TUTORIAL 7

1 Homework 6

1. Using Grover's algorithm, design a quantum circuit deciding SATISFIABILITY with a size $O(2^{n/2}poly(|\varphi|))$ where φ is a boolean formula of size $|\varphi|$ and with n input variables.
2. (Bonus) Let B be a "box gate" on 1 qubit, where there are two possibilities:
   - **NO BOMB**: $B = I$.
   - **BOMB**: B measures in the standard basis. If the output state is $|1\rangle$, the bomb explodes. If the output state is $|0\rangle$, B returns $|0\rangle$.

   Let $\varepsilon > 0$. Design a quantum algorithm that determine if B is a bomb or not with probability of the bomb exploding $< \varepsilon$ and with proability of being wrong $< \varepsilon$.

2 Unitary Approximation

The goal of the exercise is to define what are approximations of unitaries, and show that it is relevant in the sense that it will give roughly the same outcomes when composed and measured.

Recall that the norm of an operator A (the so-called *operator norm*) is defined as:

$$\|A\| := \sup_{|\psi\rangle \neq 0} \frac{\|A|\psi\rangle\|_2}{\||\psi\rangle\|_2} .$$

Furthermore, we will say that the unitary $\tilde{U}$ approximates U with precision δ if $\|\tilde{U} - U\| \leq \delta$.

1. Show that $\|\cdot\|$ is indeed a norm, and furthermore that it satisfies $\|AB\| \leq \|A\|\|B\|$.
2. Show that if $\|\tilde{U} - U\| \leq \delta$, then $\|\tilde{U}^{-1} - U^{-1}\| \leq \delta$ where U and $\tilde{U}$ are unitaries.
3. Show that if each U_i is approximated by $\tilde{U}_i$ with precision δ_i, then:
   $\|\tilde{U}_L\tilde{U}_{L-1}\dots\tilde{U}_2\tilde{U}_1 - U_LU_{L-1}\dots U_2U_1\| \leq \sum_{j=1}^{L}\delta_j$.
4. We say that U computes a binary function $F(x)$ with precision ε if $\forall x \in \{0,1\}^n, |\langle F(x)|U|x\rangle|^2 \geq 1 - \varepsilon$. Show that if that U is approximated by $\tilde{U}$ with precision δ, then $\tilde{U}$ computes $F(x)$ with precision $\epsilon + 2\delta$. *Hint:* Note that for an operator A, you have $|\langle x|A|x\rangle| \leq \|A\|$.

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 $\mathbb{P}\left(\text{output} \in f^{-1}(1)\right) = p \in (0,1)$.

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 $\mathcal{A}$.

4 List-min

You have a set of N numbers (N can be written on n bits) $X_0, \ldots, X_{N-1}$ 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 $[N] = \{0, \ldots, N-1\}$.

1. Let $i \in [N]$. Explain how to adapt the Grover algorithm to find $j \in [N]$ such that $X_i < X_j$ if it exists. How many queries to U_X do your algorithm makes ? What is its failing probability?

2. We are going to study the following algorithm:

Algorithm 1 Find-Min

$i \leftarrow U([N])$.
while 1 **do**
  Find j such that $X_j < X_i$ with Grover.
  If it is impossible, return i.
  Else, $i \leftarrow j$.
end while

(a) How many calls to 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*.