Lecture 15: Separable mappings and the LOCC paradigm

In the previous lecture we discussed separable operators. The focus of this lecture will be on analogous concepts for mappings between operator spaces. In particular, we will discuss *separable channels*, as well as the important subclass of *LOCC channels*. The acronym LOCC is short for *local operations and classical communication*, and plays a central role in the study of entanglement.

15.1 Min-rank

Before discussing separable and LOCC channels, it will be helpful to briefly discuss a generalization of the concept of separability for operators.

Suppose two complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$ are fixed, and for a given choice of a non-negative integer k let us consider the collection of operators

$$\mathrm{R}_k\left(\mathcal{X}:\mathcal{Y}\right) = \mathrm{conv}\left\{\mathrm{vec}(A)\,\mathrm{vec}(A)^* \ : \ A \in \mathrm{L}\left(\mathcal{Y},\mathcal{X}\right),\,\mathrm{rank}(A) \leq k\right\}.$$

In other words, a given positive semidefinite operator $P \in \mathrm{Pos}\left(\mathcal{X} \otimes \mathcal{Y}\right)$ is contained in $\mathrm{R}_k\left(\mathcal{X}:\mathcal{Y}\right)$ if and only if it is possible to write

$$P = \sum_{j=1}^{m} \mathrm{vec}(A_j)\,\mathrm{vec}(A_j)^*$$

for some choice of an integer m and operators $A_1,\ldots,A_m \in \mathrm{L}\left(\mathcal{Y},\mathcal{X}\right)$, each having rank at most k. This sort of expression does not require orthogonality of the operators $A_1,\ldots,A_m$, and it is not necessarily the case that a spectral decomposition of P will yield a collection of operators for which the rank is minimized.

Each of the sets $\mathrm{R}_k\left(\mathcal{X}:\mathcal{Y}\right)$ is a closed convex cone. It is easy to see that

$$\mathrm{R}_0\left(\mathcal{X}:\mathcal{Y}\right) = \{0\}, \quad \mathrm{R}_1\left(\mathcal{X}:\mathcal{Y}\right) = \mathrm{Sep}\left(\mathcal{X}:\mathcal{Y}\right), \quad \text{and} \quad \mathrm{R}_n\left(\mathcal{X}:\mathcal{Y}\right) = \mathrm{Pos}\left(\mathcal{X} \otimes \mathcal{Y}\right)$$

for $n \geq \min\{\dim(\mathcal{X}),\dim(\mathcal{Y})\}$. Moreover,

$$\mathrm{R}_k\left(\mathcal{X}:\mathcal{Y}\right) \subsetneq \mathrm{R}_{k+1}\left(\mathcal{X}:\mathcal{Y}\right)$$

for $0 \leq k < \min\{\dim(\mathcal{X}),\dim(\mathcal{Y})\}$, as $\mathrm{vec}(A)\,\mathrm{vec}(A)^*$ is contained in the set $\mathrm{R}_r\left(\mathcal{X}:\mathcal{Y}\right)$ but not the set $\mathrm{R}_{r-1}\left(\mathcal{X}:\mathcal{Y}\right)$ for $r = \mathrm{rank}(A)$.

Finally, for each positive semidefinite operator $P \in \mathrm{Pos}\left(\mathcal{X} \otimes \mathcal{Y}\right)$, we define the *min-rank* of P as

$$\text{min-rank}(P) = \min\left\{k \geq 0 \ : \ P \in \mathrm{R}_k\left(\mathcal{X}:\mathcal{Y}\right)\right\}.$$

This quantity is more commonly known as the *Schmidt number*, named after Erhard Schmidt. There is no evidence that he ever considered this concept or anything analogous—his name has presumably been associated with it because of its connection to the Schmidt decomposition.

