INF587 Exercise sheet 5

Exercise 1. *Consider a function*

$$f : \{0,1\}^2 \to \{0,1\}$$

for which there exists a unique $\mathbf{x}_1$ *such that* $f(\mathbf{x}_1) = 1$. *Apply one step of Grover's algorithm (i.e. construct the original state* $|\psi\rangle$ *and then perform a reflexion over* $|\psi_{\text{bad}}\rangle$ *and then over* $|\psi\rangle$*). More precisely:*

1. *Write the different states* $|\psi_{\text{good}}\rangle, |\psi_{\text{bad}}\rangle, |\psi\rangle$ *as defined in the lecture in this setting.*

2. *Write* $|\psi\rangle = \cos(\theta)\,|\psi_{\text{bad}}\rangle + \sin(\theta)\,|\psi_{\text{good}}\rangle$. *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 that the algorithm succeeds with probability* 1 *after* 1 *step of Grover's algorithm.*

Exercise 2 (Grover's algorithm when the number of solution is unknown)**.** *Our aim in this exercise is to give a variation of Grover's algorithm that can find solutions in* expected *time* $\sqrt{\frac{N}{t}}$ *even when the number of solutions* t *is unknown. This exercise describes the idea of the following article* ***https://arxiv.org/pdf/quant-ph/9605034.pdf****. Roughly speaking, the idea basically consists in running Grover's algorithm with exponentially increasing guesses for the number of iterations.*

Recall that we study the following problem:

- **Input***: a function* $f : \{0,1\}^n \longrightarrow \{0,1\}$,
- **Goal***: find* $\mathbf{x} \in \{0,1\}^n$ *be such that* $f(\mathbf{x}) = 1$.

Let,

$$t \stackrel{def}{=} \sharp \left\{ \mathbf{x} \in \{0,1\}^n \,:\, f(\mathbf{x}) = 1 \right\}.$$

1. *Let* t *be the unknown number of solutions and let* $\theta \stackrel{def}{=} \arcsin\sqrt{\frac{t}{2^n}}$. *Let* j *be chosen uniformly at random in* $[\![0, m-1]\!]$. *Show that the probability* P_m *to measure a solution after* j *iterations of Grover's algorithm verifies*

$$P_m \geq \frac{1}{4} \quad \textit{when } m \geq \frac{1}{\sin 2\theta}$$

Hint: *recall that* $\sin^2\alpha = \frac{1-\cos 2\alpha}{2}$ *and* $\sin(2\alpha) = 2\cos(\alpha)\sin(\alpha)$

2. *Let j be chosen uniformly at random in $[\![0, m-1]\!]$. Show that j is expected to be equal to $(m-1)/2$, namely:*

$$\mathbb{E}(j) = \frac{m-1}{2}$$

3. *Let $m_0 \stackrel{def}{=} \frac{1}{\sin 2\theta}$. Let us consider the following algorithm:*

   1. *$u \stackrel{def}{=} 0$, $\lambda \stackrel{def}{=} \frac{6}{5}$ and $m \stackrel{def}{=} \lambda^{\lceil \log_\lambda m_0 \rceil}$.*
   2. *Pick j uniformly at random in $[\![0, m-1]\!]$.*
   3. *Apply j iterations of Grover's algorithm starting from initial state $|\psi\rangle \stackrel{def}{=} \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \, |f(\mathbf{x})\rangle$.*
   4. *Measure, if the last register is one, exit.*
   5. *Otherwise, set m to $\min\left(\sqrt{2^n}, \lambda m\right)$ and go back to Step 2.*

   Show that the expected number of iterations of this algorithm before ending and therefore finding a solution is a

$$O\left(m_0\right).$$

4. *Suppose that the number t of solution is $\leq \frac{3}{4}2^n$ and $t > 0$. Give an algorithm that finds a solution in expected time $O\left(\sqrt{\frac{2^n}{t}} \max\left(n, T_f\right)\right)$ where T_f is the classical running time of f.*

5. *How treating the case $t > \frac{3}{4}2^n$ or $t = 0$? In particular, what is the expected running time of the algorithm when there are no solutions?*

Exercise 3. *Let,*

$$f : \{1, \ldots, n\} \to \{1, \ldots, m\}$$

be a function classically computable in time T_f. Construct a quantum algorithm using Grover's algorithm that finds the minimum of f in time $O(\sqrt{n}\log_2(m)\max(\log n, T_f))$.

