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

John Watrous
Institute for Quantum Computing
University of Waterloo

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

Lecture 1: Mathematical preliminaries (part 1)

Welcome to CS 766/QIC 820 Theory of Quantum Information. The goal of this lecture, as well as the next, is to present a brief overview of some of the basic mathematical concepts and tools that will be important in subsequent lectures of the course. In this lecture we will discuss various facts about linear algebra and analysis in finite-dimensional vector spaces.

1.1 Complex Euclidean spaces

We begin with the simple notion of a *complex Euclidean space*. As will be discussed later (in Lecture 3), we associate a complex Euclidean space with every discrete and finite physical system; and fundamental notions such as states and measurements of systems are represented in linear-algebraic terms that refer to these spaces.

1.1.1 Definition of complex Euclidean spaces

For any finite, nonempty set Σ, we denote by $\mathbb{C}^\Sigma$ the set of all functions from Σ to the complex numbers $\mathbb{C}$. The collection $\mathbb{C}^\Sigma$ forms a vector space of dimension $|\Sigma|$ over the complex numbers when addition and scalar multiplication are defined in the following standard way:

1. Addition: given $u, v \in \mathbb{C}^\Sigma$, the vector $u + v \in \mathbb{C}^\Sigma$ is defined by the equation $(u + v)(a) = u(a) + v(a)$ for all $a \in \Sigma$.
2. Scalar multiplication: given $u \in \mathbb{C}^\Sigma$ and $\alpha \in \mathbb{C}$, the vector $\alpha u \in \mathbb{C}^\Sigma$ is defined by the equation $(\alpha u)(a) = \alpha u(a)$ for all $a \in \Sigma$.

Any vector space defined in this way for some choice of a finite, nonempty set Σ will be called a *complex Euclidean space*.

Complex Euclidean spaces will generally be denoted by scripted capital letters near the end of the alphabet, such as $\mathcal{W}$, $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, when it is necessary or helpful to assign specific names to them. Subsets of these spaces will also be denoted by scripted letters, and when possible our convention will be to use letters near the beginning of the alphabet, such as $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, when these subsets are not themselves necessarily vector spaces. Vectors will typically be denoted by lowercase Roman letters, again near the end of the alphabet, such as u, v, w, x, y, and z.

In the case where $\Sigma = \{1, \ldots, n\}$ for some positive integer n, one typically writes $\mathbb{C}^n$ rather than $\mathbb{C}^{\{1,\ldots,n\}}$. For a given positive integer n, it is typical to view a vector $u \in \mathbb{C}^n$ as an n-tuple $u = (u_1, \ldots, u_n)$, or as a column vector of the form

$$u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}.$$

The convention to write u_i rather than $u(i)$ in such expressions is simply a matter of typographic appeal, and is avoided when it is not helpful or would lead to confusion, such as when vectors are subscripted for another purpose.

It is, of course, the case that one could simply identify $\mathbb{C}^\Sigma$ with $\mathbb{C}^n$, for $n = |\Sigma|$, with respect to any fixed choice of a bijection between Σ and $\{1, \ldots, n\}$. If it is convenient to make this simplifying assumption when proving facts about complex Euclidean spaces, we will do that; but there is also a significant convenience to be found in allowing for arbitrary (finite and nonempty) index sets, which is why we define complex Euclidean spaces in the way that we have.

1.1.2 Inner product and norms of vectors

The *inner product* $\langle u, v \rangle$ of vectors $u, v \in \mathbb{C}^\Sigma$ is defined as

$$\langle u, v \rangle = \sum_{a \in \Sigma} \overline{u(a)}\, v(a).$$

It may be verified that the inner product satisfies the following properties:

1. Linearity in the second argument: $\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle$ for all $u, v, w \in \mathbb{C}^\Sigma$ and $\alpha, \beta \in \mathbb{C}$.
2. Conjugate symmetry: $\langle u, v \rangle = \overline{\langle v, u \rangle}$ for all $u, v \in \mathbb{C}^\Sigma$.
3. Positive definiteness: $\langle u, u \rangle \geq 0$ for all $u \in \mathbb{C}^\Sigma$, with $\langle u, u \rangle = 0$ if and only if $u = 0$.

One typically refers to any function satisfying these three properties as an inner product, but this is the only inner product for vectors in complex Euclidean spaces that is considered in this course.

The *Euclidean norm* of a vector $u \in \mathbb{C}^\Sigma$ is defined as

$$\|u\| = \sqrt{\langle u, u \rangle} = \sqrt{\sum_{a \in \Sigma} |u(a)|^2}.$$

The Euclidean norm satisfies the following properties, which are the defining properties of any function that is called a norm:

1. Positive definiteness: $\|u\| \geq 0$ for all $u \in \mathbb{C}^\Sigma$, with $\|u\| = 0$ if and only if $u = 0$.
2. Positive scalability: $\|\alpha u\| = |\alpha| \, \|u\|$ for all $u \in \mathbb{C}^\Sigma$ and $\alpha \in \mathbb{C}$.
3. The triangle inequality: $\|u + v\| \leq \|u\| + \|v\|$ for all $u, v \in \mathbb{C}^\Sigma$.

