CS 766/QIC 820 Theory of Quantum Information (Fall 2011)

Lecture 14: Separable operators

For the next several lectures we will be discussing various aspects and properties of *entanglement*. Mathematically speaking, we define entanglement in terms of what it is not, rather than what it is: we define the notion of a *separable operator*, and define that any density operator that is not separable represents an entangled state.

14.1 Definition and basic properties of separable operators

Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces. A positive semidefinite operator $P \in \operatorname{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is *separable* if and only if there exists a positive integer m and positive semidefinite operators

$$Q_1, \ldots, Q_m \in \operatorname{Pos}(\mathcal{X}) \qquad \text{and} \qquad R_1, \ldots, R_m \in \operatorname{Pos}(\mathcal{Y})$$

such that

$$P = \sum_{j=1}^{m} Q_j \otimes R_j. \tag{14.1}$$

We will write $\operatorname{Sep}(\mathcal{X} : \mathcal{Y})$ to denote the collection of all such operators.[1] It is the case that $\operatorname{Sep}(\mathcal{X} : \mathcal{Y})$ is a convex cone, and it is not difficult to prove that $\operatorname{Sep}(\mathcal{X} : \mathcal{Y})$ is properly contained in $\operatorname{Pos}(\mathcal{X} \otimes \mathcal{Y})$. (We will see that this is so later in the lecture.) Operators $P \in \operatorname{Pos}(\mathcal{X} \otimes \mathcal{Y})$ that are not contained in $\operatorname{Sep}(\mathcal{X} : \mathcal{Y})$ are said to be *entangled*.

Let us also define

$$\operatorname{SepD}(\mathcal{X} : \mathcal{Y}) = \operatorname{Sep}(\mathcal{X} : \mathcal{Y}) \cap \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$$

to be the set of separable density operators acting on $\mathcal{X} \otimes \mathcal{Y}$. By thinking about spectral decompositions, one sees immediately that the set of separable density operators is equal to the convex hull of the pure product density operators:

$$\operatorname{SepD}(\mathcal{X} : \mathcal{Y}) = \operatorname{conv}\{xx^* \otimes yy^* \,:\, x \in \mathrm{S}(\mathcal{X}),\ y \in \mathrm{S}(\mathcal{Y})\}.$$

Thus, every element $\rho \in \operatorname{SepD}(\mathcal{X} : \mathcal{Y})$ may be expressed as

$$\rho = \sum_{j=1}^{m} p_j \, x_j x_j^* \otimes y_j y_j^* \tag{14.2}$$

for some choice of $m \geq 1$, a probability vector $p = (p_1, \ldots, p_m)$, and unit vectors $x_1, \ldots, x_m \in \mathcal{X}$ and $y_1, \ldots, y_m \in \mathcal{Y}$.

A few words about the intuitive meaning of states in $\operatorname{SepD}(\mathcal{X} : \mathcal{Y})$ follow. Suppose X and Y are registers in a separable state $\rho \in \operatorname{SepD}(\mathcal{X} : \mathcal{Y})$. It may be the case that X and Y are correlated,

[1] One may extend this definition to any number of spaces, defining (for instance) $\operatorname{Sep}(\mathcal{X}_1 : \mathcal{X}_2 : \cdots : \mathcal{X}_n)$ in the natural way. Our focus, however, will be on *bipartite entanglement* rather than *multipartite entanglement*, and so we will not consider this extension further.

given that ρ does not necessarily take the form of a product state $\rho = \sigma \otimes \xi$ for $\sigma \in \mathrm{D}(\mathcal{X})$ and $\xi \in \mathrm{D}(\mathcal{Y})$. However, any correlations between X and Y are in some sense classical, because ρ is a convex combination of product states. This places a strong limitation on the possible correlations between X and Y that may exist, as compared to non-separable (or entangled) states. A simple example is teleportation, discussed in Lecture 6: any attempt to substitute a separable state for the types of states we used for teleportation is doomed to fail.

