
Accessible Fidelity and Quantumness of Sets of Quantum States

Koenraad M.R. Audenaert

University of Wales, Bangor

June 10, 2004

Based on:

- Fuchs and Sasaki: `quant-ph/0302092`
- Fuchs: `quant-ph/0404122`
- Audenaert, Fuchs, King and Winter: `quant-ph/0308120`

Some Zen Questions

- You know the sound of two hands clapping.

Some Zen Questions

- You know the sound of two hands clapping.
- Q: How does *one* hand sound?

Some Zen Questions

- You know the sound of two hands clapping.
- Q: How does *one* hand sound?
- Q2: How quantum is a *single* quantum state?

Quantumness of States

- It is the feeling of at least one of the authors that “a robust notion of *quantumness* can only be attached to *a set* of states”.
- Members of a set of states can be more or less quantum w.r.t. each other; there is no good sense in which each one alone is intrinsically quantum or not.
- Mutually non-orthogonal quantum states cannot be cloned, even if these states are hemi-semi-demi-quasi-classical (coherent) states.
- The present work is an attempt at finding a notion of quantumness for sets of states.
- Basic Idea: quantify how well-preserved a set of quantum states remains after being “squeezed” through a classical channel.

Basic Scenario

- Let a set \mathcal{S} of pure states be taken from a certain Hilbert space \mathcal{H} :

$$\mathcal{S} = \{\Psi_i := |\psi\rangle\langle\psi|\}.$$

- We pass these states through a classical channel, consisting of:
- A (generalised) measurement $\{E_b\}$ with outcomes $\{b\}$:

$$\rho \mapsto b, P_b = \text{Tr}[E_b\rho]$$

$\{E_b\}$ is a POVM: $E_b \geq 0$ and $\sum_b E_b = \mathbf{I}$,

- A subsequent “resynthesis” into quantum states:

$$b \mapsto \sigma_b.$$

Average Fidelity

- As a measure of how good the states ψ_i are preserved in this process, we choose the **average fidelity** between initial and final states:

$$F = \sum_i p_i \sum_b \text{Tr}[E_b \Psi_i] \text{Tr}[\Psi_i \sigma_b],$$

- Here we had to assign an as yet arbitrary probability distribution $\{p_i\}$ to the signal states ψ_i .

An Interpretation

- The basic scenario can be interpreted in a Quantum Cryptographic setting; more precisely: of eavesdropping detection.
- Ellis wants to send messages to Bob using the signal states ψ_i . The probabilities p_i are the source probabilities.
- The eavesdropper is actually two people, Eve and Yves, who are connected by a classical phone line.
- Eve intercepts the states ψ_i , and performs a POVM E_b on them.
- Eve sends her outcomes b to Yves over the phone.
- Yves then chooses a quantum state σ_b accordingly and sends it to Bob.
- To minimise the probability of being detected, Eve and Yves must maximise the average fidelity.

Achievable and Accessible Fidelity

- By maximising the average fidelity over all resynthesis strategies $b \mapsto \sigma_b$ we get the **Achievable Fidelity** w.r.t. the measurement:

$$F(\{p_i, \psi_i\}, \{E_b\}) = \sup_{\{\sigma_b\}} F(\{p_i, \psi_i\}, \{E_b, \sigma_b\})$$

- If we maximise this further over all measurement strategies $\{E_b\}$, we get the **Accessible Fidelity** of the ensemble $\{p_i, \psi_i\}$:

$$F(\{p_i, \psi_i\}) = \sup_{\{E_b\}} F(\{p_i, \psi_i\}, \{E_b\}).$$

- This name has been chosen in analogy with the quantity of accessible information.

Quantumness

- We can get rid of the arbitrary p_i by minimising over them, giving the **Quantumness** of the set $\{\psi_i\}$:

$$Q(\{\psi_i\}) = \inf_{\{p_i\}} F(\{p_i, \psi_i\}).$$

- We minimise here, because the p_i are on Ellis' side, and he wants to fight back.
- Ellis can fight even harder by also minimising over the set $\{\psi_i\}$ itself, and this then gives the **Quantumness** of the Hilbert space \mathcal{H} :

$$Q(\mathcal{H}) = \inf_{\{\psi_i \in \mathcal{H}\}} Q(\{\psi_i\}).$$

Interpretation

- The quantumness of a set of states specifies the best use that can be made of the set for revealing the existence of an eavesdropper.
- Note that it is an inverted measure!
- In a classical world, an unconstrained eavesdropper cannot be detected, so $Q_{c1} = 1$.
- The smaller the quantumness, the greater the departure from classical characteristics.