The Euclidean norm corresponds to the special case $p = 2$ of the class of *p-norms*, defined for each $u \in \mathbb{C}^\Sigma$ as

$$\|u\|_p = \left(\sum_{a \in \Sigma} |u(a)|^p \right)^{1/p}$$

for $1 \leq p < \infty$, and

$$\|u\|_\infty = \max\{|u(a)| \,:\, a \in \Sigma\}.$$

The above three norm properties (positive definiteness, positive scalability, and the triangle inequality) hold for $\|\cdot\|$ replaced by $\|\cdot\|_p$ for any choice of $p \in [1, \infty]$.

The *Cauchy-Schwarz inequality* states that

$$|\langle u, v \rangle| \leq \|u\| \, \|v\|$$

for all $u, v \in \mathbb{C}^{\Sigma}$, with equality if and only if u and v are linearly dependent. The Cauchy-Schwarz inequality is generalized by *Hölder's inequality*, which states that

$$|\langle u, v \rangle| \leq \|u\|_p \, \|v\|_q$$

for all $u, v \in \mathbb{C}^{\Sigma}$, provided $p, q \in [1, \infty]$ satisfy $\frac{1}{p} + \frac{1}{q} = 1$ (with the interpretation $\frac{1}{\infty} = 0$).

1.1.3 Orthogonal and orthonormal sets

A collection of vectors

$$\{u_a : a \in \Gamma\} \subset \mathbb{C}^{\Sigma},$$

indexed by a given finite, nonempty set Γ, is said to be an *orthogonal set* if it holds that $\langle u_a, u_b \rangle = 0$ for all choices of $a, b \in \Gamma$ with $a \neq b$. Such a set is necessarily linearly independent, provided it does not include the zero vector.

An orthogonal set of *unit* vectors is called an *orthonormal set*, and when such a set forms a basis it is called an orthonormal basis. It holds that an orthonormal set $\{u_a : a \in \Gamma\} \subseteq \mathbb{C}^{\Sigma}$ is an orthonormal basis of $\mathbb{C}^{\Sigma}$ if and only if $|\Gamma| = |\Sigma|$.

The *standard basis* of $\mathbb{C}^{\Sigma}$ is the orthonormal basis given by $\{e_a : a \in \Sigma\}$, where

$$e_a(b) = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}$$

for all $a, b \in \Sigma$.

Remark 1.1. When using the *Dirac notation*, one writes $|a\rangle$ rather than e_a when referring to standard basis elements; and for arbitrary vectors one writes $|u\rangle$ rather than u (although ϕ, ψ, and other Greek letters are much more commonly used to name vectors). We will generally not use Dirac notation in this course, because it tends to complicate the sorts of expressions we will encounter. One exception is the use of Dirac notation for the presentation of simple examples, where it seems to increase clarity.

1.1.4 Real Euclidean spaces

Real Euclidean spaces are defined in a similar way to complex Euclidean spaces, except that the field of complex numbers $\mathbb{C}$ is replaced by the field of real numbers $\mathbb{R}$ in each of the definitions and concepts in which it arises. Naturally, complex conjugation acts trivially in the real case, and may therefore be omitted.

Although complex Euclidean spaces will play a much more prominent role than real Euclidean spaces in this course, we will restrict our attention to real Euclidean spaces in the context of convexity theory. This will not limit the applicability of these concepts: they will generally be applied to the real Euclidean space consisting of all Hermitian operators acting on a given complex Euclidean space. Such spaces will be discussed later in this lecture.

1.2 Linear operators

Given complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, one writes $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ to refer to the collection of all linear mappings of the form

$$A : \mathcal{X} \to \mathcal{Y}. \tag{1.1}$$

Such mappings will be referred to as *linear operators*, or simply *operators*, from $\mathcal{X}$ to $\mathcal{Y}$ in this course. Parentheses are typically omitted when expressing the action of linear operators on vectors when there is little chance of confusion in doing so. For instance, one typically writes Au rather than $A(u)$ to denote the vector resulting from the application of an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ to a vector $u \in \mathcal{X}$.

The set $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ forms a vector space, where addition and scalar multiplication are defined as follows:

1. Addition: given $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$, the operator $A + B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is defined by the equation

   $$(A + B)u = Au + Bu$$

   for all $u \in \mathcal{X}$.
2. Scalar multiplication: given $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ and $\alpha \in \mathbb{C}$, the operator $\alpha A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is defined by the equation

   $$(\alpha A)u = \alpha\, Au$$

   for all $u \in \mathcal{X}$.

The dimension of this vector space is given by $\dim(\mathrm{L}(\mathcal{X}, \mathcal{Y})) = \dim(\mathcal{X}) \dim(\mathcal{Y})$.

