Lecture 16

Definition 3 (Mixed quantum state)**.** Let $d \in \mathbb{N}$. A d-dimensional mixed (quantum) state is a matrix $\rho \in \mathbb{C}^{d\times d}$ that is Hermitian, positive semi-definite (PSD), and has trace 1.[3]

Quantum states $|\psi\rangle \in \mathbb{C}^d$ are often called "pure quantum states" and can be viewed as mixed quantum states of rank 1 via $|\psi\rangle \leftrightarrow |\psi\rangle\langle\psi|$.

Fact 4. In quantum information, a probability distribution over quantum states $(p_1, |\psi_1\rangle), \ldots, (p_k, |\psi_k\rangle)$ is described as the matrix $\sum_{i=1}^k p_i |\psi_i\rangle\langle\psi_i|$, which can be checked to be a mixed quantum state according to the definition above. The converse also holds in the sense that every mixed quantum state ρ can be written in the form $\sum_{i=1}^k p_i |\psi_i\rangle\langle\psi_i|$, by considering its spectral decomposition.

Comment: the mapping from distribution to matrix is not invertible but it does not destroy information, since the information content of $(p_i, |\psi_i\rangle)$ *is* $\sum_i p_i |\psi_i\rangle\langle\psi_i|$. Put another way: you cannot distinguish between $(p_i, |\psi_i\rangle)$ and $(p'_i, |\psi'_i\rangle)$ using any procedure if their corresponding mixed states are the same. E.g., $(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$ and $(\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle)$.

The effect of a quantum measurement on a mixed quantum state is consistent with the effect of a quantum measurement on (pure) quantum states.

Definition 4 (Schatten p-norms)**.** Let $p \in [1, \infty)$ and $d \in \mathbb{N}$. The Schatten p-norm of $A \in \mathbb{C}^{d\times d}$ is defined to be

$$\|A\|_p \coloneqq [\mathrm{Tr}[(A^\dagger A)^{p/2}]]^{1/p} \tag{10}$$

The Schatten ∞-norm of A is defined to be the the spectral norm of A, which coincides with $\lim_{p\to\infty} \|A\|_p$.

Definition 5 (Fidelity between mixed quantum states)**.** For $\rho, \sigma \in \mathbb{C}^{d\times d}$ that are mixed quantum states, the fidelity between ρ and σ is defined to be

$$F(\rho, \sigma) \coloneqq \|\sqrt{\rho}\sqrt{\sigma}\|_1^2, \tag{11}$$

Comment: 04/03/26: I think I missed a square in the definition I gave of F in class. The above is the correct one.

Comment: have $F(\rho, \sigma) = \mathrm{tr}[|\sqrt{\rho}\sqrt{\sigma}|]^2$, where $|X| \coloneqq \sqrt{X^\dagger X}$. (This definition is symmetric.) Note: for C Hermitian of the form $\sum_i \lambda_i |v_i\rangle\langle v_i|$ with $\lambda_i \geq 0$, $\sqrt{C}$ is defined to be $\sum_i \sqrt{\lambda_i} |v_i\rangle\langle v_i|$. Also $F(A, B) = F(B, A)$ follows from $\mathrm{tr}[|X|] = \mathrm{tr}[|X^\dagger|]$ for any $X \in \mathbb{C}^d$ – think SVD.

Lemma 2 (Pretty Good Measurement)**.** *Let $\rho_1, \ldots, \rho_N \in \mathbb{C}^{d\times d}$ be mixed quantum states. Then there exists a procedure that succeeds in distinguishing them with probability at least $1 - N\sqrt{\max_{a\neq b} F(\rho_a, \rho_b)}$.*

Proof. Omitted. See [Harrow and Winter'06] (which applies von Neumann's minimax theorem to [Barnum and Knill'00]). □

Lemma 3 (Hölder's inequality for Schatten p-norms)**.** *Let $p \in [1, \infty]$ and $p^* \in [1, \infty]$ satisfy $1/p + 1/p^* = 1$. Let $d \in \mathbb{N}$. Then, for $A, B \in \mathbb{C}^{d\times d}$, we have*

$$\|AB\|_1 \leq \|A\|_p \|B\|_{p^*}. \tag{12}$$

Proof. Omitted, non-trivial. Variant more often seen is $|\langle A, B\rangle| \leq \|A\|_p \|B\|_{p^*}$, where $\langle A, B\rangle \coloneqq A^\dagger B$. Here's a reduction to that variant. Let $r \coloneqq \mathrm{rk}(A)$. Write

$$AB = \sum_{i=1}^r \sigma_i |u_i\rangle\langle v_i|, \tag{13}$$

so $\|AB\|_1 = \sum_{i=1}^r \sigma_i$.

