TUTORIAL 6

1 Homework 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 From Order Finding to Factoring

Let $N = p \cdot q$ (with p, q prime numbers of the order of magnitude $2^{\lambda/2}$) be an RSA modulus. During the lecture, you saw a quantum algorithm SHOR which takes as input $x \in \mathbb{Z}_N^\times$ and returns its order, that is to say the smallest $r > 0$ such that $x^r = 1 \mod N$. We are going to see how to factor N using this algorithm. In the following, we will look at elements $x \mod N$ which will be represented as elements in $[0, N-1]$.

We are going to use the following classical results from algebra:

Theorem 2.1 (Bezout's theorem)**.** *For any $x, y \in \mathbb{Z}$, there exists $u, v \in \mathbb{Z}$ such that $xu + yv = \gcd(x, y)$. Reciprocally, if there exists $u, v \in \mathbb{Z}$ such that $xu + yv = d$, then $\gcd(x, y)|d$.*

Theorem 2.2 (Chinese Remainder Theorem)**.** *If $M = \prod_{i=1}^{p} n_i$, where the n_i are integers greater than 1 which are pairwise coprime, then*
$$\mathbb{Z}_M \simeq \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_p}$$
*via the **ring** isomorphism $(x \mod N) \mapsto (x \mod n_1, \ldots, x \mod n_p)$.*

Theorem 2.3. *Let G a finite commutative group, let $x \in G$ with order $w(x)$. If $x^r = 1$, then $w(x)|r$.*

1. Using the Bezout's Theorem, compute $|\mathbb{Z}_l^\times|$ for l a prime number.
2. Using the Chinese Remainder Theorem, compute $\phi(N) = |\mathbb{Z}_N^\times|$.

3. Take x uniform in $\mathbb{Z}_N$. What is the probability that $x \in \mathbb{Z}_N^\times$?

4. Let $x \in \mathbb{Z}_N^\times$ of odd order. Show that $-x$ has even order. Deduce that if x is uniformly sampled in $\mathbb{Z}_N^\times$, what the probability for x to have even order is $\geq 1/2$.

5. Sample x uniform in $\mathbb{Z}_N^\times$ of even order. Let r be its order. Assume that $x^{r/2} \pm 1 \neq 1, N$ (it can be proven to happen with a small probability ε), propose a way to find a non-trivial factor of N.

6. Deduce an algorithm making calls to SHOR which finds a non-trivial factor of N with high probability. Give its expected number of call to SHOR.

3 Modular Exponentiation

We are going to construct the gate $\Lambda_m(M_a)|k\rangle|x\rangle \mapsto |k\rangle|a^k \cdot x \mod N\rangle$ for any $a \in \mathbb{Z}_N$. In what is following, every quantum algorithm will be allowed to use ancillas and N can be represented over k qubits.

1. Let F and F^{-1} be computed by Boolean circuits of size $\leq L$ and depth $\leq d$. Show that F can be realized by a reversible circuit of size $O(L+n)$ and depth $O(d)$ using ancillas. (Recall that in those cases, we know how to construct a quantum circuit $F^\oplus$ such that $F^\oplus|x\rangle|y\rangle|0^m\rangle = |x\rangle|y \oplus F(x)\rangle|0^m\rangle$.)

2. Show that for every $a \in (\mathbb{Z}_N)^\times$ there exists an efficient quantum gate

$$T_a|x\rangle \mapsto |ax \mod N\rangle$$

3. Propose a classical algorithm that on input x, k, N computes $x^k \mod N$ by doing $O(\log(k))$ operations in $\mathbb{Z}_N$.

4. Conclude.

4 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 $\|\tilde{U}^{-1} - U^{-1}\| \leq \delta$.

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 $|\langle x|A|x\rangle| \leq \|A\|$.