The *kernel* of an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is the subspace of $\mathcal{X}$ defined as

$$\ker(A) = \{u \in \mathcal{X} \,:\, Au = 0\},$$

while the *image* of A is the subspace of $\mathcal{Y}$ defined as

$$\mathrm{im}(A) = \{Au \,:\, u \in \mathcal{X}\}.$$

The *rank* of A, denoted $\mathrm{rank}(A)$, is the dimension of the subspace $\mathrm{im}(A)$. For every operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ it holds that

$$\dim(\ker(A)) + \mathrm{rank}(A) = \dim(\mathcal{X}).$$

1.2.1 Matrices and their association with operators

A *matrix* over the complex numbers is a mapping of the form

$$M : \Gamma \times \Sigma \to \mathbb{C}$$

for finite, nonempty sets Σ and Γ. The collection of all matrices of this form is denoted $\mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$. For $a \in \Gamma$ and $b \in \Sigma$ the value $M(a, b)$ is called the (a, b) *entry* of M, and the elements a and b are referred to as *indices* in this context: a is the *row index* and b is the *column index* of the entry $M(a, b)$.

The set $\mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ is a vector space with respect to vector addition and scalar multiplication defined in the following way:

1. Addition: given $M, K \in \mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$, the matrix $M + K \in \mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ is defined by the equation

   $$(M + K)(a, b) = M(a, b) + K(a, b)$$

   for all $a \in \Gamma$ and $b \in \Sigma$.

2. Scalar multiplication: given $M \in \mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ and $\alpha \in \mathbb{C}$, the matrix $\alpha M \in \mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ is defined by the equation
$$(\alpha M)(a,b) = \alpha M(a,b)$$
for all $a \in \Gamma$ and $b \in \Sigma$.

As a vector space, $\mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ is therefore equivalent to the complex Euclidean space $\mathbb{C}^{\Gamma\times\Sigma}$.

Multiplication of matrices is defined in the following standard way. Given matrices $M \in \mathcal{M}_{\Gamma,\Delta}(\mathbb{C})$ and $K \in \mathcal{M}_{\Delta,\Sigma}(\mathbb{C})$, for finite nonempty sets Γ, Δ, and Σ, the matrix $MK \in \mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ is defined as
$$(MK)(a,b) = \sum_{c\in\Delta} M(a,c)K(c,b)$$
for all $a \in \Gamma$ and $b \in \Sigma$.

Linear operators from one complex Euclidean space to another are naturally represented by matrices. For $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} = \mathbb{C}^{\Gamma}$, one associates with each operator $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ a matrix $M_A \in \mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ defined as
$$M_A(a,b) = \langle e_a, Ae_b\rangle$$
for each $a \in \Gamma$ and $b \in \Sigma$. Conversely, to each matrix $M \in \mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ one associates a linear operator $A_M \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ defined by
$$(A_M u)(a) = \sum_{b\in\Sigma} M(a,b)u(b) \tag{1.2}$$
for each $a \in \Gamma$. The mappings $A \mapsto M_A$ and $M \mapsto A_M$ are linear and inverse to one other, and compositions of linear operators are represented by matrix multiplications: $M_{AB} = M_A M_B$ whenever $A \in \mathrm{L}(\mathcal{Y},\mathcal{Z})$, $B \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ and $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are complex Euclidean spaces. Equivalently, $A_{MK} = A_M A_K$ for any choice of matrices $M \in \mathcal{M}_{\Gamma,\Delta}(\mathbb{C})$ and $K \in \mathcal{M}_{\Delta,\Sigma}(\mathbb{C})$ for finite nonempty sets Σ, Δ, and Γ.

This correspondence between linear operators and matrices will hereafter not be mentioned explicitly in these notes: we will freely switch between speaking of operators and speaking of matrices, depending on which is more suitable within the context at hand. A preference will generally be given to speak of operators, and to implicitly associate a given operator's matrix representation with it as necessary. More specifically, for a given choice of complex Euclidean spaces $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} \in \mathbb{C}^{\Gamma}$, and for a given operator $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$, the matrix $M_A \in \mathcal{M}_{\Gamma,\Sigma}(\mathbb{C})$ will simply be denoted A and its (a,b)-entry as $A(a,b)$.

1.2.2 The entry-wise conjugate, transpose, and adjoint

For every operator $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$, for complex Euclidean spaces $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} = \mathbb{C}^{\Gamma}$, one defines three additional operators,
$$\overline{A} \in \mathrm{L}(\mathcal{X},\mathcal{Y}) \quad \text{and} \quad A^{\mathsf{T}}, A^{*} \in \mathrm{L}(\mathcal{Y},\mathcal{X}),$$
as follows:

1. The operator $\overline{A} \in \mathrm{L}(\mathcal{X},\mathcal{Y})$ is the operator whose matrix representation has entries that are complex conjugates to the matrix representation of A:
$$\overline{A}(a,b) = \overline{A(a,b)}$$
for all $a \in \Gamma$ and $b \in \Sigma$.

2. The operator $A^{\mathsf{T}} \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ is the operator whose matrix representation is obtained by *transposing* the matrix representation of A:

$$A^{\mathsf{T}}(b, a) = A(a, b)$$

for all $a \in \Gamma$ and $b \in \Sigma$.

