COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 1

1. **State discrimination.**

   (a) For an arbitrary orthonormal measuring basis $\{|b\rangle, |b^\perp\rangle\}$, the probability of getting outcome $|b\rangle$ when performing the measurement on the state $|\psi_2\rangle$ is

   $$|\langle b|\psi_2\rangle|^2 = |e^{i\varphi}\langle b|\psi_1\rangle|^2 = |\langle b|\psi_1\rangle|^2,$$

   which is the same as the probability of getting outcome $|b\rangle$ when performing the measurement on the state $|\psi_1\rangle$ as desired.

   (b) In the first case, we can choose the basis $\{|0\rangle, |1\rangle\}$, which will give a maximal value of $\frac{1}{2}$.

   In the second case, we can choose the basis $\{|+\rangle, |-\rangle\}$, which will give a maximal value of 1.

   (c) Set $\theta \in [0, \pi/2]$ to be the value such that $\cos\theta = |\langle\psi_1|\psi_2\rangle|$. Then there exists $\varphi \in [0, 2\pi)$ such that $\langle\psi_1|\psi_2\rangle = e^{i\varphi}\cdot\cos\theta$. We can write $|\psi_2\rangle = e^{i\varphi}\cdot\cos\theta\,|\psi_1\rangle + \sin\theta\,|\psi_1^\perp\rangle$ for some state $|\psi_1^\perp\rangle$ orthogonal to the state $|\psi_1\rangle$.

   Let U be the unitary that maps $|\psi_1\rangle$ to $e^{-i\varphi}|0\rangle$, and $|\psi_1^\perp\rangle$ to $|1\rangle$. Then $U|\psi_2\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle = |\psi_2'\rangle$ and $U|\psi_1\rangle = e^{-i\varphi}|\psi_1'\rangle$.

   Now say we have the optimal orthonormal basis $|b_1'\rangle, |b_2'\rangle$ for the vectors $|\psi_1'\rangle$ and $|\psi_2'\rangle$. We show the basis vectors $|b_1\rangle = U^\dagger|b_1'\rangle$ and $|b_2\rangle = U^\dagger|b_2'\rangle$ will yield the same optimal value for $|\psi_1\rangle, |\psi_2\rangle$. To see this, note for any other orthonormal basis $|c_1\rangle|c_2\rangle$,

   $$\begin{aligned}
   \frac{1}{2}\left(|\langle b_1|\psi_1\rangle|^2 + |\langle b_2|\psi_2\rangle|^2\right) &= \frac{1}{2}\left(|\langle b_1'|UU^\dagger|\psi_1'\rangle|^2 + |\langle b_2'|UU^\dagger|\psi_2'\rangle|^2\right)\\
   &= \frac{1}{2}\left(|\langle b_1'|\psi_1'\rangle|^2 + |\langle b_2'|\psi_2'\rangle|^2\right)\\
   &\geq \frac{1}{2}\left(|\langle c_1|U^\dagger|\psi_1'\rangle|^2 + |\langle c_2|U^\dagger|\psi_2'\rangle|^2\right)\\
   &= \frac{1}{2}\left(|\langle c_1|\psi_1\rangle|^2 + |\langle c_2|\psi_2\rangle|^2\right)
   \end{aligned}$$

   where we use the optimality of $|b_1'\rangle, |b_2'\rangle$. These calculations show the optimal value is recovered in the original basis AND that it stays optimal.

   In summary, we find $\theta \in [0, \pi/2], \varphi \in [0, 2\pi)$ such that $\langle\psi_1|\psi_2\rangle = e^{i\varphi}\cdot\cos\theta$. Then from $|b_1'\rangle, |b_2'\rangle$, we recover $|b_1\rangle, |b_2\rangle$ by calculating the unique unitary transformation U sending $|\psi_1\rangle \to e^{-i\varphi}|\psi_1'\rangle$ and $|\psi_2\rangle \to |\psi_2'\rangle$ and then applying $U^\dagger|b_1'\rangle$ and $U^\dagger|b_2'\rangle$.

(d) From part (a), global phases do not change the value. Consequently without loss of generality, we can assume our optimal choice of bases are

$$|b_1'\rangle = \cos\varphi\,|0\rangle + e^{i\tau}\sin\varphi\,|1\rangle$$
$$|b_2'\rangle = \sin\varphi\,|0\rangle - e^{i\tau}\cos\varphi\,|1\rangle$$

We can calculate

$$\begin{aligned}\frac{1}{2}\left(|\langle b_1'|\psi_1'\rangle|^2 + |\langle b_2'|\psi_2'\rangle|^2\right) &= \cos^2\varphi + |\sin\varphi\cos\theta - e^{-i\tau}\sin\theta\cos\varphi|^2 \\ &= \cos^2\varphi + \sin^2\varphi\cos^2\theta + \sin^2\theta\cos^2\varphi - 2\cos\tau\sin\theta\cos\theta\sin\varphi\cos\varphi,\end{aligned}$$

which is maximized when $\cos\tau = 1$ or $\cos\tau = -1$.