Hint: *You can consider different thresholds T and try to find values x such that $f(x) \leq T$, and use Grover's algorithm without proving it.*

Exercise 4 (Grover with probability one)**.** *We claimed during the lecture (without proof) that Grover's algorithm can be tweaked to work with probability* 1 *if we know the number of solutions exactly. The goal of this exercise is to provide such an exact algorithm. Roughly, the idea is to increase the dimension (adding a qubit!) in order to slightly change the angle* θ *of Grover's algorithm in order to have a "perfect" number of iterations, namely for which it is not necessary to round up.*

Let,

$$f : \{0,1\}^n \to \{0,1\} \textit{ such that there exists a } \text{unique } \mathbf{x}_0 \textit{ verifying } f(\mathbf{x}_0) = 1.$$

Our aim is to recover $\mathbf{x}_0$ with probability one.

1. *Give the success probability of the basic version of Grover's algorithm after k iterations.*

2. *Suppose that the optimal number of iterations* $\widetilde{k} = \frac{\pi}{4\arcsin\left(\frac{1}{\sqrt{2^n}}\right)} - \frac{1}{2}$ *is not an integer. Show that if we round* $\widetilde{k}$ *up to the nearest integer, doing* $\lceil \widetilde{k} \rceil$ *iterations, then the algorithm will have success probability strictly less than* 1*.*

3. *Define now the following function:*

$$g : \mathbf{y} \in \{0,1\}^{n+1} \longmapsto \begin{cases} f(\mathbf{x}) & \textit{if } \mathbf{y} = (\mathbf{x}|0) \\ 0 & \textit{otherwise.} \end{cases}$$

   Show how you can implement the following $(n+1)$*-qubit unitary*

$$\mathbf{S}_g : |\mathbf{y}\rangle \mapsto (-1)^{g(\mathbf{y})} |\mathbf{y}\rangle$$

   using one query to f *(of the usual form* $\mathbf{U}_f : |\mathbf{x}, b\rangle \mapsto |\mathbf{x}, f(\mathbf{x}) \oplus b\rangle$*) and a few elementary gates.*

4. *Let* $\gamma \in [0, 2\pi)$ *and let* $\mathbf{U}_\gamma \stackrel{def}{=} \begin{pmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{pmatrix}$ *be the corresponding rotation matrix. Let*

$$\mathbf{A} = \mathbf{H}^{\otimes n} \otimes \mathbf{U}_\gamma$$

   be an $(n+1)$*-qubit unitary. What is the probability (as a function of* γ*) that measuring the state* $\mathbf{A}\,|0^{n+1}\rangle$ *in the computational basis gives a solution* $\mathbf{y} \in \{0,1\}^{n+1}$ *such that* $g(\mathbf{y}) = 1$*?*

5. *Give a quantum algorithm that finds the unique solution* $\mathbf{x}_0$ *with probability one using* $O(\sqrt{N})$ *queries to* f*.*