A simple application of Carathéodory's Theorem establishes that for every separable state $\rho \in \mathrm{SepD}(\mathcal{X} : \mathcal{Y})$, there exists an expression of the form (14.2) for some choice of $m \leq \dim(\mathcal{X} \otimes \mathcal{Y})^2$. Notice that $\mathrm{Sep}(\mathcal{X} : \mathcal{Y})$ is the cone generated by $\mathrm{SepD}(\mathcal{X} : \mathcal{Y})$:

$$\mathrm{Sep}(\mathcal{X} : \mathcal{Y}) = \{\lambda\rho \,:\, \lambda \geq 0,\, \rho \in \mathrm{SepD}(\mathcal{X} : \mathcal{Y})\}.$$

The same bound $m \leq \dim(\mathcal{X} \otimes \mathcal{Y})^2$ may therefore be taken for some expression (14.1) of any $P \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y})$.

Next, let us note that $\mathrm{SepD}(\mathcal{X} : \mathcal{Y})$ is a compact set. To see this, we first observe that the unit spheres $\mathrm{S}(\mathcal{X})$ and $\mathrm{S}(\mathcal{Y})$ are compact, and therefore so too is the Cartesian product $\mathrm{S}(\mathcal{X}) \times \mathrm{S}(\mathcal{Y})$. The function

$$f : \mathcal{X} \times \mathcal{Y} \to \mathrm{L}(\mathcal{X} \otimes \mathcal{Y}) : (x, y) \mapsto xx^* \otimes yy^*$$

is continuous, and continuous functions map compact sets to compact sets, so the set

$$\{xx^* \otimes yy^* \,:\, x \in \mathrm{S}(\mathcal{X}),\, y \in \mathrm{S}(\mathcal{Y})\}$$

is compact as well. Finally, it is a basic fact from convex analysis that the convex hull of any compact set is compact.

The set $\mathrm{Sep}(\mathcal{X} \otimes \mathcal{Y})$ is of course not compact, given that it is not bounded. It is a closed, convex cone, however, because it is the cone generated by a compact, convex set that does not contain the origin.

14.2 The Woronowicz–Horodecki criterion

Next we will discuss a necessary and sufficient condition for a given positive semidefinite operator to be separable. Although this condition, sometimes known as the *Woronowicz–Horodecki criterion*, does not give us an efficiently computable method to determine whether or not an operator is separable, it is useful nevertheless in an analytic sense.

The Woronowicz–Horodecki criterion is based on the fundamental fact from convex analysis that says that closed convex sets are determined by the closed half-spaces that contain them. Here is one version of this fact that is well-suited to our needs.

Fact. Let $\mathcal{X}$ be a complex Euclidean space and let $\mathcal{A} \subset \mathrm{Herm}(\mathcal{X})$ be a closed, convex cone. For any choice of an operator $B \in \mathrm{Herm}(\mathcal{X})$ with $B \notin \mathcal{A}$, there exists an operator $H \in \mathrm{Herm}(\mathcal{X})$ such that

1. $\langle H, A \rangle \geq 0$ for all $A \in \mathcal{A}$, and
2. $\langle H, B \rangle < 0$.

It should be noted that the particular statement above is only valid for closed convex cones, not general closed convex sets. For a general closed, convex set, it may be necessary to replace 0 with some other real scalar for each choice of B.

Theorem 14.1 (Woronowicz–Horodecki criterion)**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$. It holds that $P \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y})$ if and only if*

$$(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Y})$$

for every positive and unital mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$.

Proof. One direction of the proof is simple. If $P \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y})$, then we have

$$P = \sum_{j=1}^{m} Q_j \otimes R_j$$

for some choice of $Q_1, \ldots, Q_m \in \mathrm{Pos}(\mathcal{X})$ and $R_1, \ldots, R_m \in \mathrm{Pos}(\mathcal{Y})$. Thus, for every positive mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ we have

$$(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P) = \sum_{j=1}^{m} \Phi(Q_j) \otimes R_j \in \mathrm{Sep}(\mathcal{Y} : \mathcal{Y}) \subset \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Y}).$$

A similar fact holds for any choice of a positive mapping $\Psi \in \mathrm{T}(\mathcal{X}, \mathcal{W})$, for $\mathcal{W}$ being any complex Euclidean space, taken in place of Φ, by similar reasoning.