In the first case, $|b_1'\rangle = \cos\varphi\,|0\rangle + \sin\varphi\,|1\rangle$ and $|b_2'\rangle = \sin\varphi\,|0\rangle - \cos\varphi\,|1\rangle$ as desired.

In the second case, $|b_1'\rangle = \cos\varphi\,|0\rangle - \sin\varphi\,|1\rangle$ and $|b_2'\rangle = \sin\varphi\,|0\rangle + \cos\varphi\,|1\rangle$, which is the same as $\cos\varphi'\,|0\rangle + \sin\varphi'\,|1\rangle$, $\sin\varphi'\,|0\rangle - \cos\varphi'\,|1\rangle$ up to a global phase for $\varphi' = -\varphi$. Since a global phase does not change the value, we can always find an optimal basis of the desired form.

(e) Continuing our calculations from above, we can assume that $|b_1'\rangle, |b_2'\rangle$ have the desired form, and we have that

$$\begin{aligned}\frac{1}{2}\left(|\langle b_1'|\psi_1'\rangle|^2 + |\langle b_2'|\psi_2'\rangle|^2\right) &= \cos^2\varphi + (\sin\varphi\cos\theta - \sin\theta\cos\varphi)^2 \\ &= \cos^2\varphi + \sin^2(\varphi - \theta) \\ &= \frac{1+\cos 2\varphi}{2} + \frac{1-\cos(2\varphi - 2\theta)}{2} \\ &= 1 - \sin(2\varphi - \theta)\sin\theta \\ &\leq 1 + \sin\theta,\end{aligned}$$

where we use that $\theta \in [0, \pi/2]$ from part (c).

Equality is achieved if $2\varphi - \theta \in -\frac{\pi}{2} + 2\pi\mathbb{Z} \Leftrightarrow \varphi \in \frac{\theta}{2} - \frac{\pi}{4} + \pi\mathbb{Z}$.

(f) We note from our previous work, the optimal value was precisely $1 + \sin\theta$, where $\theta \in [0, \pi/2]$ satisfies that $\langle\psi_1|\psi_2\rangle = e^{i\varphi}\cdot\cos\theta$ for some φ. Therefore, as a function of $|\psi_1\rangle$ and $|\psi_2\rangle$, the maximum value of Eq. (1) is $1 + \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}$.

We can use the above results to find the optimal basis.

$$|b_1\rangle = U^\dagger|b_1'\rangle = \cos(\theta/2 + 3\pi/4)U^\dagger|0\rangle + \sin(\theta/2 + 3\pi/4)U^\dagger|1\rangle$$
$$|b_2\rangle = U^\dagger|b_2'\rangle = \sin(\theta/2 + 3\pi/4)U^\dagger|0\rangle - \cos(\theta/2 + 3\pi/4)U^\dagger|1\rangle$$

where U is the unitary transformation that sends $|\psi_1\rangle \to e^{-i\varphi}|0\rangle$ and $|\psi_2\rangle \to \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$.

2. **Unambiguous quantum state discrimination.**

(a) Alice does not output $|0\rangle$, so she will not mis-identify a state $|+\rangle$ as $|0\rangle$. Alice only outputs $|+\rangle$ when she gets the outcome $|1\rangle$ when measuring in the basis $\{|0\rangle, |1\rangle\}$, so she will not mis-identify a state $|0\rangle$ as $|+\rangle$. Therefore, Alice does not make any mistakes.

If Bob sends $|0\rangle$, Alice will always get the outcome $|0\rangle$ when measuring it, and therefore Alice will output $\perp$ with certainty. That is, $p = 1$.

If Bob sends $|+\rangle$, Alice will get the outcome $|0\rangle$ with probability $1/2$ when measuring it, and therefore Alice will output $\perp$ with probability $1/2$. That is, $q = \frac{1}{2}$.

(b) Using the same argument as part (a), we can show that Alice does not make any mistakes, $p = \frac{1}{2}$ and $q = 1$.

