# TUTORIAL 8

## 1 Minimum of a List

You have a set of $N$ numbers ($N$ can be written on $n$ bits) $x_0, \dots, x_{N-1}$ than can be encoded on $b$ bits and an access to a gate $U_x|i\rangle|y\rangle \to |i\rangle|y \oplus x_i\rangle$. We denote $[N] = \{0, \dots, N-1\}$.

In the following, we are going to use the "unknown target" version of Grover algorithm: UNK-GROVER. This is a version of Grover that finds a marked element in a list of $N$ elements, and makes $O(\sqrt{N/r})$ queries to the elements of the list where $r$ is the (unknown) number of marked elements. UNK-GROVER succeeds with probability $\geq 2/3$ (that we can amplify).

1. Let $i \in [N]$. Explain how to adapt UNK-GROVER to find $j \in [N]$ such that $x_i < x_j$ if it exists. How many queries to $U_x$ does your algorithm makes?

2. We are going to study the following algorithm:

**Algorithm 1** Find-Min

```
i ← U([N]).
while 1 do
    Find j such that x_j < x_i with UNK-GROVER.
    If it is impossible, return i.
    Else, i ← j.
end while
```

   (a) How many calls to $U_x$ makes algorithm 1 in the worst case?

   (b) Show that if $x_j$ is the element of rank $r$, the probability that $j$ is picked from the algorithm at some point is $1/r$. *Hint: induction on $N$.*

   (c) Compute an upper bound on the expected number of queries to $U_x$ made by algorithm 1.

   (d) Conclude by proposing a quantum algorithm doing $O(\sqrt{N})$ calls to $U_x$ that find a minimum in the $x_i$ with probability $\geq 2/3$. *Hint: Markov.*

## 2 QMA, quantum generalization of NP

We consider the following complexity class: we say that a promise problem $L = (L_{\text{YES}}, L_{\text{NO}})$ is in the class **QMA** if there exist a polynomial-time classical algorithm $\mathcal{C}$ such that $\mathcal{C}(x)$ is a quantum circuit realizing $U_x$, such that it satisfies the two following properties:

- **Completeness:** $x \in L_{\text{YES}} \Rightarrow \exists|\psi\rangle$ such that measuring the first qubit of $U_x|\psi\rangle \otimes |0\rangle$ gives $1$ with probality $\geq \frac{2}{3}$

- **Soundness:** $x \in L_{\text{NO}} \Rightarrow \forall|\psi\rangle$, measuring the first qubit of $U_x|\psi\rangle \otimes |0\rangle$ gives $1$ with probality $\leq \frac{1}{3}$

1. Show that **NP** $\subseteq$ **QMA**.

2. Show that **BQP** $\subseteq$ **QMA**.

3. Call **QMA**$[c(n), s(n)]$ the variant of **QMA** where the completeness error $\frac{2}{3}$ is replaced by $c(n)$ and the soundness error $\frac{1}{3}$ is replaced by $s(n)$. Can you prove that **QMA** $=$ **QMA**$[c(n), s(n)]$ with $c(n) - s(n) \geq \frac{1}{p(n)}$ for a positive polynomial $p$? We will nonetheless assume this result for this exercise.

4. Recall that the $k$-LOCAL HAMILTONIAN problem takes as input the description of $H = \sum_{j=1}^{r} H_j[S_j]$ acting on $(\mathbb{C}^2)^{\otimes n}$, with $H_j$ $k$-local and $\mathrm{sp}(H_j) \subseteq \{0, 1\}$ (so $H_j$ is a projector), and parameters $0 < a < b$ with $b - a \geq \frac{1}{\mathrm{poly}(n)}$. The goal is to output $1$ if $\lambda_{\min}(H) \leq a$ and $0$ if $\lambda_{\min}(H) \geq b$. We want to show that $k$-LOCAL HAMILTONIAN is in **QMA**. We consider the following quantum algorithm:

   - Sample $j$ uniformly in $\{1, \ldots, r\}$
   - We can decompose $H_j = \sum_{i=1}^{n_j} |b_i^j\rangle\langle b_i^j|$, with $(|b_i^j\rangle)_{i\in[n]}$ basis of $(\mathbb{C}^2)^{\otimes n}$. Apply the change of basis $V_j$ such that $V_j^\dagger = (|b_i^j\rangle)_{i\in[n]}$, measure in the standard basis. If the output $i \notin [n_j]$, then output $1$; else output $0$.

   (a) Justify why we can construct such a quantum algorithm with a polynomial-size quantum circuit using ancillas and measuring only its first output.

   (b) On input $|\eta\rangle$, first compute the probability that given $j$, you get $1$. Then prove that the global probability of getting $1$ is $1 - \frac{\langle \eta | H | \eta \rangle}{r}$.

   (c) Find a lower bound on the probability of outputting $1$ in the completeness part of **QMA** for the $k$-LOCAL HAMILTONIAN using the certificate $|\eta\rangle$, where $|\eta\rangle$ is an eigenvector of $H$ for eigenvalue $\lambda_{\min}(H)$, under the hypothesis that $\lambda_{\min}(H) \leq a$.

   (d) Find an upper bound on the probability of outputting $1$ in the soundness part of **QMA** for the $k$-LOCAL HAMILTONIAN under the hypothesis that $\lambda_{\min}(H) \geq b$.

   (e) Conclude.

*Remark.* The $k$-LOCAL HAMILTONIAN is in fact **QMA**-complete for $k \geq 2$. $\square$

## 3 Matrix Exponentials

1. Compute $\exp(iX)$, $\exp(iZ)$, $\exp(iX) \cdot \exp(iZ)$, $\exp(i(X + Z))$.

2. **Tail-cut of the matrix exponential**. Assume that $A$ is a matrix of norm $\leq 1$. Let $0 < \varepsilon < 0.99$ and $t > 0$. Show that there exists a constant $c > 0$ independant of $A, \varepsilon$ and $t$ such that:

$$\left\| \sum_{k=0}^{c\cdot(t+\log(1/\varepsilon))} \frac{(itA)^k}{k!} - \exp(itA) \right\| < \varepsilon \,.$$

   You can use freely that $k! \leq \left(\frac{k}{e}\right)^k$.

3. What tail-cut bound do you have to take if $\|A\| \leq 1$ is not supposed anymore?