15.2 Separable mappings between operator spaces

A completely positive mapping $\Phi \in T(\mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{Y}_B)$, is said to be *separable* if and only if there exists operators $A_1, \dots, A_m \in L(\mathcal{X}_A, \mathcal{Y}_A)$ and $B_1, \dots, B_m \in L(\mathcal{X}_B, \mathcal{Y}_B)$ such that

$$\Phi(X) = \sum_{j=1}^{m} (A_j \otimes B_j) X (A_j \otimes B_j)^* \tag{15.1}$$

for all $X \in L(\mathcal{X}_A \otimes \mathcal{X}_B)$. This condition is equivalent to saying that Φ is a nonnegative linear combination of tensor products of completely positive mappings. We denote the set of all such separable mappings as

$$\text{SepT}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B).$$

When we refer to a *separable channel*, we (of course) mean a channel that is a separable mapping, and we write

$$\text{SepC}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B) = \text{SepT}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B) \cap C(\mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{Y}_B)$$

to denote the set of separable channels (for a particular choice of $\mathcal{X}_A$, $\mathcal{X}_B$, $\mathcal{Y}_A$, and $\mathcal{Y}_B$).

The use of the term *separable* to describe mappings of the above form is consistent with the following observation.

Proposition 15.1. *Let* $\Phi \in T(\mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{Y}_B)$ *be a mapping. It holds that*

$$\Phi \in \text{SepT}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$$

if and only if

$$J(\Phi) \in \text{Sep}(\mathcal{Y}_A \otimes \mathcal{X}_A : \mathcal{Y}_B \otimes \mathcal{X}_B).$$

Remark 15.2. The statement of this proposition is deserving of a short discussion. If it is the case that

$$\Phi \in T(\mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{Y}_B),$$

then it holds that

$$J(\Phi) \in L(\mathcal{Y}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_A \otimes \mathcal{X}_B).$$

The set $\text{Sep}(\mathcal{Y}_A \otimes \mathcal{X}_A : \mathcal{Y}_B \otimes \mathcal{X}_B)$, on the other hand, is a subset of $L(\mathcal{Y}_A \otimes \mathcal{X}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_B)$, not $L(\mathcal{Y}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_A \otimes \mathcal{X}_B)$; the tensor factors are not appearing in the proper order to make sense of the proposition. To state the proposition more formally, we should take into account that a permutation of tensor factors is needed.

To do this, let us define an operator $W \in L(\mathcal{Y}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{X}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_B)$ by the action

$$W(y_A \otimes y_B \otimes x_A \otimes x_B) = y_A \otimes x_A \otimes y_B \otimes x_B$$

on vectors $x_A \in \mathcal{X}_A$, $x_B \in \mathcal{X}_B$, $y_A \in \mathcal{Y}_A$, and $y_B \in \mathcal{Y}_B$. The mapping W is like a unitary operator, in the sense that it is a norm preserving and invertible linear mapping. (It is not exactly a unitary operator as we defined them in Lecture 1 because it does not map a space to itself, but this is really just a minor point about a choice of terminology.) Rather than writing

$$J(\Phi) \in \text{Sep}(\mathcal{Y}_A \otimes \mathcal{X}_A : \mathcal{Y}_B \otimes \mathcal{X}_B)$$

in the proposition, we should write

$$WJ(\Phi)W^* \in \text{Sep}\,(\mathcal{Y}_A \otimes \mathcal{X}_A : \mathcal{Y}_B \otimes \mathcal{X}_B)\,.$$

Omitting permutations of tensor factors like this is common in quantum information theory. When every space being discussed has its own name, there is often no ambiguity in omitting references to permutation operators such as W because it is implicit that they should be there, and it can become something of a distraction to refer to them explicitly.

