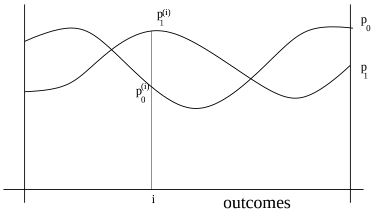
Topics in Quantum Information | **U. Waterloo CO 781, Spring 2004**
Ashwin Nayak (Instructor) | **Annika Niehage (Scribe)**
Distinguishability of states. Strong coin-flipping. | **May 25, 2004**

Recall 1 *Last lecture we saw that for two density matrices ρ_0 and ρ_1 there exists an optimal basis for measurement such that*

$$\| p_1 - p_0 \|_1 \quad = \quad \| \rho_0 - \rho_1 \|_{\mathrm{tr}}$$

where p_0 and p_1 are the distribution on outcomes.

Bayes' Strategy



Given a sample from one of two distributions p_0 or p_1, Bayes' strategy gives us the optimal procedure to identify which distribution it may have come from. The best strategy to guess 0 or 1 from outcome i: guess $b = 0/1$ if $p_b(i) > p_{\bar{b}}(i)$. This means that for every outcome you always favour the distribution with the maximum probability value at that point.

Exercise 2 *Verify that if ρ_0 or ρ_1 was chosen with probability $\frac{1}{2}$ and then measured in the optimal basis and use Bayes' strategy,*

$$\mathrm{Prob(guess\ is\ correct)} \quad = \quad \frac{1}{2} + \frac{\| \rho_0 - \rho_1 \|_{\mathrm{tr}}}{4}$$

1 Another measure: Fidelity

Recall 3 *Every $\rho \in \mathcal{K}$ may be purified to a pure state $\psi \in \mathcal{H} \otimes \mathcal{K}$, given*

$$\begin{array}{lcl} \rho_0,\ \rho_1 \in \mathcal{K} & \longrightarrow & \text{purifications } \psi_0,\ \psi_1 \in \mathcal{H} \otimes \mathcal{K} \\ & & (\dim(\mathcal{H}) \geq \mathrm{rank}(\rho_0), \mathrm{rank}(\rho_1)) \end{array}$$

Question:

- How close are $\psi_0,\ \psi_1$?
- How large can $|\langle \psi_0 | \psi_1 \rangle|^2$ be? (the "**overlap**")

e.g. $\left\{ (\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle) \right\}$ & $\left\{ (\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle) \right\}$ can be obtained from the same purification ψ.

Definition 4 *The* **Fidelity** *of ρ_0 and ρ_1 is defined by the following equation:*

$$\mathrm{F}(\rho_0, \rho_1) \quad = \quad \max |\langle \psi_0 | \psi_1 \rangle|^2$$

where the maximum is taken over all purifications ψ_0, ψ_1 over the same space.

The use of 'maximum' rather than 'supremum' in the definition above is justified by the following theorem.

Theorem 5 *(Uhlmann '70s)*

1. *Fidelity $\mathrm{F}(\rho_0, \rho_1)$ is achieved by purifications ψ_0, ψ_1 in a space $\mathcal{H} \otimes \mathcal{K}$ with $\dim(\mathcal{H}) \geq \dim(\mathcal{K})$ and*

$$\mathrm{F}(\rho_0, \rho_1) \quad = \quad \| \sqrt{\rho_0} \cdot \sqrt{\rho_1} \|_{\mathrm{tr}}^2 .$$

2. *Given any purification ψ_0 of ρ_0 in the space $\mathcal{H} \otimes \mathcal{K}$ as above, there exists a purification $\tilde{\psi}_1$ of ρ_1 such that*

$$\left| \langle \psi_0 | \tilde{\psi}_1 \rangle \right|^2 \quad = \quad \mathrm{F}(\rho_0, \rho_1)$$

Proof : see Nielsen & Chuang

□

Properties 6

1. $0 \leq \mathrm{F}(\rho_0, \rho_1) \leq 1$, *and it is symmetric.*
2. *If $\rho_0 = \rho_1$, then $\mathrm{F}(\rho_0, \rho_1) = 1$. If $\rho_0 \cdot \rho_1 = 0$, then $\mathrm{F}(\rho_0, \rho_1) = 0$.*
   (In fact, these are also necessary conditions.)
3. *If $\rho_0 = |\psi\rangle\langle\psi|$, then $\mathrm{F}(\rho_0, \rho_1) = \langle \psi | \rho_1 | \psi \rangle$.*
4. *If $\rho_0 = |\psi_0\rangle\langle\psi_0|$ and $\rho_1 = |\psi_1\rangle\langle\psi_1|$, then $\mathrm{F}(\rho_0, \rho_1) = |\langle \psi_0 | \psi_1 \rangle|^2$*

Proof : All the properties may be derived directly from the definition of fidelity. However, Uhlmann's theorem simplifies the proofs.