3. The operator $A^* \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is the unique operator that satisfies the equation

$$\langle v, Au \rangle = \langle A^* v, u \rangle$$

for all $u \in \mathcal{X}$ and $v \in \mathcal{Y}$. It may be obtained by performing both of the operations described in items 1 and 2:

$$A^* = \overline{A^{\mathsf{T}}}.$$

The operators $\overline{A}$, A^{T}, and A^* will be called the *entry-wise conjugate*, *transpose*, and *adjoint* operators to A, respectively.

The mappings $A \mapsto \overline{A}$ and $A \mapsto A^*$ are conjugate linear and the mapping $A \mapsto A^{\mathsf{T}}$ is linear:

$$\begin{aligned}
\overline{\alpha A + \beta B} &= \overline{\alpha}\,\overline{A} + \overline{\beta}\,\overline{B}, \\
(\alpha A + \beta B)^* &= \overline{\alpha} A^* + \overline{\beta} B^*, \\
(\alpha A + \beta B)^{\mathsf{T}} &= \alpha A^{\mathsf{T}} + \beta B^{\mathsf{T}},
\end{aligned}$$

for all $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ and $\alpha, \beta \in \mathbb{C}$. These mappings are bijections, each being its own inverse.

Every vector $u \in \mathcal{X}$ in a complex Euclidean space $\mathcal{X}$ may be identified with the linear operator in $\mathrm{L}(\mathbb{C}, \mathcal{X})$ that maps $\alpha \mapsto \alpha u$. Through this identification the linear mappings $\overline{u} \in \mathrm{L}(\mathbb{C}, \mathcal{X})$ and $u^{\mathsf{T}}, u^* \in \mathrm{L}(\mathcal{X}, \mathbb{C})$ are defined as above. As an element of $\mathcal{X}$, the vector $\overline{u}$ is of course simply the entry-wise complex conjugate of u, i.e., if $\mathcal{X} = \mathbb{C}^{\Sigma}$ then

$$\overline{u}(a) = \overline{u(a)}$$

for every $a \in \Sigma$. For each vector $u \in \mathcal{X}$ the mapping $u^* \in \mathrm{L}(\mathcal{X}, \mathbb{C})$ satisfies $u^* v = \langle u, v \rangle$ for all $v \in \mathcal{X}$. The space of linear operators $\mathrm{L}(\mathcal{X}, \mathbb{C})$ is called the *dual space* of $\mathcal{X}$, and is often denoted by $\mathcal{X}^*$ rather than $\mathrm{L}(\mathcal{X}, \mathbb{C})$.

Assume that $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} = \mathbb{C}^{\Gamma}$. For each choice of $a \in \Gamma$ and $b \in \Sigma$, the operator $E_{a,b} \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is defined as $E_{a,b} = e_a e_b^*$, or equivalently

$$E_{a,b}(c, d) = \begin{cases} 1 & \text{if } (a = c) \text{ and } (b = d) \\ 0 & \text{if } (a \neq c) \text{ or } (b \neq d). \end{cases}$$

The set $\{E_{a,b} : a \in \Gamma,\ b \in \Sigma\}$ is a basis of $\mathrm{L}(\mathcal{X}, \mathcal{Y})$, and will be called the *standard basis* of this space.

1.2.3 Direct sums

The *direct sum* of n complex Euclidean spaces $\mathcal{X}_1 = \mathbb{C}^{\Sigma_1}, \ldots, \mathcal{X}_n = \mathbb{C}^{\Sigma_n}$ is the complex Euclidean space

$$\mathcal{X}_1 \oplus \cdots \oplus \mathcal{X}_n = \mathbb{C}^{\Delta},$$

where

$$\Delta = \{(1, a_1) : a_1 \in \Sigma_1\} \cup \cdots \cup \{(n, a_n) : a_n \in \Sigma_n\}.$$

One may view Δ as the *disjoint union* of $\Sigma_1, \ldots, \Sigma_n$.

For vectors $u_1 \in \mathcal{X}_1, \ldots, u_n \in \mathcal{X}_n$, the notation $u_1 \oplus \cdots \oplus u_n \in \mathcal{X}_1 \oplus \cdots \oplus \mathcal{X}_n$ refers to the vector for which

$$(u_1 \oplus \cdots \oplus u_n)(j, a_j) = u_j(a_j),$$

for each $j \in \{1, \ldots, n\}$ and $a_j \in \Sigma_j$. If each vector u_j is viewed as a column vector of dimension $\left|\Sigma_j\right|$, the vector $u_1 \oplus \cdots \oplus u_n$ may be viewed as a (block) column vector

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

having dimension $|\Sigma_1| + \cdots + |\Sigma_n|$. Every element of the space $\mathcal{X}_1 \oplus \cdots \oplus \mathcal{X}_n$ can be written as $u_1 \oplus \cdots \oplus u_n$ for a unique choice of vectors $u_1, \ldots, u_n$. The following identities hold for every choice of $u_1, v_1 \in \mathcal{X}_1, \ldots, u_n, v_n \in \mathcal{X}_n$, and $\alpha \in \mathbb{C}$:

$$u_1 \oplus \cdots \oplus u_n + v_1 \oplus \cdots \oplus v_n = (u_1 + v_1) \oplus \cdots \oplus (u_n + v_n)$$

$$\alpha(u_1 \oplus \cdots \oplus u_n) = (\alpha u_1) \oplus \cdots \oplus (\alpha u_n)$$

$$\langle u_1 \oplus \cdots \oplus u_n, v_1 \oplus \cdots \oplus v_n \rangle = \langle u_1, v_1 \rangle + \cdots + \langle u_n, v_n \rangle .$$