Proof. Given an expression (15.1) for Φ, we have

$$J(\Phi) = \sum_{j=1}^m \text{vec}(A_j)\,\text{vec}(A_j)^* \otimes \text{vec}(B_j)\,\text{vec}(B_j)^* \in \text{Sep}\,(\mathcal{Y}_A \otimes \mathcal{X}_A : \mathcal{Y}_B \otimes \mathcal{X}_B)\,.$$

On the other hand, if $J(\Phi) \in \text{Sep}\,(\mathcal{Y}_A \otimes \mathcal{X}_A : \mathcal{Y}_B \otimes \mathcal{X}_B)$ we may write

$$J(\Phi) = \sum_{j=1}^m \text{vec}(A_j)\,\text{vec}(A_j)^* \otimes \text{vec}(B_j)\,\text{vec}(B_j)^*$$

for some choice of operators $A_1, \dots, A_m \in \text{L}\,(\mathcal{X}_A, \mathcal{Y}_A)$ and $B_1, \dots, B_m \in \text{L}\,(\mathcal{X}_B, \mathcal{Y}_B)$. This implies Φ may be expressed in the form (15.1). $\square$

Let us now observe the simple and yet useful fact that separable mappings cannot increase min-rank. This implies, in particular, that separable mappings cannot create entanglement out of thin air: if a separable operator is input to a separable mapping, the output will also be separable.

Theorem 15.3. *Let $\Phi \in \text{SepT}\,(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$ be a separable mapping and let $P \in \text{R}_k\,(\mathcal{X}_A : \mathcal{X}_B)$. It holds that*

$$\Phi(P) \in \text{R}_k\,(\mathcal{Y}_A : \mathcal{Y}_B)\,.$$

In other words, $\text{min-rank}(\Phi(Q)) \leq \text{min-rank}(Q)$ *for every* $Q \in \text{Pos}\,(\mathcal{X}_A \otimes \mathcal{X}_B)$.

Proof. Assume $A_1, \dots, A_m \in \text{L}\,(\mathcal{X}_A, \mathcal{Y}_A)$ and $B_1, \dots, B_m \in \text{L}\,(\mathcal{X}_B, \mathcal{Y}_B)$ satisfy

$$\Phi(X) = \sum_{j=1}^m (A_j \otimes B_j)X(A_j \otimes B_j)^*$$

for all $X \in \text{L}\,(\mathcal{X}_A \otimes \mathcal{X}_B)$. For any choice of $Y \in \text{L}\,(\mathcal{X}_B, \mathcal{X}_A)$ we have

$$\Phi(\text{vec}(Y)\,\text{vec}(Y)^*) = \sum_{j=1}^m \text{vec}\left(A_j Y B_j^\mathsf{T}\right)\text{vec}\left(A_j Y B_j^\mathsf{T}\right)^*\,.$$

As

$$\text{rank}\left(A_j Y B_j^\mathsf{T}\right) \leq \text{rank}(Y)$$

for each $j = 1, \dots, m$, it holds that

$$\Phi(\text{vec}(Y)\,\text{vec}(Y)^*) \in \text{R}_r\,(\mathcal{Y}_A : \mathcal{Y}_B)$$

for $r = \text{rank}(Y)$. The theorem follows by convexity. $\square$

Finally, let us note that the separable mappings are closed under composition, as the following proposition claims.

Proposition 15.4. *Suppose* $\Phi \in \mathrm{SepT}\,(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$ *and* $\Psi \in \mathrm{SepT}\,(\mathcal{Y}_A, \mathcal{Z}_A : \mathcal{Y}_B, \mathcal{Z}_B)$. *It holds that* $\Psi\Phi \in \mathrm{SepT}\,(\mathcal{X}_A, \mathcal{Z}_A : \mathcal{X}_B, \mathcal{Z}_B)$.

Proof. Suppose

$$\Phi(X) = \sum_{j=1}^{m} (A_j \otimes B_j) X (A_j \otimes B_j)^*$$

and

$$\Psi(Y) = \sum_{k=1}^{n} (C_k \otimes D_k) Y (C_k \otimes D_k)^*.$$

It follows that

$$(\Psi\Phi)(X) = \sum_{k=1}^{n} \sum_{j=1}^{m} \left[(C_k A_j) \otimes (D_k B_j)\right] X \left[(C_k A_j) \otimes (D_k B_j)\right]^*,$$

which has the required form for separability. $\qquad\square$

15.3 LOCC channels

We will now discuss LOCC channels, or channels implementable by *local operations and classical communication*. Here we are considering the situation in which two parties, Alice and Bob, collectively perform some sequence of operations and/or measurements on a shared quantum system, with the restriction that quantum operations must be performed locally, and all communication between them must be classical. LOCC channels will be defined, in mathematical terms, as those that can obtained as follows.