Let us now assume that $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is not separable. The fact stated above, there must exist a Hermitian operator $H \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y})$ such that:

1. $\langle H, Q \otimes R \rangle \geq 0$ for all $Q \in \mathrm{Pos}(\mathcal{X})$ and $R \in \mathrm{Pos}(\mathcal{Y})$, and
2. $\langle H, P \rangle < 0$.

Let $\Psi \in \mathrm{T}(\mathcal{Y}, \mathcal{X})$ be the unique mapping for which $J(\Psi) = H$. For any $Q \in \mathrm{Pos}(\mathcal{X})$ and $R \in \mathrm{Pos}(\mathcal{Y})$ we therefore have

$$\begin{aligned}
0 \leq \langle H, Q \otimes R \rangle &= \left\langle (\Psi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})}) \left(\mathrm{vec}(\mathbb{1}_{\mathcal{Y}}) \, \mathrm{vec}(\mathbb{1}_{\mathcal{Y}})^*\right), Q \otimes R \right\rangle \\
&= \langle \mathrm{vec}(\mathbb{1}_{\mathcal{Y}}) \, \mathrm{vec}(\mathbb{1}_{\mathcal{Y}})^*, \Psi^*(Q) \otimes R \rangle = \mathrm{vec}(\mathbb{1}_{\mathcal{Y}})^* \left(\Psi^*(Q) \otimes R\right) \mathrm{vec}(\mathbb{1}_{\mathcal{Y}}) \\
&= \mathrm{Tr}\left(\Psi^*(Q) R^{\mathsf{T}}\right) = \left\langle \overline{R}, \Psi^*(Q) \right\rangle.
\end{aligned}$$

From this we conclude that Ψ^* is a positive mapping.

Suppose for the moment that we do not care about the unital condition on Φ that is required by the statement of the theorem. We could then take $\Phi = \Psi^*$ to complete the proof, because

$$\begin{aligned}
\mathrm{vec}(\mathbb{1}_{\mathcal{Y}})^* \left((\Psi^* \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P) \right) \mathrm{vec}(\mathbb{1}_{\mathcal{Y}}) &= \left\langle \mathrm{vec}(\mathbb{1}_{\mathcal{Y}}) \, \mathrm{vec}(\mathbb{1}_{\mathcal{Y}})^*, \left(\Psi^* \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})}\right)(P) \right\rangle \\
&= \left\langle (\Psi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})}) \left(\mathrm{vec}(\mathbb{1}_{\mathcal{Y}}) \, \mathrm{vec}(\mathbb{1}_{\mathcal{Y}})^*\right), P \right\rangle = \langle H, P \rangle < 0,
\end{aligned}$$

establishing that $(\Psi^* \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P)$ is not positive semidefinite.

To obtain a mapping Φ that is unital, and satisfies the condition that $(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P)$ is not positive semidefinite, we will simply tweak Ψ^* a bit. First, given that $\langle H, P \rangle < 0$, we may choose $\varepsilon > 0$ sufficiently small so that

$$\langle H, P \rangle + \varepsilon \, \mathrm{Tr}(P) < 0.$$

Now define $\Xi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ as

$$\Xi(X) = \Psi^*(X) + \varepsilon \, \mathrm{Tr}(X) \mathbb{1}_{\mathcal{Y}}$$

for all $X \in \mathrm{L}(\mathcal{X})$, and let $A = \Xi(\mathbb{1}_{\mathcal{X}})$. Given that Ψ^* is positive and ε is greater than zero, it follows that $A \in \mathrm{Pd}(\mathcal{Y})$, and so we may define $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ as

$$\Phi(X) = A^{-1/2}\Xi(X)A^{-1/2}$$

for every $X \in \mathrm{L}(\mathcal{X})$.

