TUTORIAL 7

1 Assignment 5

The objective of this problem is to show that the phase estimation algorithm can still return a good approximation if the angle θ is not of the form $\theta = \frac{j}{2^m}$.

1. Show that after applying the phase estimation circuit described in class, we obtain (in the first register) the state
$$\frac{1}{2^m} \sum_{j=0}^{2^m-1} \left(\sum_{k=0}^{2^m-1} e^{2\pi i k(\theta - j2^{-m})} \right) |j\rangle \ .$$
2. We now measure this state in the standard basis. Compute the probability p_j of obtaining outcome j.
3. Suppose we are aiming for a precision of $t < m$ bits, i.e., we would like the outcome to be some j such that $|\theta - j2^{-m}| \leq 2^{-t-1}$ or $|\theta - j2^{-m}| \geq 1 - 2^{-t-1}$. Compute a lower bound on the probability of obtaining such an outcome. The bound should be such that if t is fixed and m grows, the probability of success goes to 1. For this you may use the following inequality without proof: for $\gamma \in [-\pi, \pi]$, $|1 - e^{i\gamma}| \geq \frac{2}{\pi}|\gamma|$.
Hint: Start the analysis by computing the probability of obtaining a wrong output j.

2 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 ≤ 1. Let $0 < \varepsilon < 0.99$ and $t > 0$. Show that there exists a constant $c > 0$ independant of A, ε 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?

3 Amplitude Amplification

Consider the following problem. Given a boolean function $f : \{0,1\}^n \to \{0,1\}$, we assume we have access to a unitary query oracle Z_f such that $Z_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$. We suppose we have a quantum circuit $\mathcal{A}$ without intermediate measurements (so $\mathcal{A}$ is a unitary) such that when we measure $\mathcal{A}|0^n\rangle$ in the computational basis, we have that $\mathbb{P}(\text{output} \in f^{-1}(1)) = p \in (0,1)$.

1. Classicaly, how many calls to $\mathcal{A}$ do you need to make on average to get an element of $f^{-1}(1)$?

   The *amplitude amplification* algorithm aims at finding an element of $f^{-1}(1)$ with high probability. It depends on a parameter k wich will be defined later, and works in the following way:

   (a) Setup the starting state $|U\rangle = \mathcal{A}|0^n\rangle$.

   (b) Repeat the following steps k times:

      i. Apply Z_f.

      ii. Apply $\mathcal{A}R\mathcal{A}^{-1}$, where $R = 2|0^n\rangle\langle 0^n| - I_{2^n}$ is the reflexion through $|0^n\rangle$.

   (c) Measure in the standard basis and check that $f(\text{output}) = 1$.

2. Recall why we can construct an efficient circuit computing $\mathcal{A}^{-1}$.

3. Find orthogonal states $|G\rangle$ and $|B\rangle$ such that $|U\rangle = \sqrt{p}|G\rangle + \sqrt{1-p}|B\rangle$.

4. In span$(|G\rangle, |B\rangle)$, describe the action of Z_f and $\mathcal{A}R\mathcal{A}^{-1}$. Draw a picture of what happens.

5. Find k such that the *amplitude amplification* algorithm works with high probability. What is its complexity? Compare to the classical strategy.

6. Show that Grover's algorithm is a particular case of amplitude amplification for good Z_f and $\mathcal{A}$.