CSE 598, Fall 2024, Homework #2

Instructor: Zilin Jiang

Question 2(e) Let $U' = \sum_i |\phi_i\rangle \langle\psi_i|$. For every j, we have $U' |\psi_j\rangle = \sum_i |\phi_i\rangle \langle\psi_i \mid \psi_j\rangle = |\phi_j\rangle$. Thus U and U' agree on the ψ-basis, and so $U = U'$.

Remark. One needs to mention that U and $\sum_i |\phi_i\rangle \langle\psi_i|$ are equal because they agree on a basis of $\mathbb{C}^d$.

Question 3 Let n be a large integer depending on ε to be chosen later. Set $\theta = \pi/(2n)$. The idea is to perform a series of n measurements where the bases are

$$\{R_\theta |0\rangle, R_\theta |1\rangle\}, \{R_{2\theta} |0\rangle, R_{2\theta} |1\rangle\}, \dots, \{R_{n\theta} |0\rangle, R_{n\theta} |1\rangle\},$$

where $R_?$ is the rotation transformation with a specific angle. After the first the measurement, we have the mixed state

$$\begin{cases} R_\theta |0\rangle & \text{with probability } \cos^2\theta; \\ R_\theta |1\rangle & \text{with probability } \sin^2\theta. \end{cases}$$

Consider the mixed state after the second measurement. If the state is $R_\theta |0\rangle$ after the second measurement, then the mixed state after the second measurement is

$$\begin{cases} R_{2\theta} |0\rangle & \text{with probability } \cos^2\theta; \\ R_{2\theta} |1\rangle & \text{with probability } \sin^2\theta. \end{cases}$$

If the state is $R_\theta |1\rangle$ after the second measurement, then the mixed state after the second measurement is

$$\begin{cases} R_{2\theta} |0\rangle & \text{with probability } \sin^2\theta; \\ R_{2\theta} |1\rangle & \text{with probability } \cos^2\theta. \end{cases}$$

Compounding the probabilities, overall the mixed state after the second measurement is

$$\begin{cases} R_{2\theta} |0\rangle & \text{with probability } \cos^2\theta\cos^2\theta + \sin^2\theta\sin^2\theta; \\ R_{2\theta} |1\rangle & \text{with probability } 2\sin^2\theta\cos^2\theta. \end{cases}$$

In particular, after the second measurement, the probability that the state is $R_{2\theta}|0\rangle$ is at least $\cos^4\theta$. Similarly, we can prove that after the kth measurement, the probability that the state is $R_{k\theta}|0\rangle$ is at least $\cos^{2k}\theta$. When $k = n$, the output state is $R_{n\theta}|0\rangle = |1\rangle$ with probability at least

$$\cos^{2n}\theta = \cos^{2n}\left(\frac{\pi}{2n}\right).$$

Recall that $\cos\theta = 1 - 2\sin^2(\theta/2)$. Since $\theta = \pi/(2n) \in [0, \pi/2]$, and so $\sin(\theta/2) \in (0, \theta/2)$, we have

$$\cos\theta = 1 - 2\sin^2(\theta/2) > 1 - 2(\theta/2)^2,$$

which implies that

$$\cos^{2n}\theta > \left(1 - \frac{\theta^2}{2}\right)^n = \left(1 - \frac{\pi^2}{8n^2}\right)^n.$$

One can use standard tools from calculus to show that the last expression tends to 1 as n approaches infinity. Thus it is possible to choose n large enough so that the probability of outputting $|1\rangle$ is at least $1 - \varepsilon$.

Remark. There is an adaptive strategy (which consists of several runs where each run might depend on previous ones). Measure in the $\{|+\rangle, |-\rangle\}$ basis and then measure in the $\{|0\rangle, |1\rangle\}$ basis. The output is $|0\rangle$ and $|1\rangle$ equally likely. When the readout is $|1\rangle$, we output the qubit immediately. Otherwise, we repeat the process. Every iteration, we output $|1\rangle$ with probability $1/2$. As long as $2^{-n} < \varepsilon$, up to n iterations suffice.

Question 6(b) By applying a CNOT gate with the second qubit as the control, and then a Hadamard gate on the second qubit, one can work out that the output state will be transformed to on of the following:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle.$$

Now Bob only need to measure in the standard basis to tell Alice's message.

Remark. If the CNOT gate is applied with the first qubit as the control, and then a Hadamard gate on the first qubit, the output state will be $|vu\rangle$ rather than $|uv\rangle$.