1. Alice and Bob can independently apply channels to their own registers, independently of the other player.

2. Alice can transmit information to Bob through a classical channel, and likewise Bob can transmit information to Alice through a classical channel.

3. Alice and Bob can compose any finite number of operations that correspond to items 1 and 2.

Many problems and results in quantum information theory concern LOCC channels in one form or another, often involving Alice and Bob's ability to manipulate entangled states by means of such operations.

15.3.1 Definition of LOCC channels

Let us begin with a straightforward formal definition of LOCC channels. There are many other equivalent ways that one could define this class; we are simply picking one way.

Product channels

Let $\mathcal{X}_A, \mathcal{X}_B, \mathcal{Y}_A, \mathcal{Y}_B$ be complex Euclidean spaces and suppose that $\Phi_A \in \mathrm{C}\,(\mathcal{X}_A, \mathcal{Y}_A)$ and $\Phi_B \in \mathrm{C}\,(\mathcal{X}_B, \mathcal{Y}_B)$ are channels. The mapping

$$\Phi_A \otimes \Phi_B \in \mathrm{C}\,(\mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{Y}_B)$$

is then said to be a *product channel*. Such a channel represents the situation in which Alice and Bob perform independent operations on their own quantum systems.

Classical communication channels

Let $\mathcal{X}_A$, $\mathcal{X}_B$, and $\mathcal{Z}$ be complex Euclidean spaces, and assume $\mathcal{Z} = \mathbb{C}^\Sigma$ for Σ being a finite and nonempty set. Let $\Delta \in C\left(\mathcal{Z}\right)$ denote the *completely dephasing channel*

$$\Delta(Z) = \sum_{a \in \Sigma} Z(a,a) E_{a,a}.$$

This channel may be viewed as a perfect classical communication channel that transmits symbols in the set Σ without error. It may equivalently be seen as a quantum channel that measures everything sent into it with respect to the standard basis of $\mathcal{Z}$, transmitting the result to the receiver.

Now, the channel

$$\Phi \in C\left(\left(\mathcal{X}_A \otimes \mathcal{Z}\right) \otimes \mathcal{X}_B, \mathcal{X}_A \otimes \left(\mathcal{Z} \otimes \mathcal{X}_B\right)\right)$$

defined by

$$\Phi((X_A \otimes Z) \otimes X_B) = X_A \otimes (\Delta(Z) \otimes X_B)$$

represents a classical communication channel from Alice to Bob, while the similarly defined channel

$$\Phi \in C\left(\mathcal{X}_A \otimes \left(\mathcal{Z} \otimes \mathcal{X}_B\right), \left(\mathcal{X}_A \otimes \mathcal{Z}\right) \otimes \mathcal{X}_B\right)$$

given by

$$\Phi(X_A \otimes (Z \otimes X_B)) = (X_A \otimes \Delta(Z)) \otimes X_B$$

represents a classical communication channel from Bob to Alice. In both of these cases, the spaces $\mathcal{X}_A$ and $\mathcal{X}_B$ represent quantum systems held by Alice and Bob, respectively, that are unaffected by the transmission. Of course the only difference between the two channels is the interpretation of who sends and who receives the register Z corresponding to the space $\mathcal{Z}$, which is represented by the parentheses in the above expressions.

When we speak of a *classical communication channel*, we mean either an Alice-to-Bob or Bob-to-Alice classical communication channel.

