COMS 4281 - Introduction to Quantum Computing Fall 2025

Practice Worksheet 5 - Phase Estimation and the factoring algorithm

This practice worksheet is intended to cover material up to October 30. The weekly quiz (due November 7th, 11:59pm) will be based on this worksheet. The final exam will have questions inspired by the worksheets.

Since the midterm, we have learned about the Quantum Fourier Transform, Phase Estimation, and Shor's factoring algorithm.

Problem 1: Eigenvectors and eigenvalues of unitary matrices

What are the eigenvectors and the corresponding eigenvalues of the following unitary matrices?

(a) $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

(b) $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$

(c) $I - 2\left|\psi\right\rangle\!\left\langle\psi\right|$ where $\left|\psi\right\rangle$ is an arbitrary quantum state in $\mathbb{C}^2$.

(d) Let V be a unitary that maps an orthonormal basis $\{\left|v_1\right\rangle, \left|v_2\right\rangle, \ldots, \left|v_d\right\rangle\}$ to the standard basis $\{\left|1\right\rangle, \left|2\right\rangle, \ldots, \left|d\right\rangle\}$ of $\mathbb{C}^d$. Let $\theta_1, \theta_2, \ldots, \theta_d$ be numbers between 0 and 1. Consider the unitary

$$U = V^\dagger \begin{pmatrix} e^{2\pi i\theta_1} & & & \\ & e^{2\pi i\theta_2} & & \\ & & \ddots & \\ & & & e^{2\pi i\theta_d} \end{pmatrix} V \ .$$

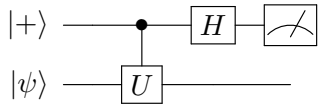
What are its eigenvalues and eigenvalues?

Problem 2: Analyzing single-ancilla qubit phase estimation

Let U be a unitary, and let $\left|\psi\right\rangle$ be an eigenvector (also called an *eigenstate*) with eigenvalue $e^{2\pi i\theta}$ for some $0 \leq \theta < 1$.

(a) What is the eigenvalue of U^k corresponding to the eigenvector $\left|\psi\right\rangle$?

(b) Analyze the following phase estimation circuit.



Work out the math to show that the probability of getting $\left|0\right\rangle$ is $\cos^2(\pi\theta)$. What is the probability of getting $\left|1\right\rangle$?

(c) Let's do a bit of statistical analysis. Suppose we repeatedly run the phase estimation circuit t times to get outcomes $X_1, X_2, \ldots, X_t \in \{0, 1\}$. We can try to estimate the probability of getting $|0\rangle$ by counting the number of times X_j is equal to 0 and dividing by t:

$$E = \frac{\#\text{ of times } X_j = 0}{t} .$$

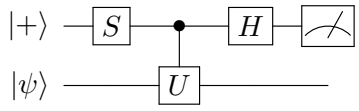
By law of large numbers, we expect E to converge to $\cos^2(\pi\theta)$, but we want to have a more precise estimate of the rate of convergence. Show that, by letting $t = O(\frac{1}{\epsilon^2})$, the empirical estimate E will satisfy

$$\Pr\left[|E - \cos^2(\pi\theta)| \geq \epsilon\right] \leq \frac{1}{100} .$$

Here, the choice of 1/100 is arbitrary (and affects the constant in the $O(\cdot)$ notation). In other words, by taking $O(1/\epsilon^2)$ samples, one can estimate $\cos^2(\pi\theta)$ up to additive error ϵ.

Hint: Look up Chebyshev's inequality and calculate the variance of E.

(d) Do the same analysis for this circuit

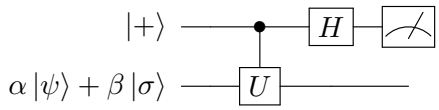


where $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ and show that the probability of getting $|0\rangle$ is $\cos^2(\pi\theta + \frac{\pi}{4})$.

(e) Imagine that you know the numbers $\cos^2(\pi\theta)$ and $\cos^2(\pi\theta + \frac{\pi}{4})$ exactly. How do you recover $0 \leq \theta < 1$ exactly?

Problem 3: Phase estimation on superposition of eigenvectors

Suppose that U additionally has the eigenvector $|\sigma\rangle$ with eigenvalue $e^{2\pi i\phi}$ that is orthogonal to $|\psi\rangle$. Suppose that we run run the phase estimation circuit



with the superposition $\alpha|\psi\rangle + \beta|\sigma\rangle$ in the second register. What is the joint state of both registers right before the measurement? What is the probability of getting outcome $|0\rangle$? What is the post-measurement state?

Problem 4: Modular multiplication unitary

Let N be a positive integer and let $1 \leq x < N$ be such that $\gcd(x, N) = 1$, i.e., they are co-prime. Recall the modular multiplication unitary

$$U|y\rangle = |xy \bmod N\rangle .$$

Let $r = \text{ord}(x)$ (i.e. $x^r = 1 \bmod N$).

(a) Show that for all $0 \leq s < r$, the vector

$$|v_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\Big(-2\pi i \frac{k}{r} s \Big) \Big| x^k \bmod N \Big\rangle$$

is an eigenvector of U with eigenvalue $\exp\Big(2\pi i \frac{s}{r}\Big)$.

(b) Show that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |v_s\rangle = |1\rangle \ .$$