Let $U \in \mathbb{C}^{d\times d}$ unitary be such that $U^\dagger |v_i\rangle = |u_i\rangle$. Then

$$AB = \sum_{i=1}^r \sigma_i U^\dagger |v_i\rangle\langle v_i|. \tag{14}$$

So

$$\mathrm{tr}[UAB] = \sum_{i=1}^r \sigma_i. \tag{15}$$

But

$$\mathrm{tr}[UAB] = \langle A^\dagger U^\dagger, B\rangle \leq \|A^\dagger U^\dagger\|_p \|B\|_{p^*} = \|A\|_p \|B\|_{p^*}, \tag{16}$$

where the last equality uses the unitary invariance of the Schatten p-norm and its invariance under conjugate transpose. □

[3] In fact, the usual PSD definition, i.e., $u^\dagger \rho u \geq 0$ for all $u \in \mathbb{C}^d$, implies ρ has to be Hermitian; so the Hermitian part of the definition is somewhat redundant.

Remark 3. Further ingredients: von Neumann's trace inequality: $|\operatorname{tr}[AB]| \leq \sum_{i=1}^{d} \sigma_i(A)\sigma_i(B)$ (see [Stackexchange post]) and the normal Hölder's inequality.

The next lemma follows from Hölder's inequality with $p = 2$.

Lemma 4. *Let ρ, σ be mixed quantum states. Then $F(\rho, \sigma) \leq \operatorname{tr}[\Pi_\rho \cdot \sigma]$, where Π_ρ is the orthogonal projector onto the support of ρ.*

Proof. Have $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2 = \|\sqrt{\rho} \cdot \Pi_\rho \sqrt{\sigma}\|_1^2 \leq \|\sqrt{\rho}\|_2^2 \cdot \|\Pi_\rho\sqrt{\sigma}\|_2^2 = \operatorname{tr}[\rho] \cdot \operatorname{tr}[\sqrt{\sigma}\Pi_\rho\sqrt{\sigma}] = \operatorname{tr}[\Pi_\rho\sigma]$. □

Lemma 5. *Let G be a finite group, $H, H' \leq G$ (subgroups of G), and $g, g' \in G$. Then*

$$|gH \cap g'H'| = \begin{cases} |H \cap H'| & \text{if } g^{-1}g' \in HH', \\ 0 & \text{otherwise.} \end{cases} \tag{17}$$

Proof. See Homework 2. □

Lemma 6. *Let G be a finite group. Then G has at most $|G|^{\log_2 |G|} = 2^{(\log_2 |G|)^2}$ subgroups.*

Proof. For distinct elements $g_1, \ldots, g_k$, the subgroup they generate is the subgroup formed by all words of the form $g_{i_1}^{b_1} \ldots g_{i_l}^{b_l}$, where $b_j \in \{-1, 1\}$ and $i_j \in [k]$ (the empty word corresponds to e). Written $\langle g_1, \ldots, g_k \rangle$. We say the g_is are independent generators of $\langle g_1, \ldots, g_k \rangle$ if $g_i \notin \langle \{g_j : j \neq i\} \rangle$ for all i.

Every subgroup can be specified by a finite number k of independent generators. Moreover, the number of elements in the subgroup is at least 2^k. This can be seen by induction: true for $k = 0$ (the empty set generates the subgroup $\{e\}$), suppose true for $k-1$, then group axioms imply that $\{g_k h \mid h \in \langle g_1, \ldots, g_{k-1} \rangle\}$ has at least 2^{k-1} elements, none of which are in $\langle g_1, \ldots, g_{k-1} \rangle$ as $g_k \notin \langle g_1, \ldots, g_{k-1} \rangle$. So $k \leq \log_2 |G|$.

Since e cannot be an independent generator, the number of choices of independent generators is at most

$$\binom{|G| - 1}{\leq \log_2 |G|} \leq (|G| - 1 + 1)^{\log_2 |G|}, \tag{18}$$

where the inequality follows by considering the number of ways of choosing one or zero elements from $|G| - 1$ elements.[4] □

All of the above serves as preliminaries for the following result.

Proposition 1. *Let G be a finite group. Let $\mathcal{H}$ be the set of all subgroups of G. Then $Q(\mathrm{HSP}(G, \mathcal{H})) = O(\log^2(|G|))$.*

Proof. We will cover this following Chapter 10.3 of [AMC]. □

[4] In fact, the inequality is loose and also holds if the LHS counts ordered tuples rather than subsets. However, it does yield the right "order-of-magnitude", see Corollary 1.6 in this paper and the surrounding text.