Introduction to Quantum Computer Science and Applications

Exercise Sheet 7

Exercise 1. *Consider two quantum states ρ, σ, and an m-outcome* POVM $\{\mathbf{F}_1, \dots, \mathbf{F}_m\}$ *where each* $\mathbf{F}_i = \mathbf{M}_i \mathbf{M}_i^\dagger$ *and* $\sum_i \mathbf{F}_i = \mathbf{Id}$. *We define*

$$p_i = \mathrm{tr}(\mathbf{F}_i \rho) \quad \textit{and } q_i = \mathrm{tr}(\mathbf{F}_i \sigma).$$

Our goal is to show that

$$\Delta(\rho, \sigma) \geq \Delta(p, q).$$

with $\Delta(p,q) = \frac{1}{2} \sum_i |p_i - q_i|$.

1. *To what correspond the values p_i and q_i?*
2. *We perform the spectral decomposition* $\rho - \sigma = \sum_i \lambda_i |e_i\rangle\langle e_i|$. *We define*

$$\mathbf{Q} = \sum_{i:\, \lambda_i \geq 0} \lambda_i |e_i\rangle\langle e_i| \quad \textit{and} \quad \mathbf{S} = \sum_{i:\, \lambda_i < 0} -\lambda_i |e_i\rangle\langle e_i|$$

   Notice that $|\rho - \sigma| = \mathbf{Q} + \mathbf{S}$ *and* $\rho - \sigma = \mathbf{Q} - \mathbf{S}$. *Show that for each* $i \in [\![1, m]\!]$

$$|p_i - q_i| \leq \mathrm{tr}(\mathbf{F}_i(\mathbf{Q} + \mathbf{S})).$$

3. *Conclude that* $\Delta(\rho, \sigma) \geq \Delta(p, q)$.

Exercise 2. *Assume Alice has two states ρ_0 and ρ_1 and sends to Bob ρ_b for a randomly chosen $b \in \{0, 1\}$. The aim of Bob is to recover b.*

1. *Use the previous exercise to show that Bob can guess b with probability at most*

$$\frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}.$$

   Hint: *any strategy for Bob can be expressed as a 2-outcome* POVM $\{\mathbf{F}_0, \mathbf{F}_1\}$ *where outcome i corresponds to his guess. Express his winning as a function of* $\mathrm{tr}(\mathbf{F}_0 \rho_0)$ *and* $\mathrm{tr}(\mathbf{F}_1 \rho_1)$.

2. *Give a strategy for which the probability of Bob to win reaches the above upper-bound.*

   Hint: *diagonalize $\rho_0 - \rho_1$, giving a basis to perform a measurement*

Comment: *the strategy of* 2 *is known as Helström measurement.*

Exercise 3 (Unambiguous state discrimination)**.** *Assume we have two qubits*

$$|\varphi_0\rangle = |0\rangle \quad \textit{and} \quad |\varphi_1\rangle = \cos(\theta)\,|0\rangle + \sin(\theta)\,|1\rangle$$

with $\theta \in [0, \frac{\pi}{2})$*. Suppose Bob is given* $|\varphi_b\rangle$ *for a random unknown* $b \in \{0,1\}$ *and his goal is to guess* b*. We want a measurement that has up to* 3 *outcomes:* "0", "1" *and* "2" *such that the measurement always succeeds when measuring "0" or "1" (the "2" outcome corresponds to "unknown").*

Let $|f_1\rangle = \sin(\theta)\,|0\rangle - \cos(\theta)\,|1\rangle$*. We consider the three outcome* POVM $\{\mathbf{F}_0, \mathbf{F}_1, \mathbf{F}_2\}$ *with* $\mathbf{F}_i = \mathbf{M}_i \mathbf{M}_i^\dagger$ *where*

$$\mathbf{F}_0 = \frac{1}{1+\cos(\theta)}\,|f_1\rangle\langle f_1|\,, \quad \mathbf{F}_1 = \frac{1}{1+\cos(\theta)}\,|1\rangle\langle 1| \quad \textit{and} \quad \mathbf{F}_2 = (\mathbf{I} - \mathbf{F}_0 - \mathbf{F}_1)\,.$$