Now suppose that $\mathcal{X}_1 = \mathbb{C}^{\Sigma_1}, \ldots, \mathcal{X}_n = \mathbb{C}^{\Sigma_n}$ and $\mathcal{Y}_1 = \mathbb{C}^{\Gamma_1}, \ldots, \mathcal{Y}_m = \mathbb{C}^{\Gamma_m}$ for positive integers n and m, and finite, nonempty sets $\Sigma_1, \ldots, \Sigma_n$ and $\Gamma_1, \ldots, \Gamma_m$. The matrix associated with a given operators of the form $A \in \mathrm{L}\left(\mathcal{X}_1 \oplus \cdots \oplus \mathcal{X}_n, \mathcal{Y}_1 \oplus \cdots \oplus \mathcal{Y}_m\right)$ may be identified with a block matrix

$$A = \begin{pmatrix} A_{1,1} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \cdots & A_{m,n} \end{pmatrix},$$

where $A_{j,k} \in \mathrm{L}\left(\mathcal{X}_k, \mathcal{Y}_j\right)$ for each $j \in \{1, \ldots, m\}$ and $k \in \{1, \ldots, n\}$. These are the uniquely determined operators for which it holds that

$$A(u_1 \oplus \cdots \oplus u_n) = v_1 \oplus \cdots \oplus v_m,$$

for $v_1 \in \mathcal{Y}_1, \ldots, v_m \in \mathcal{Y}_m$ defined as

$$v_j = (A_{j,1} u_1) + \cdots + (A_{j,n} u_n)$$

for each $j \in \{1, \ldots, m\}$.

1.2.4 Tensor products

The *tensor product* of $\mathcal{X}_1 = \mathbb{C}^{\Sigma_1}, \ldots, \mathcal{X}_n = \mathbb{C}^{\Sigma_n}$ is the complex Euclidean space

$$\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n = \mathbb{C}^{\Sigma_1 \times \cdots \times \Sigma_n}.$$

For vectors $u_1 \in \mathcal{X}_1, \ldots, u_n \in \mathcal{X}_n$, the vector $u_1 \otimes \cdots \otimes u_n \in \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$ is defined as

$$(u_1 \otimes \cdots \otimes u_n)(a_1, \ldots, a_n) = u_1(a_1) \cdots u_n(a_n).$$

Vectors of the form $u_1 \otimes \cdots \otimes u_n$ are called *elementary tensors*. They span the space $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$, but not every element of $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$ is an elementary tensor.

The following identities hold for every choice of $u_1, v_1 \in \mathcal{X}_1, \ldots, u_n, v_n \in \mathcal{X}_n$, $\alpha \in \mathbb{C}$, and $k \in \{1, \ldots, n\}$:

$$\begin{aligned} u_1 \otimes \cdots \otimes u_{k-1} \otimes (u_k + v_k) \otimes u_{k+1} \otimes \cdots \otimes u_n & \\ = u_1 \otimes \cdots \otimes u_{k-1} \otimes u_k \otimes u_{k+1} \otimes \cdots \otimes u_n & \\ + u_1 \otimes \cdots \otimes u_{k-1} \otimes v_k \otimes u_{k+1} \otimes \cdots \otimes u_n & \end{aligned}$$

$$\alpha(u_1 \otimes \cdots \otimes u_n) = (\alpha u_1) \otimes u_2 \otimes \cdots \otimes u_n = \cdots = u_1 \otimes u_2 \otimes \cdots \otimes u_{n-1} \otimes (\alpha u_n)$$

$$\langle u_1 \otimes \cdots \otimes u_n, v_1 \otimes \cdots \otimes v_n \rangle = \langle u_1, v_1 \rangle \cdots \langle u_n, v_n \rangle .$$

It is worthwhile to note that the definition of tensor products just presented is a concrete definition that is sometimes known as the *Kronecker product*. In contrast, tensor products are often defined in a more abstract way that stresses their close connection to *multilinear functions*. There is valuable intuition to be drawn from this connection, but for our purposes it will suffice that we take note of the following fact.