Finite compositions

Finally, for complex Euclidean spaces $\mathcal{X}_A$, $\mathcal{X}_B$, $\mathcal{Y}_A$ and $\mathcal{Y}_B$, an *LOCC channel* is any channel of the form

$$\Phi \in C\left(\mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{Y}_B\right)$$

that can be obtained from the composition of any finite number of product channels and classical communication channels. (The input and output spaces of each channel in the composition is arbitrary, so long as the first channel inputs $\mathcal{X}_A \otimes \mathcal{X}_B$ and the last channel outputs $\mathcal{Y}_A \otimes \mathcal{Y}_B$. The intermediate channels can act on arbitrary complex Euclidean spaces so long as they are product channels or classical communication channels and the composition makes sense.) We will write

$$\text{LOCC}\left(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B\right)$$

to denote the collection of all LOCC channels as just defined.

Note that by defining LOCC channels in terms of finite compositions, we are implicitly fixing the number of messages exchanged by Alice and Bob in the realization of any specific LOCC channel.

15.3.2 LOCC channels are separable

There are many simple questions concerning LOCC channels that are not yet answered. For instance, it is not known whether LOCC $(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$ is a closed set for any nontrivial choice of spaces $\mathcal{X}_A$, $\mathcal{X}_B$, $\mathcal{Y}_A$ and $\mathcal{Y}_B$. (For LOCC channels involving three or more parties—Alice, Bob, and Charlie, say—it was only proved this past year that the corresponding set of LOCC channels is not closed.) It is a related problem to better understand the number of message transmissions needed to implement LOCC channels.

In some situations, we may conclude interesting facts about LOCC channels by reasoning about separable channels. To this end, let us state a simple but very useful proposition.

Proposition 15.5. *Let* $\Phi \in \text{LOCC}\,(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$ *be an LOCC channel. It holds that*

$$\Phi \in \text{SepC}\,(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)\,.$$

Proof. The set of separable channels is closed under composition, and product channels are obviously separable, so it remains to observe that classical communication channels are separable.
Suppose

$$\Phi((X_A \otimes Z) \otimes X_B) = X_A \otimes (\Delta(Z) \otimes X_B)$$

is a classical communication channel from Alice to Bob. It holds that

$$\Phi(\rho) = \sum_{a \in \Sigma} \left[(\mathbb{1}_{\mathcal{X}_A} \otimes e_a^*) \otimes (e_a \otimes \mathbb{1}_{\mathcal{X}_B})\right] \rho \left[(\mathbb{1}_{\mathcal{X}_A} \otimes e_a^*) \otimes (e_a \otimes \mathbb{1}_{\mathcal{X}_B})\right]^*,$$

which demonstrates that

$$\Phi \in \text{SepC}\,(\mathcal{X}_A \otimes \mathcal{Z}, \mathcal{X}_A \otimes \mathbb{C} : \mathbb{C} \otimes \mathcal{X}_B, \mathcal{Z} \otimes \mathcal{X}_B) = \text{SepC}\,(\mathcal{X}_A \otimes \mathcal{Z}, \mathcal{X}_A : \mathcal{X}_B, \mathcal{Z} \otimes \mathcal{X}_B)$$

as required. A similar argument proves that every Bob-to-Alice classical communication channel is a separable channel. $\qquad\square$

In case the argument above about classical communication channels looks like abstract nonsense, it may be helpful to observe that the key feature of the channel Δ that allows the argument to work is that it can be expressed in Kraus form, where all of the Kraus operators have rank equal to one.

It must be noted that the separable channels do not give a perfect characterization of LOCC channels: there exist separable channels that are not LOCC channels. Nevertheless, we will still be able to use this proposition to prove various things about LOCC channels. One simple example follows.

Corollary 15.6. *Suppose* $\rho \in \text{D}\,(\mathcal{X}_A \otimes \mathcal{X}_B)$ *and* $\Phi \in \text{LOCC}\,(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$. *It holds that*

$$\text{min-rank}(\Phi(\rho)) \leq \text{min-rank}(\rho).$$

In particular, if $\rho \in \text{SepD}\,(\mathcal{X}_A : \mathcal{X}_B)$ *then* $\Phi(\rho) \in \text{SepD}\,(\mathcal{Y}_A : \mathcal{Y}_B)$.