1. *Let* $|w\rangle = -\sin(\theta/2)\,|0\rangle + \cos(\theta/2)\,|1\rangle$ *and* $|w^\perp\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,|1\rangle$*. Show that*

$$\frac{|f_1\rangle\langle f_1| + |1\rangle\langle 1|}{2} = \cos^2(\theta/2)\,|w\rangle\langle w| + \sin^2(\theta/2)\,|w^\perp\rangle\langle w^\perp|\,.$$

2. *Show that* $\mathbf{F}_2 = (1 - \tan^2(\theta/2))\,|w^\perp\rangle\langle w^\perp|$ *and that* $(1 - \tan^2(\theta/2)) \geq 0$*. From there, we easily have that* $\mathbf{F}_0, \mathbf{F}_1, \mathbf{F}_2$ *are positive semi-definite and that* $\{\mathbf{F}_i\}$ *is a valid* POVM*.*

3. *Show that this* POVM *satisfies our requirements. What is the probability of correctly guessing b here? Compare with the optimal guessing probability seen during the lecture. Is there a difference? Why?*

Exercise 4. *Recall the Fuchs-van de Graaf inequalities*

$$1 - F(\rho,\sigma) \leq \Delta(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}.$$

1. *Give two quantum states* ρ, σ *st.* $\Delta(\rho,\sigma) = \frac{1}{2}$ *and* $1 - F(\rho,\sigma) = \Delta(\rho,\sigma)$*.*

2. *Give two quantum states* ρ, σ *st.* $\Delta(\rho,\sigma) = \frac{1}{2}$ *and* $\Delta(\rho,\sigma) = \sqrt{1 - F(\rho,\sigma)^2}$*.*

Notations. $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Trignometric relations:

$$\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$$
$$\sin(x+y) = \sin(x)\cos(y) + \sin(y)\cos(x)$$

In particular: $\cos(2x) = 2\cos^2(x) - 1$ and $\sin(2x) = 2\cos(x)\sin(x)$.
We define

$$A(\rho,\sigma) = \arccos F(\rho,\sigma).$$

which implies that $A(\rho,\sigma) \in [0,\pi/2]$ and $F(\rho,\sigma) = \cos A(\rho,\sigma)$. Let us admit that $A(\cdot,\cdot)$ is a distance measure; in particular it satisfies the triangle inequality for any ρ,ζ,σ:

$$A(\rho,\zeta) \le A(\rho,\sigma) + A(\sigma,\zeta).$$

Exercise 5. *Our goal is to show the following result (used to show that Alice's optimal strategy to cheat in the quantum bit commitment scheme is* $\frac{1}{2} + \frac{F(\rho_0,\rho_1)}{2}$*)*

$$\max_{\zeta}\left\{\frac{1}{2}F^2(\rho,\zeta) + \frac{1}{2}F^2(\zeta,\sigma)\right\} = \frac{1}{2} + \frac{F(\rho,\sigma)}{2}. \tag{1}$$

1. *Show that for any angles* $\alpha,\beta \in [0,\pi/2]$

$$\cos(\alpha+\beta) \ge \cos^2(\alpha) + \cos^2(\beta) - 1.$$

Hint: *you can use the following inequality that comes from the concavity of the cos function on* $[0,\pi]$*:* $\forall x,y \in [0,\pi]:\ \cos\left(\frac{x+y}{2}\right) \ge \frac{1}{2}(\cos(x) + \cos(y))$ *as well as known trigonometric equalities*

2. *Using the angle distance, show that*

$$\max_{\zeta}\{\frac{1}{2}F^2(\rho,\zeta) + \frac{1}{2}F^2(\zeta,\sigma)\} \le \frac{1}{2} + \frac{F(\rho,\sigma)}{2}.$$

3. *For any states* ρ,σ*, show that there exists* ζ *st.*

$$\frac{1}{2}F^2(\rho,\zeta) + \frac{1}{2}F^2(\zeta,\sigma) \ge \frac{1}{2} + \frac{F(\rho,\sigma)}{2}.$$

Hint: *Consider purifications* $|\varphi\rangle, |\psi\rangle$ *of* ρ,σ *from Uhlmann's theorem and look at the state „ in between" $|\varphi\rangle$ and $|\psi\rangle$.*