It is clear that Φ is both positive and unital, and it remains to prove that $(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P)$ is not positive semidefinite. This may be verified as follows:

$$\begin{aligned}
&\left\langle \operatorname{vec}\left(\sqrt{A}\right) \operatorname{vec}\left(\sqrt{A}\right)^*, (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P) \right\rangle \\
&\qquad = \left\langle \operatorname{vec}(\mathbb{1}_{\mathcal{Y}}) \operatorname{vec}(\mathbb{1}_{\mathcal{Y}})^*, (\Xi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P) \right\rangle \\
&\qquad = \left\langle (\Xi^* \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})}) \left(\operatorname{vec}(\mathbb{1}_{\mathcal{Y}}) \operatorname{vec}(\mathbb{1}_{\mathcal{Y}})^*\right), P \right\rangle \\
&\qquad = \langle J(\Xi^*), P \rangle \\
&\qquad = \langle J(\Psi) + \varepsilon \mathbb{1}_{\mathcal{Y}\otimes\mathcal{X}}, P \rangle \\
&\qquad = \langle H, P \rangle + \varepsilon \operatorname{Tr}(P) \\
&\qquad < 0.
\end{aligned}$$

It follows that $(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(P)$ is not positive semidefinite, and so the proof is complete. □

This theorem allows us to easily prove that certain positive semidefinite operators are not separable. For example, consider the operator

$$P = \frac{1}{n} \operatorname{vec}(\mathbb{1}_{\mathcal{X}}) \operatorname{vec}(\mathbb{1}_{\mathcal{X}})^*$$

for $\mathcal{X} = \mathbb{C}^{\Sigma}$, $|\Sigma| = n$. We consider the transposition mapping $T \in \mathrm{T}(\mathcal{X})$, which is positive and unital. We have

$$(T \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(P) = \frac{1}{n} \sum_{a,b\in\Sigma} E_{b,a} \otimes E_{a,b} = \frac{1}{n} W,$$

for $W \in \mathrm{L}(\mathcal{X} \otimes \mathcal{X})$ being the *swap operator*: $W(u \otimes v) = v \otimes u$ for all $u, v \in \mathcal{X}$. This operator is not positive semidefinite (provided $n \geq 2$), which is easily verified by noting that W has negative eigenvalues. For instance,

$$W(e_a \otimes e_b - e_b \otimes e_a) = -(e_a \otimes e_b - e_b \otimes e_a)$$

for $a \neq b$. We therefore have that P is not separable by Theorem 14.1.

14.3 Separable ball around the identity

Finally, we will prove that there exists a small region around the identity operator $\mathbb{1}_{\mathcal{X}} \otimes \mathbb{1}_{\mathcal{Y}}$ where *every* Hermitian operator is separable. This fact gives us an intuitive connection between noise and entanglement, which is that entanglement cannot exist in the presence of too much noise.

We will need two facts, beyond those we have already proved, to establish this result. The first is straightforward, and is as follows.

Lemma 14.2. *Let $\mathcal{X}$ and $\mathcal{Y} = \mathbb{C}^{\Sigma}$ be complex Euclidean spaces, and consider an operator $A \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$ given by*

$$A = \sum_{a,b \in \Sigma} A_{a,b} \otimes E_{a,b}$$

for $\{A_{a,b} : a, b \in \Sigma\} \subset \mathrm{L}(\mathcal{X})$. It holds that

$$\|A\|^2 \leq \sum_{a,b \in \Sigma} \|A_{a,b}\|^2 .$$

Proof. For each $a \in \Sigma$ define

$$B_a = \sum_{b \in \Sigma} A_{a,b} \otimes E_{a,b}.$$

We have that

$$\|B_a B_a^*\| = \left\| \sum_{b \in \Sigma} A_{a,b} A_{a,b}^* \otimes E_{a,a} \right\| \leq \sum_{b \in \Sigma} \|A_{a,b} A_{a,b}^*\| = \sum_{b \in \Sigma} \|A_{a,b}\|^2 .$$

Now,

$$A = \sum_{a \in \Sigma} B_a,$$

and given that $B_a^* B_b = 0$ for $a \neq b$, we have that

$$A^* A = \sum_{a \in \Sigma} B_a^* B_a.$$

Therefore

$$\|A\|^2 = \|A^* A\| \leq \sum_{a \in \Sigma} \|B_a^* B_a\| \leq \sum_{a,b \in \Sigma} \|A_{a,b}\|^2$$

as claimed. $\square$

The second fact that we need is a theorem about positive unital mappings, which says that they cannot increase the spectral norm of operators.

