})^\star$ *which denotes* $\mathbb{Z}/p\mathbb{Z}\backslash\{0\}$ *equipped with the usual multiplication of integers modulo* p. *Furthermore it is given* $\alpha \overset{def}{=} g^a$ *where* $a \in [\![0, p-1]\!]$.
- **Output:** a

Our aim in this exercise is to study classical and quantum algorithms to solve this problem. As we will see the discrete logarithm problem is an instantiation of HSP *in the Abelian case.*

1. *Let us admit that* $(\mathbb{Z}/p\mathbb{Z})^\star$ *(equipped with the multiplication* mod p*) is a group for the multiplication. But why do each element admit an inverse? Given a group element, is it easy to (classically) compute its inverse?*

2. *Our aim in this question is to study a non-trivial algorithm to solve the discrete logarithm (known as* **baby-step giant-step***)*

   (a) *Let* $m \in [\![1, p]\!]$ *and* (q, r) *be the result of the Euclidean division of* a *by* m. *Show that*

   $$g^r = \alpha (g^{-m})^q$$

   (b) *Let us consider the following algorithm (baby-step giant-step)*

```
 Input: $g, \alpha$
Output: $a$ be such that $g^a = \alpha$.
        1. For all $r \in [\![0, m-1]\!]$:
                 $g^r$ and store the pair $(r, g^r)$ in a table
        2. Compute $g^{-m}$
        3. Set $\gamma \leftarrow \alpha$
        4. For all $0 \leq i \leq p$:
           (a) Check to see if $\gamma$ is the second component ($g^r$) of any pair in the
               table
```

(b) *If so, return* $im + r$
(c) *If not,* $\gamma \leftarrow \gamma g^{-m}$

Show that the algorithm is correct. What is the running time? What is the optimal choice for m*?*

(c) *In conclusion, in what amount of time can we solve classically the discrete logarithm problem?*

3. *Consider the group* $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$ *and the function*

$$f : (x, y) \in \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \longmapsto g^x \alpha^{-y} \in (\mathbb{Z}/p\mathbb{Z})^\star$$

It the function f *efficiently computable? Give the associated cost. Show that* f *hides a subgroup* H *of* $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$ *that you describe.*

4. *The group* G *and the function* f *defined in the previous question give an instantiation of* HSP *in the Abelian case. Therefore we can apply Kitaev's algorithm. What is the output of this algorithm in this case?*

5. *What do you deduce?*