Exercise 5. *Consider an efficiently computable function (to simplify formulas suppose that* $T_f = 1$*)* $f : \{0, \dots, 2^n - 1\} \longrightarrow \{0, 1\}$*. We also consider a string* $s = s_0, \dots, s_{S-1} \in \{0, 1\}^S$*. The goal is to find* S *consecutive values of* $f(x)$ *that are equal to* s*. More formally, we want to find* $x \in \{0, \dots, 2^n - S\}$ *st.* $f(x) = s_0$*,* $f(x + 1) = s_1, \dots, f(x + S - 1) = s_{S-1}$*. 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* $g : \{0, \dots, S - 1\} \longrightarrow \{0, 1\}$ *such that* $g(i) = s_i$*.*
   (a) *Assume you have access to a version of Grover's algorithm, that outputs a solution to a search problem for a function* $\ell : \mathcal{I} \longrightarrow \{0, 1\}$ *if there is a solution and* $\perp$ *if there is no solution. Assume also that this routine works with probability* 1 *and takes time* $O\left(\sqrt{\sharp\mathcal{I}}\right)$*. Construct an algorithm* $\mathcal{A}$ *that for any input* x*, outputs* 1 *if* $x = x_0$ *and* 0 *otherwise in time* $O\left(\sqrt{S}\right)$*.*
   (b) *Construct a quantum algorithm that finds* x_0 *in time* $O(\sqrt{S}2^{n/2})$*.*

Comment: this exercise illustrates that amplitude amplification can provide an exponential improvement over Grover's algorithm.

Exercise 6. *Let* $f : \{0, 1\}^n \to \{0, 1\}^n$ *that we can query in the usual way. We are promised that this function is 2-to-1: for all* $\mathbf{x} \in \{0, 1\}^n$ *there exists a unique* $\mathbf{y} \neq \mathbf{x}$ *such that* $f(\mathbf{x}) = f(\mathbf{y})$*.*

1. *Choose* S *uniformly at random among the sets of size* s *in* $\{0, 1\}^n$*. What is the expected number of solutions in* S*?*
2. *Give a classical randomized algorithm that finds a collision with probability* $\geq 1/2$ *using* $O\left(\sqrt{2^n}\right)$ *queries to* f*.*
3. *Give a quantum algorithm that finds a collision with* $O\left(\sqrt{2^n}\right)$ *queries to* f*.*

4. *Give a quantum algorithm that finds a collision using $O\left(2^{n/3}\right)$ queries to f. In this question you recover the algorithm given in* `https://arxiv.org/pdf/quant-ph/9705002.pdf`.

Hint: *Combine both classical and quantum approaches*

Exercise 7 (Approximating Unitary Operators)**.** *Let* $\mathbf{U}$ *and* $\mathbf{V}$ *be two unitaries. Let,*

$$E(\mathbf{U},\mathbf{V}) = \max_{|\psi\rangle\,:\,\||\psi\rangle\|=1} \|(\mathbf{U}-\mathbf{V})\,|\psi\rangle\,\|$$

where $\|\cdot\|$ *denotes the norm of the considered Hilbert space for quantum states.* $E(\mathbf{U},\mathbf{V})$ *is known as the operator norm of* $\mathbf{U}-\mathbf{V}$.

The distance between two unitaries $\mathbf{A}$ *and* $\mathbf{B}$ *is defined as* $E\left(\mathbf{A},\mathbf{B}\right)$.

1. *Let* M *be a* POVM *element associated with the measurement, and let* $P_{\mathbf{U}}$ *(or* $P_{\mathbf{V}}$*) be the probability of obtaining the corresponding measurement outcome if the operation* $\mathbf{U}$ *(or* $\mathbf{V}$*) was performed. Show that*

$$|P_{\mathbf{U}} - P_{\mathbf{V}}| \le 2E(\mathbf{U},\mathbf{V})$$

2. *Show that*

$$E(\mathbf{U}_m\mathbf{U}_{m-1}\cdots\mathbf{U}_1, \mathbf{V}_m\mathbf{V}_{m-1}\cdots\mathbf{V}_1) \le \sum_{i=1}^{m} E(\mathbf{U}_i,\mathbf{V}_i)$$

3. *Deduce that if* $\mathbf{A},\mathbf{U},\mathbf{V}$ *are unitaries, then*

$$|P_{\mathbf{AU}} - P_{\mathbf{AV}}| \le 2E\left(\mathbf{U},\mathbf{V}\right)$$

4. (*i*) *What is the distance between the* 2×2 *identity matrix and the phase-gate* $\begin{pmatrix}1 & 0\\ 0 & e^{i\varphi}\end{pmatrix}$*?*