Theorem 14.3 (Russo–Dye)**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be positive and unital. It holds that*

$$\|\Phi(X)\| \leq \|X\|$$

for every $X \in \mathrm{L}(\mathcal{X})$.

Proof. Let us first prove that $\|\Phi(U)\| \leq 1$ for every unitary operator $U \in \mathrm{U}(\mathcal{X})$. Assume $\mathcal{X} = \mathbb{C}^{\Sigma}$, and let

$$U = \sum_{a \in \Sigma} \lambda_a \, u_a u_a^*$$

be a spectral decomposition of U. It holds that

$$\Phi(U) = \sum_{a \in \Sigma} \lambda_a \Phi(u_a u_a^*) = \sum_{a \in \Sigma} \lambda_a P_a,$$

where $P_a = \Phi(u_a u_a^*)$ for each $a \in \Sigma$. As Φ is positive, we have that $P_a \in \mathrm{Pos}(\mathcal{Y})$ for each $a \in \Sigma$, and given that Φ is unital we have

$$\sum_{a \in \Sigma} P_a = \mathbb{1}_{\mathcal{Y}}.$$

By Naimark's Theorem there exists a linear isometry $A \in \mathrm{U}(\mathcal{Y}, \mathcal{Y} \otimes \mathcal{X})$ such that

$$P_a = A^*(\mathbb{1}_{\mathcal{Y}} \otimes E_{a,a})A$$

for each $a \in \Sigma$, and therefore

$$\Phi(U) = A^* \left(\sum_{a \in \Sigma} \lambda_a \mathbb{1}_{\mathcal{Y}} \otimes E_{a,a} \right) A = A^*(\mathbb{1}_{\mathcal{Y}} \otimes VUV^*)A$$

for

$$V = \sum_{a \in \Sigma} e_a u_a^*.$$

As U and V are unitary and A is an isometry, the bound $\|\Phi(U)\| \leq 1$ follows from the submultiplicativity of the spectral norm.

For general X, it suffices to prove $\|\Phi(X)\| \leq 1$ whenever $\|X\| \leq 1$. Because every operator $X \in \mathrm{L}(\mathcal{X})$ with $\|X\| \leq 1$ can be expressed as a convex combination of unitary operators, the required bound follows from the convexity of the spectral norm. □

Theorem 14.4. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and suppose that $A \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y})$ satisfies $\|A\|_2 \leq 1$. It holds that*

$$\mathbb{1}_{\mathcal{X} \otimes \mathcal{Y}} - A \in \mathrm{Sep}(\mathcal{X} : \mathcal{Y}).$$

Proof. Let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be positive and unital. Assume $\mathcal{Y} = \mathbb{C}^\Sigma$ and write

$$A = \sum_{a,b \in \Sigma} A_{a,b} \otimes E_{a,b}.$$

We have

$$(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(A) = \sum_{a,b \in \Sigma} \Phi(A_{a,b}) \otimes E_{a,b},$$

and therefore

$$\left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(A) \right\|^2 \leq \sum_{a,b \in \Sigma} \|\Phi(A_{a,b})\|^2 \leq \sum_{a,b \in \Sigma} \|A_{a,b}\|^2 \leq \sum_{a,b \in \Sigma} \|A_{a,b}\|_2^2 = \|A\|_2^2 \leq 1.$$

The first inequality is by Lemma 14.2 and the second inequality is by Theorem 14.3. The positivity of Φ implies that $(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(A)$ is Hermitian, and thus $(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(A) \leq \mathbb{1}_{\mathcal{Y} \otimes \mathcal{Y}}$. Therefore we have

$$(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(\mathbb{1}_{\mathcal{X} \otimes \mathcal{Y}} - A) = \mathbb{1}_{\mathcal{Y} \otimes \mathcal{Y}} - (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(A) \geq 0.$$

As this holds for all positive and unital mappings Φ, we have that $\mathbb{1}_{\mathcal{X} \otimes \mathcal{Y}} - A$ is separable by Theorem 14.1. □