(c) The probability of mis-identifying $|0\rangle$ as $\perp$ is

$$\mathrm{Tr}(E_3 |0\rangle\langle 0|) = \mathrm{Tr}(|0\rangle\langle 0| - \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1| \cdot |0\rangle\langle 0| - \frac{\sqrt{2}}{1+\sqrt{2}} |-\rangle\langle -| \cdot |0\rangle\langle 0|) = \frac{\sqrt{2}}{2}$$

Similarly, the probability of mis-identifying $|1\rangle$ as $\perp$ is

$$\mathrm{Tr}(E_3 |+\rangle\langle +|) = \frac{\sqrt{2}}{2}$$

Remark 1. One can verify that E_1, E_2, E_3 are all positive semidefinite, and $E_1 + E_2 + E_3 = \mathbb{I}$, and thus $\{E_1, E_2, E_3\}$ forms a valid POVM. Clearly, using this strategy, Alice never identifies $|+\rangle$ as $|0\rangle$ and vice versa. This POVM achieves an average probability of mis-identifying $\frac{p+q}{2} = \frac{\sqrt{2}}{2}$, which is smaller than $(1 + \frac{1}{2})/2$, the average probability of mis-identifying of the best projective measurement, showing that performing a general POVM may have a practical advantage over a projective measurement.

3. **Classical one-time pad.**

4. **Density matrices.**

5. **Classical-quantum states.**

6. **Quantum one-time pad.**

(a) Recall that a correct encryption scheme constitutes a well defined encryption function which takes a single quantum bit to a single quantum bit, E, and a well defined decryption function, D, which should operate as the inverse of E. Observe that E is well defined in the problem since $E = H^k$ where k is the secret key (we are only concerned with encrypting a single qubit). We wish to similarly define an

inverse operation D. Since H is a valid quantum map over pure states, it must be a unitary transformation. Consequently, $H^{-1} = H^\dagger$. Now, notice that setting $D = (H^\dagger)^k$ will be an inverse of E,

$$D(E(|\psi\rangle)) = (H^\dagger)^k (H)^k |\psi\rangle = (H^\dagger H)^k |\psi\rangle = \mathbb{I}^k |\psi\rangle = |\psi\rangle$$

Thus, this encryption scheme is correct.

(b) Unfortunately for Alice, this encryption scheme is not correct. We will give an attack, described by the adversial game framework described in class. We first recollect this framework. An adversary gives Alice two qubits $\{|\psi_1\rangle, |\psi_2\rangle\}$. Alice then chooses any one of these $|\psi_i\rangle$ and a value for k, then returns to the adversary the qubit $E(|\psi_i\rangle)$. Given this qubit, the adversary final responds with which qubit was encrypted, namely responding with a $j \in \{1, 2\}$. The adversary wins if $\mathbf{Pr}[j = i] > 1/2$, otherwise Alice wins and her scheme is secure.

We describe such a winning strategy for the adversary. Recall that Alice has fixed H defining her scheme. Furthermore, we recall that the eigenvectors of H must be orthogonal since it is a unitary transformation. Denote these eigenvectors $|v_1\rangle$ and $|v_2\rangle$. Furthermore, considering their normalization makes them a set of two qubits. Now, suppose the adversary sends Alice these two qubits: $\{|v_1\rangle, |v_2\rangle\}$. Alice then chooses some k and i, and responds with $H^k |v_i\rangle$. The adversary then measures this qubit in the $\{|v_1\rangle, |v_2\rangle\}$ basis. Following this, if the adversary observes $|v_1\rangle$ he responds with $j = 1$, otherwise he must have observed $|v_2\rangle$ and in that case he responds with $j = 2$. Analyzing this scheme, observe that if $i = 1$, then $p_1 = |\langle v_1| H^k |v_1\rangle|^2 = |\langle v_1\rangle v_1|^2 = 1$ and $j = 1$ with probability 1, regardless of the value of k. Similarly, if $i = 2$ then $p_2 = |\langle v_2| H^k |v_2\rangle|^2 = |\langle v_2\rangle v_2|^2 = 1$ and $j = 2$ with probability 1. Thus we get,

$$\begin{aligned}\mathbf{Pr}[i = j] =& \mathbf{Pr}[i = j \mid i = 1] \cdot \mathbf{Pr}[i = 1] + \mathbf{Pr}[i = j \mid i = 2] \cdot \mathbf{Pr}[i = 2] \\ =& \mathbf{Pr}[i = 1] + \mathbf{Pr}[i = 2] \\ =& 1 > 1/2\end{aligned}$$

Hence, this scheme cannot be secure.

7. **Quantum one-time pad applied to bipartite state.**