Proof of (3). We will use the following matrix identity:
Let $M = \sum_i \sigma_i |u_i\rangle\langle v_i|$ be a matrix with $\sigma_i \geq 0$, $\{u_i\}$ and $\{v_i\}$ orthonormal bases, and $\| M \|_{\mathrm{tr}} = \sum_i \sigma_i$. Then we get

$$\begin{aligned} M^\dagger M &= (\sum_j \sigma_j |v_j\rangle\langle u_j|)(\sum_i \sigma_i |u_i\rangle\langle v_i|) \\ &= \sum_j \sigma_j^2 |v_j\rangle\langle v_j| \end{aligned}$$

and so

$$\| M \|_{\mathrm{tr}} = \mathrm{Tr}(\sqrt{M^\dagger M}) = \mathrm{Tr}(\sqrt{M\, M^\dagger})$$

Now, by Uhlmann's Theorem we get

$$\begin{aligned} \mathrm{F}(\rho_0, \rho_1) &= \| \, |\psi\rangle\langle\psi| \sqrt{\rho_1} \, \|_{\mathrm{tr}}^2 \\ &= \mathrm{Tr}(\sqrt{|\psi\rangle\langle\psi| \sqrt{\rho_1} \sqrt{\rho_1} |\psi\rangle\langle\psi|})^2 \\ &= \langle \psi | \rho_1 | \psi \rangle \end{aligned}$$

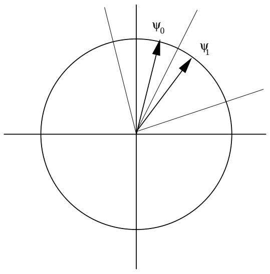
Theorem 7 *(Fuchs & van de Graaf '99)*

$$1-\sqrt{\mathrm{F}(\rho_0,\rho_1)} \overset{(*)}{\leq} \frac{1}{2}\,\|\,\rho_0-\rho_1\,\|_{\mathrm{tr}} \overset{(**)}{\leq} \sqrt{1-\mathrm{F}(\rho_0,\rho_1)}.$$

Remark 8 *We observe that we get equality in the theorem above*

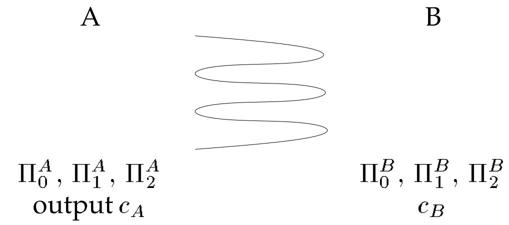
- *for* $(*)$ *and* $(**)$ *if* $\rho_0 \perp \rho_1$,
- *for* $(**)$ *if we use pure states.*

Verify the following picture:



I.e., that the optimal basis for distinguishing two pure states is the one that is symmetrically oriented with respect to the two states.

2 Strong Coin Flipping



Definition 9 *A strong coin flipping protocol is a communication protocol between two parties A, B that start without any input and produce one output each c_A, c_B such that:*

1. *If A and B are honest (follow the protocol), then*

$$\mathrm{Prob}(\mathrm{c_A} = \mathrm{c_B} = 0/1) \;=\; \frac{1}{2}$$

2. *If only A is dishonest, then*

$$\mathrm{Prob}(\mathrm{c_B} = 0/1) \;\leq\; \frac{1}{2}+\epsilon$$

with $\epsilon < \frac{1}{2}$. Similarly, if B is dishonest.

Protocol [Aharonov, Ta-Shma, Vazirani, Yao '00] [ATVY'00] gave a general schema to construct a protocol with the properties above, and showed that bias $\epsilon < 1/2$ is achievable with quantum communication. Their schema is shown in the following diagram.

	A		B
1)	picks random $a \in_R \{0,1\}$	$\xrightarrow{\text{weakly commits to a}}$	
2)		$\xleftarrow{b}$	picks random $b \in_R \{0,1\}$
3)		$\xrightarrow{a,\text{ verification state}}$	checks that commitment and verifies that the state and & a are consistent
4)	output $c_A = a \oplus b$		& if not says - "A is cheating". Else, output $c_B = a \oplus b$.

The best known protocol due to Ambainis [2001] and Spekkens and Rudolph [2002] also have the same form. In detail, the commitment, reveal stage, and check look like the following:

The commitment: A constructs:

$$|\psi_a\rangle = \frac{1}{\sqrt{2}}(|aa\rangle + |22\rangle)$$

and sends **one** qutrit to B.

Reveal stage: A sends the second qutrit.

Bob's check: Bob checks that the two qutrits are in state $|\psi_a\rangle$ (i.e., measures according to the projection operators $|\psi_a\rangle\langle\psi_a|$, $I - |\psi_a\rangle\langle\psi_a|$).

We will analyse this protocol in the next lecture.