Properties, Known and Desired

- The quantumness of a d -dimensional Hilbert space is

$$Q(\mathcal{H}) = \frac{2}{d+1}.$$

(Proven in Fuchs `quant-ph/0404122`). Thus the qubit space is least quantum of all Hilbert spaces.

- What is the minimal required number of states ψ_i to achieve minimal quantumness? Is it d^2 ? Or less?

(News Flash! News Flash! R. Blume-Kohout seems to have found an answer...)

- Accessible fidelity and quantumness of a set of states are both **multiplicative** w.r.t. tensor products. (Proven in Audenaert et al `quant-ph/0308120`) This is the topic of the rest of my talk.

Multiplicativity

- Given two ensembles $\mathcal{E}_1 = \{p_i, \psi_i\}$ and $\mathcal{E}_2 = \{q_j, \theta_j\}$, their tensor product is $\mathcal{E}_1 \otimes \mathcal{E}_2 = \{p_i q_j, \psi_i \otimes \theta_j\}$.
- Multiplicativity of accessible fidelity is:

$$F(\mathcal{E}_1 \otimes \mathcal{E}_2) = F(\mathcal{E}_1) F(\mathcal{E}_2).$$

- An eavesdropper cannot benefit from saving up consecutive signal states and performing a global measurement.

Multiplicativity

- Likewise, given two sets $\mathcal{S}_1 = \{\psi_i\}$ and $\mathcal{S}_2 = \{\theta_j\}$, their tensor product is $\mathcal{S}_1 \otimes \mathcal{S}_2 = \{\psi_i \otimes \theta_j\}$.
- Multiplicativity of the quantumness of a set is

$$Q(\mathcal{S}_1 \otimes \mathcal{S}_2) = Q(\mathcal{S}_1) Q(\mathcal{S}_2).$$

- This corresponds to optimal probabilities $p_{i,j}$ being of the form $p_{i,j} = p_i q_j$. Hence, it is not in Ellis' interest either to generate correlations between separate transmissions.
- Surprisingly, quantumness of a Hilbert space is not multiplicative

$$Q(\mathcal{H}_1 \otimes \mathcal{H}_2) = \frac{2}{d_1 d_2 + 1} < Q(\mathcal{H}_1) Q(\mathcal{H}_2).$$

- So it is in Ellis' interest to save up message symbols and encode them into entangled states.
-

Accessible Fidelity, More Explicitly

- The Accessible Fidelity of the ensemble $\{p_i, \psi_i\}$ is

$$F(\{p_i, \psi_i\}) = \sup_{\{E_b, \sigma_b\}} \sum_i p_i \sum_b \text{Tr}[E_b \Psi_i] \text{Tr}[\Psi_i \sigma_b].$$

- The maximisation over the resent states can be done explicitly.
- As the σ_b are completely arbitrary, they can be optimised separately. By Rayleigh-Ritz and the positivity of X , the maximum of $\text{Tr}[X \sigma_b]$ is just $\|X\|$. Thus:

$$\begin{aligned} F(\{p_i, \psi_i\}) &= \sup_{\{E_b, \sigma_b\}} \sum_b \text{Tr} \left[\left(\sum_i p_i \text{Tr}[E_b \Psi_i] \Psi_i \right) \sigma_b \right] \\ &= \sup_{\{E_b\}} \sum_b \left\| \sum_i p_i \text{Tr}[E_b \Psi_i] \Psi_i \right\|. \end{aligned}$$

Accessible Fidelity, More Explicitly

- Let $\Phi(\rho)$ be the map

$$\rho \mapsto \Phi(\rho) := \sum_i p_i \text{Tr}[\rho \Psi_i] \Psi_i,$$

then

$$F(\{p_i, \psi_i\}) = \sup_{\{E_b \geq 0\}} \left\{ \sum_b \|\Phi(E_b)\| : \sum_b E_b = \mathbf{I} \right\},$$

where it has been more explicitly mentioned that the E_b form a POVM.

- This is the first characterisation of Accessible Fidelity we will use.

Accessible Fidelity, Another Way

- We can modify this slightly by introducing the following correspondence:

$$q_b = \text{Tr}[E_b]/d, \quad S_b = E_b/q_b.$$

The point is that the q_b form a probability distribution. This gives

$$F(\{p_i, \psi_i\}) = \sup_{\{q_b, S_b\}} \left\{ \sum_b q_b \|\Phi(S_b)\| : \sum_b q_b S_b = \mathbf{I} \right\},$$

- To a convex analyst, this very much looks like the **Concave Hull** of the function $S \mapsto \|\Phi(S)\|$, evaluated in the identity matrix \mathbf{I} !
- This means we immediately get a **dual** formulation:

$$F(\{p_i, \psi_i\}) = \inf_{X \geq 0} \left\{ \text{Tr}[X \mathbf{I}] : (\forall T \geq 0 : \text{Tr}[XT] \geq \|\Phi(T)\|) \right\}$$