   (*ii*) *What is the distance between the* 4×4 *identity matrix and the controlled version of the phase gate of* (*i*)*?*

   (*iii*) *What is the distance between the* $2^n\times 2^n$ *identity matrix* $\mathbf{I}_{2^n}$ *and the controlled phase gate of* (*ii*) *tensored with* $\mathbf{I}_{2^{n-2}}$*?*

(iv) *Give a quantum circuit with $O(n \log n)$ elementary gates that has distance less than C/n (for some constant C) from the Fourier transform* $\mathbf{QFT}_{\mathbb{Z}/2^n\mathbb{Z}}$.

Hint: *you can use that* $\cos \varepsilon \underset{\varepsilon \to 0}{=} 1 - \frac{x^2}{2}(1 + O(1))$

Exercise 8 (About characters).

Let G be a finite group.

1. *Prove that for any character $\chi \in \widehat{G}$,*

$$\sum_{g \in G} \chi(g) = \begin{cases} \sharp G & \text{if } \chi = 1 \\ 0 & \text{otherwise.} \end{cases}$$

2. *How do you deduce from that*

$$\sum_{g \in G} \chi_x(g)\overline{\chi_y}(g) = \begin{cases} \sharp G & \text{if } \chi_x = \chi_y \\ 0 & \text{otherwise.} \end{cases}$$

3. *Consider the function f_x*

$$\begin{aligned} f_g : \widehat{G} &\longrightarrow G \\ \chi &\longmapsto \chi(g), \text{ such that} \end{aligned}$$

What can you say about f_g?

4. *How can you deduce from the previous point that we also have*

$$\sum_{\chi \in \widehat{G}} \chi(x)\overline{\chi}(y) = \begin{cases} \sharp G & \text{if } x = y \\ 0 & \text{otherwise.} \end{cases}$$

5. *Let H be a subgroup of G. Show that*

$$\sum_{h \in H} \chi_g(h) = \begin{cases} \sharp H & \text{if } g \in H^\perp \\ 0 & \text{otherwise.} \end{cases} \quad \text{and} \quad \sum_{h^\perp \in H^\perp} \chi_g(h^\perp) = \begin{cases} \sharp H^\perp & \text{if } g \in H \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 9 (Poisson summation formula and application).

1. *Let G be a finite group and H be a subgroup. Show the Poisson summation formula, for any function $f : G \longrightarrow \mathbb{C}$,*

$$\frac{1}{\sqrt{\sharp H}} \sum_{h \in H} f(h) = \frac{1}{\sqrt{\sharp H^{\perp}}} \sum_{h^{\perp} \in H^{\perp}} \widehat{f}(h)$$

You can admit that $\sharp H^{\perp} \, \sharp H = \sharp G$.

2. *Recall that the characters of $\mathbb{Z}/2^n\mathbb{Z}$ are given by the χ_x's where $\chi_x(y) \stackrel{def}{=} e^{-\frac{2i\pi xy}{2^n}}$. Let $i \in [\![0, n-1]\!]$*

$$(2^i) \stackrel{def}{=} \left\{ x2^i \,:\, x \in \mathbb{Z}/2^n\mathbb{Z} \right\}$$

is the subgroup of $\mathbb{Z}/2^n\mathbb{Z}$ generated by 2^i. Determine $(2^i)^{\perp}$.

3. *Given a function $f : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{C}$ which is 2^i-periodic. Show that it vanishes on $(2^i)^{\perp}$.*

4. *Suppose that you have $\widehat{f}$ for free. Is it easy to find its period (here 2^i)? What do you conclude?*

Exercise 10. *Is computing the Quantum Fourier Transform in $\mathbb{Z}/2^n\mathbb{Z}$ or $\mathbb{F}_2^n$ helps to compute the classical Fourier transform?*