Analysis around the fingerprint state

Consider the state $|\psi_{x_1x_2x_3x_4}\rangle = \frac{1}{2}\left((-1)^{x_1}|00\rangle + (-1)^{x_2}|01\rangle + (-1)^{x_3}|10\rangle + (-1)^{x_4}|11\rangle\right)$ that depends on 4 bits x_1, x_2, x_3, x_4.

Exercise 1. *We assume $x_2, x_3, x_4 = 0$. Consider the states $|\phi_b\rangle = |\psi_{b000}\rangle$. This is 2-qubit state on some registers AB where A is the register corresponding to the first qubit and B is the register corresponding to the second qubit.*

1. *Give an expression for $|\phi_0\rangle$ and $|\phi_1\rangle$.*
2. *Compute $\rho_b^A = tr_B|\phi_b\rangle\langle\phi_b|$ for both $b = 0$ and $b = 1$.*
3. *Compute $\Delta(\rho_0^A, \rho_1^A)$. Give a measurement that, given ρ_b^A, outputs b with probability P_b with $\frac{1}{2}(P_0 + P_1) = \frac{3}{4}$ and argue that this measurement is optimal.*

Exercise 2. *We still assume $x_2, x_3, x_4 = 0$. Our goal is to analyze what is the probability of recovering x_1 assuming we now have access to the full state $|\phi_{x_1}\rangle$ (so Alice and Bob are together here).*

1. *Compute $\langle\phi_0|\phi_1\rangle$. Argue that there is a measurement that, given $|\phi_b\rangle$ for $b \in \{0, 1\}$, outputs b with probability P_b with $\frac{1}{2}(P_0 + P_1) = \frac{1}{2} + \frac{\sqrt{3}}{4}$.*
2. *Find the measurement that distinguishes $|\phi_0\rangle$ and $|\phi_1\rangle$ wp. $\frac{1}{2} + \frac{\sqrt{3}}{4}$. One can use without proof $\frac{1}{2} + \frac{\sqrt{3}}{4} = \cos^2(\pi/12)$.*

Exercise 3. *We now don't have $x_2, x_3, x_4 = 0$ anymore. Assume we are in one of the two following cases*

1. *$x_1 = x_2 = x_3 = x_4$.*
2. *$x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$, but the 4 bits are not all equal.*

Give a measurement on $|\psi_{x_1x_2x_3x_4}\rangle$ that determines with certainty in which case we are.

Angle distance

The quantity $1 - F$ is not a distance since it doesn't satisfy the triangle inequality. Our goal here is to construct a distance out of the fidelity.

Definition 1. *For any two quantum states ρ, σ, we define their angle as $Angle(\rho, \sigma) = Arccos(F(\rho, \sigma))$*

Fix two pure states $|\psi\rangle$ and $|\phi\rangle$ with $|\langle\psi|\phi\rangle| = \cos(\alpha)$, then $Angle(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \alpha$. The notion of angle for mixed states somehow extends the notion of angle that exists for pure states.

The angle is a distance. It satisfies the following properties

- $Angle(\rho, \sigma) = 0 \Leftrightarrow \rho = \sigma$
- $0 \leq Angle(\rho, \sigma) \leq \pi/2$
- $Angle(\rho, \sigma) = Angle(\sigma, \rho)$
- $Angle(\rho, \tau) \leq Angle(\rho, \sigma) + Angle(\sigma, \tau)$

Exercise 4. *Our goal is to show the following result: for any quantum states ρ, σ, we have*

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

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

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

(Hint: you can use the following inequality that comes from the concavity of the cos function on $[0, \pi]$:

$$\forall x, y \in [0,\pi] : \cos(\frac{x+y}{2}) \geq \frac{1}{2}\left(\cos(x) + \cos(y)\right).$$

as well as known trigonometric equalities)

2. *Using the angle distance, show that*

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

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

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

(Hint: Consider purifications $|A\rangle, |B\rangle$ of ρ, σ from Ulhmann's theorem and look at the state " in between" $|A\rangle$ and $|B\rangle$.)

Exercise 5 (Strong Concavity of the Fidelity)**.** *Let p_i and q_i be probability distributions over the same index set, and ρ_i, σ_i also density operators indexed over the same index set. Our goal is to show that*

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq \sum_i \sqrt{p_i q_i} F(\rho_i, \sigma_i).$$

1. *We take purifications $|\psi_i\rangle$ of ρ_i and purifications $|\phi_i\rangle$ of σ_i st. $F(\rho_i, \sigma_i) = \langle\psi_i|\phi_i\rangle$. Argue why this is always possible.*
2. *Let $|\psi\rangle = \sum_i \sqrt{p_i}\,|\psi_i\rangle\,|i\rangle$ and $|\phi\rangle = \sum_i \sqrt{q_i}\,|\phi_i\rangle\,|i\rangle$. Show that*

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq |\langle\psi|\phi\rangle|.$$

3. *Conclude.*

Exercise 6 (Simple bit commitment protocol)**.** *We consider the following simple bit commitment protocol:*

- *Commit phase: If Alice wants to commit to $b = 0$, she sends $|0\rangle$ to Bob. If Alice wants to commit to $b = 1$, she sends $|+\rangle$ to Bob.*
- *Reveal phase: Alice reveals b. If $b = 0$, Bob measures his qubit in the computational basis and checks whether he got $|0\rangle$. If $b = 1$, Bob measures his qubit in the computational basis and checks whether he got $|+\rangle$.*

1. *Assuming Alice is honest and she chooses b at random, what is Bob's probability of guessing b after the commit phase?*
2. *Think of the best way to cheat for Alice in the following sense: find a quantum state $|\phi\rangle$ that Alice can send after the commit phase that will allow to successfully reveal any of the 2 values wp. $\cos^2(\pi/8)$.*