Proposition 1.2. *Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}$ be complex Euclidean spaces, and let $\phi : \mathcal{X}_1 \times \cdots \times \mathcal{X}_n \to \mathcal{Y}$ be a multilinear function (i.e., a function for which the mapping $u_j \mapsto \phi(u_1, \ldots, u_n)$ is linear for all $j \in \{1, \ldots, n\}$ and all choices of $u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n$. It holds that there exists an operator $A \in \mathrm{L}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y})$ for which*

$$\phi(u_1, \ldots, u_n) = A(u_1 \otimes \cdots \otimes u_n).$$

1.3 Algebras of operators

For every complex Euclidean space $\mathcal{X}$, the notation $\mathrm{L}(\mathcal{X})$ is understood to be a shorthand for $\mathrm{L}(\mathcal{X}, \mathcal{X})$. The space $\mathrm{L}(\mathcal{X})$ has special algebraic properties that are worthy of note. In particular, $\mathrm{L}(\mathcal{X})$ is an *associative algebra*; it is a vector space, and the composition of operators is associative and bilinear:

$$\begin{aligned} (AB)C &= A(BC), \\ C(\alpha A + \beta B) &= \alpha CA + \beta CB, \\ (\alpha A + \beta B)C &= \alpha AC + \beta BC, \end{aligned}$$

for every choice of $A, B, C \in \mathrm{L}(\mathcal{X})$ and $\alpha, \beta \in \mathbb{C}$.

The identity operator $\mathbb{1} \in \mathrm{L}(\mathcal{X})$ is the operator defined as $\mathbb{1}u = u$ for all $u \in \mathcal{X}$, and is denoted $\mathbb{1}_{\mathcal{X}}$ when it is helpful to indicate explicitly that it acts on $\mathcal{X}$. An operator $A \in \mathrm{L}(\mathcal{X})$ is *invertible* if there exists an operator $B \in \mathrm{L}(\mathcal{X})$ such that $BA = \mathbb{1}$. When such an operator B exists it is necessarily unique, also satisfies $AB = \mathbb{1}$, and is denoted A^{-1}. The collection of all invertible operators in $\mathrm{L}(\mathcal{X})$ is denoted $\mathrm{GL}(\mathcal{X})$, and is called the *general linear group* of $\mathcal{X}$.

For every pair of operators $A, B \in \mathrm{L}(\mathcal{X})$, the *Lie bracket* $[A, B] \in \mathrm{L}(\mathcal{X})$ is defined as $[A, B] = AB - BA$.

1.3.1 Trace and determinant

Operators in the algebra $\mathrm{L}(\mathcal{X})$ are represented by *square* matrices, which means that their rows and columns are indexed by the same set. We define two important functions from $\mathrm{L}(\mathcal{X})$ to $\mathbb{C}$, the *trace* and the *determinant*, based on matrix representations of operators as follows:

1. The *trace* of an operator $A \in \mathrm{L}(\mathcal{X})$, for $\mathcal{X} = \mathbb{C}^{\Sigma}$, is defined as
$$\mathrm{Tr}(A) = \sum_{a \in \Sigma} A(a, a).$$
2. The *determinant* of an operator $A \in \mathrm{L}(\mathcal{X})$, for $\mathcal{X} = \mathbb{C}^{\Sigma}$, is defined by the equation
$$\mathrm{Det}(A) = \sum_{\pi \in Sym(\Sigma)} \mathrm{sign}(\pi) \prod_{a \in \Sigma} A(a, \pi(a)),$$
where $Sym(\Sigma)$ is the group of permutations on the set Σ and $\mathrm{sign}(\pi)$ is the *sign* of the permutation π (which is $+1$ if π is expressible as a product of an even number of transpositions of elements of the set Σ, and -1 if π is expressible as a product of an odd number of transpositions).

The trace is a linear function, and possesses the property that
$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$
for any choice of operators $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ and $B \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$, for arbitrary complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$.

By means of the trace, one defines an inner product on the space $\mathrm{L}(\mathcal{X}, \mathcal{Y})$, for any choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, as
$$\langle A, B \rangle = \mathrm{Tr}\left(A^* B\right)$$
for all $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$. It may be verified that this inner product satisfies the requisite properties of being an inner product:

1. Linearity in the second argument:
$$\langle A, \alpha B + \beta C \rangle = \alpha \langle A, B \rangle + \beta \langle A, C \rangle$$
for all $A, B, C \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ and $\alpha, \beta \in \mathbb{C}$.
2. Conjugate symmetry: $\langle A, B \rangle = \overline{\langle B, A \rangle}$ for all $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$.
3. Positive definiteness: $\langle A, A \rangle \geq 0$ for all $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$, with $\langle A, A \rangle = 0$ if and only if $A = 0$.

This inner product is sometimes called the *Hilbert–Schmidt inner product*.

The determinant is multiplicative,
$$\mathrm{Det}(AB) = \mathrm{Det}(A)\,\mathrm{Det}(B)$$
for all $A, B \in \mathrm{L}(\mathcal{X})$, and its value is nonzero if and only if its argument is invertible.

1.3.2 Eigenvectors and eigenvalues

If $A \in \mathrm{L}(\mathcal{X})$ and $u \in \mathcal{X}$ is a nonzero vector such that $Au = \lambda u$ for some choice of $\lambda \in \mathbb{C}$, then u is said to be an *eigenvector* of A and λ is its corresponding *eigenvalue*.