Accessible Fidelity, Another Way

- Some further algebra:
- Putting $X = a\sigma$, $\text{Tr}[\sigma] = 1$, gives

$$\begin{aligned} F(\{p_i, \psi_i\}) &= \inf_{a, \sigma} \{a : (\forall T \geq 0 : a \text{Tr}[\sigma T] \geq \|\Phi(T)\|)\} \\ &= \inf_{a, \sigma} \{a : a \geq \sup_{T \geq 0} \|\Phi(T / \text{Tr}[\sigma T])\|\} \\ &= \inf_{\sigma} \sup_{T \geq 0} \|\Phi(T / \text{Tr}[\sigma T])\| \\ &= \inf_{\sigma} \sup_{\rho} \|\Phi(\sigma^{-1/2} \rho \sigma^{-1/2})\|. \end{aligned}$$

- In the last line we have introduced the normalised state

$$\rho = \sigma^{1/2} T \sigma^{1/2} / \text{Tr}[\sigma T].$$

Accessible Fidelity, Another Way

- In the last expression, we can recognise a well-known quantity!
- The **maximal output purity** of a CP map, as measured by the operator norm $\|\cdot\|$, is defined as

$$\nu_\infty(\Phi) := \sup_{\rho} \|\Phi(\rho)\|.$$

- If we define the CP map

$$\Lambda_\sigma : \rho \mapsto \sigma^{-1/2} \rho \sigma^{-1/2},$$

then we can write

$$\begin{aligned} F(\{p_i, \psi_i\}) &= \inf_{\sigma} \sup_{\rho} \|\Phi(\sigma^{-1/2} \rho \sigma^{-1/2})\| \\ &= \inf_{\sigma} \nu_\infty(\Phi \circ \Lambda_\sigma) \end{aligned}$$

- This is the second characterisation of Accessible Fidelity we will use.
-

Multiplicativity of Accessible Fidelity

- We need to show $F(\mathcal{E}_1 \otimes \mathcal{E}_2) = F(\mathcal{E}_1) F(\mathcal{E}_2)$.
- The inequality $F(\mathcal{E}_1 \otimes \mathcal{E}_2) \geq F(\mathcal{E}_1) F(\mathcal{E}_2)$ follows from the (primal) characterisation

$$F(\{p_i, \psi_i\}) = \sup_{\{E_b\}} \sum_b \|\Phi(E_b)\|,$$

- The CP map Φ corresponding to $\mathcal{E}_1 \otimes \mathcal{E}_2$ is seen to be $\Phi_1 \otimes \Phi_2$.
- By restricting the supremum in $F(\mathcal{E}_1 \otimes \mathcal{E}_2)$ to tensor product POVMs $E_{b,c} = E_b \otimes F_c$, we find as optimum $F(\mathcal{E}_1) F(\mathcal{E}_2)$.

Multiplicativity of Accessible Fidelity

- The opposite inequality $F(\mathcal{E}_1 \otimes \mathcal{E}_2) \leq F(\mathcal{E}_1) F(\mathcal{E}_2)$ follows from the (dual) characterisation

$$F(\{p_i, \psi_i\}) = \inf_{\sigma} \nu_{\infty}(\Phi \circ \Lambda_{\sigma}).$$

- It is crucial to note that the CP map $\Phi \circ \Lambda_{\sigma}$ is **entanglement breaking**.
- Chris King has proven that ν_{∞} is multiplicative for entanglement breaking maps.
- We thus find

$$\begin{aligned} F(\mathcal{E}_1 \otimes \mathcal{E}_2) &= \inf_{\sigma} \nu_{\infty}((\Phi_1 \otimes \Phi_2) \circ \Lambda_{\sigma}) \\ &\leq \inf_{\sigma_1, \sigma_2} \nu_{\infty}((\Phi_1 \otimes \Phi_2) \circ (\Lambda_{\sigma_1} \otimes \Lambda_{\sigma_2})) \\ &= \inf_{\sigma_1, \sigma_2} \nu_{\infty}(\Phi_1 \circ \Lambda_{\sigma_1}) \nu_{\infty}(\Phi_2 \circ \Lambda_{\sigma_2}) \\ &= F(\mathcal{E}_1) F(\mathcal{E}_2). \end{aligned}$$

Multiplicativity of Set Quantumness

- The proof of multiplicativity of set quantumness is, rather surprisingly, completely different and does not rely at all on the previous proof.

Multiplicativity of Set Quantumness

- The proof of multiplicativity of set quantumness is, rather surprisingly, completely different and does not rely at all on the previous proof.
- But I will not bother you with it, so...

Koniec