For every operator $A \in \mathrm{L}(\mathcal{X})$, one has that

$$p_A(z) = \mathrm{Det}(z\mathbb{1}_{\mathcal{X}} - A)$$

is a monic polynomial in z having degree $\dim(\mathcal{X})$. This polynomial is the *characteristic polynomial* of A. The *spectrum* of A, denoted $\mathrm{spec}(A)$, is the multiset containing the roots of the polynomial $p_A(z)$, with each root appearing a number of times equal to its multiplicity. As p_A is monic, it holds that

$$p_A(z) = \prod_{\lambda \in \mathrm{spec}(A)} (z - \lambda)$$

Each element $\lambda \in \mathrm{spec}(A)$ is an eigenvalue of A.

The trace and determinant may be expressed in terms of the spectrum as follows:

$$\mathrm{Tr}(A) = \sum_{\lambda \in \mathrm{spec}(A)} \lambda$$

and

$$\mathrm{Det}(A) = \prod_{\lambda \in \mathrm{spec}(A)} \lambda$$

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

1.4 Important classes of operators

A collection of classes of operators that have importance in quantum information are discussed in this section.

1.4.1 Normal operators

An operator $A \in \mathrm{L}(\mathcal{X})$ is *normal* if and only if it commutes with its adjoint: $[A, A^*] = 0$, or equivalently $AA^* = A^*A$. The importance of this collection of operators, for the purposes of this course, is mainly derived from two facts: (1) the normal operators are those for which the spectral theorem (discussed later in Section 1.5) holds, and (2) most of the special classes of operators that are discussed below are subsets of the normal operators.

1.4.2 Hermitian operators

An operator $A \in \mathrm{L}(\mathcal{X})$ is *Hermitian* if $A = A^*$. The set of Hermitian operators acting on a given complex Euclidean space $\mathcal{X}$ will hereafter be denoted $\mathrm{Herm}(\mathcal{X})$ in this course:

$$\mathrm{Herm}(\mathcal{X}) = \{A \in \mathrm{L}(\mathcal{X}) \,:\, A = A^*\}.$$

Every Hermitian operator is obviously a normal operator.

The eigenvalues of every Hermitian operator are necessarily real numbers, and can therefore be ordered from largest to smallest. Under the assumption that $A \in \mathrm{Herm}(\mathcal{X})$ for $\mathcal{X}$ an n-dimensional complex Euclidean space, one denotes the k-th largest eigenvalue of A by $\lambda_k(A)$. Equivalently, the vector

$$\lambda(A) = (\lambda_1(A), \lambda_2(A), \ldots, \lambda_n(A)) \in \mathbb{R}^n$$

is defined so that

$$\mathrm{spec}(A) = \{\lambda_1(A), \lambda_2(A), \ldots, \lambda_n(A)\}$$

and

$$\lambda_1(A) \geq \lambda_2(A) \geq \cdots \geq \lambda_n(A).$$

The sum of two Hermitian operators is obviously Hermitian, as is any real scalar multiple of a Hermitian operator. This means that the set $\mathrm{Herm}(\mathcal{X})$ forms a vector space over the real numbers. The inner product of two Hermitian operators is real as well, $\langle A, B\rangle \in \mathbb{R}$ for all $A, B \in \mathrm{Herm}(\mathcal{X})$, so this space is in fact a real inner product space.

We can, in fact, go a little bit further along these lines. Assuming that $\mathcal{X} = \mathbb{C}^\Sigma$, and that the elements of Σ are ordered in some fixed way, let us define a Hermitian operator $H_{a,b} \in \mathrm{Herm}(\mathcal{X})$, for each choice of $a, b \in \Sigma$, as follows:

$$H_{a,b} = \begin{cases} E_{a,a} & \text{if } a = b \\ \frac{1}{\sqrt{2}}(E_{a,b} + E_{b,a}) & \text{if } a < b \\ \frac{1}{\sqrt{2}}(iE_{a,b} - iE_{b,a}) & \text{if } a > b. \end{cases}$$

The collection $\{H_{a,b} : a, b \in \Sigma\}$ is orthonormal (with respect to the inner product defined on $\mathrm{L}(\mathcal{X})$), and every Hermitian operator $A \in \mathrm{Herm}(\mathcal{X})$ can be expressed as a real linear combination of matrices in this collection. It follows that $\mathrm{Herm}(\mathcal{X})$ is a vector space of dimension $|\Sigma|^2$ over the real numbers, and that there exists an isometric isomorphism between $\mathrm{Herm}(\mathcal{X})$ and $\mathbb{R}^{\Sigma\times\Sigma}$. This fact will allow us to apply facts about convex analysis, which typically hold for real Euclidean spaces, to $\mathrm{Herm}(\mathcal{X})$ (as will be discussed in the next lecture).

1.4.3 Positive semidefinite operators

An operator $A \in \mathrm{L}(\mathcal{X})$ is *positive semidefinite* if and only if it holds that $A = B^*B$ for some operator $B \in \mathrm{L}(\mathcal{X})$. Hereafter, when it is reasonable to do so, a convention to use the symbols P, Q and R to denote general positive semidefinite matrices will be followed. The collection of positive semidefinite operators acting on $\mathcal{X}$ is denoted $\mathrm{Pos}(\mathcal{X})$, so that

$$\mathrm{Pos}(\mathcal{X}) = \{B^*B : B \in \mathrm{L}(\mathcal{X})\}.$$

There are alternate ways to describe positive semidefinite operators that are useful in different situations. In particular, the following items are equivalent for a given operator $P \in \mathrm{L}(\mathcal{X})$:

1. P is positive semidefinite.
2. $P = B^*B$ for some choice of a complex Euclidean space $\mathcal{Y}$ and an operator $B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$.
3. u^*Pu is a nonnegative real number for every choice of $u \in \mathcal{X}$.
4. $\langle Q, P\rangle$ is a nonnegative real number for every $Q \in \mathrm{Pos}(\mathcal{X})$.

5. P is Hermitian and every eigenvalue of P is nonnegative.
6. There exists a complex Euclidean space $\mathcal{Y}$ and a collection of vectors $\{u_a : a \in \Sigma\} \subset \mathcal{Y}$, such that $P(a,b) = \langle u_a, u_b \rangle$.

Item 6 remains valid if the additional constraint $\dim(\mathcal{Y}) = \dim(\mathcal{X})$ is imposed.

The notation $P \geq 0$ is also used to mean that P is positive semidefinite, while $A \geq B$ means that $A - B$ is positive semidefinite. (This notation is only used when A and B are both Hermitian.)

1.4.4 Positive definite operators

A positive semidefinite operator $P \in \mathrm{Pos}(\mathcal{X})$ is said to be *positive definite* if, in addition to being positive semidefinite, it is invertible. The notation

$$\mathrm{Pd}(\mathcal{X}) = \{P \in \mathrm{Pos}(\mathcal{X}) : \mathrm{Det}(P) \neq 0\}$$

will be used to denote the set of such operators for a given complex Euclidean space $\mathcal{X}$. The following items are equivalent for a given operator $P \in \mathrm{L}(\mathcal{X})$:

1. P is positive definite.
2. $\langle u, Pu \rangle$ is a positive real number for every choice of a nonzero vector $u \in \mathcal{X}$.
3. P is Hermitian, and every eigenvalue of P is positive.
4. P is Hermitian, and there exists a positive real number $\varepsilon > 0$ such that $P \geq \varepsilon \mathbb{1}$.

1.4.5 Density operators

Positive semidefinite operators having trace equal to 1 are called *density operators*, and it is conventional to use lowercase Greek letters such as ρ, ξ, and σ to denote such operators. The notation

$$\mathrm{D}(\mathcal{X}) = \{\rho \in \mathrm{Pos}(\mathcal{X}) : \mathrm{Tr}(\rho) = 1\}$$

is used to denote the collection of density operators acting on a given complex Euclidean space.

1.4.6 Orthogonal projections

A positive semidefinite operator $P \in \mathrm{Pos}(\mathcal{X})$ is an *orthogonal projection* if, in addition to being positive semidefinite, it satisfies $P^2 = P$. Equivalently, an orthogonal projection is any Hermitian operator whose only eigenvalues are 0 and 1. For each subspace $\mathcal{V} \subseteq \mathcal{X}$, we write $\Pi_{\mathcal{V}}$ to denote the unique orthogonal projection whose image is equal to the subspace $\mathcal{V}$.

It is typically that the term *projection* refers to an operator $A \in \mathrm{L}(\mathcal{X})$ that satisfies $A^2 = A$, but which might not be Hermitian. Given that there is no discussion of such operators in this course, we will use the term *projection* to mean *orthogonal projection*.

1.4.7 Linear isometries and unitary operators

An operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is a *linear isometry* if it preserves the Euclidean norm—meaning that $\|Au\| = \|u\|$ for all $u \in \mathcal{X}$. The condition that $\|Au\| = \|u\|$ for all $u \in \mathcal{X}$ is equivalent to $A^*A = \mathbb{1}_{\mathcal{X}}$. The notation

$$\mathrm{U}(\mathcal{X}, \mathcal{Y}) = \{A \in \mathrm{L}(\mathcal{X}, \mathcal{Y}) : A^*A = \mathbb{1}_{\mathcal{X}}\}$$

is used throughout this course. Every linear isometry preserves not only the Euclidean norm, but inner products as well: $\langle Au, Av \rangle = \langle u, v \rangle$ for all $u, v \in \mathcal{X}$.

The set of linear isometries mapping $\mathcal{X}$ to itself is denoted $\mathrm{U}(\mathcal{X})$, and operators in this set are called *unitary operators*. The letters U, V, and W are conventionally used to refer to unitary operators. Every unitary operator $U \in \mathrm{U}(\mathcal{X})$ is invertible and satisfies $UU^* = U^*U = \mathbb{1}_{\mathcal{X}}$, which implies that every unitary operator is normal.

1.5 The spectral theorem

The *spectral theorem* establishes that every *normal* operator can be expressed as a linear combination of projections onto pairwise orthogonal subspaces. The spectral theorem is so-named, and the resulting expressions are called spectral decompositions, because the coefficients of the projections are determined by the spectrum of the operator being considered.

1.5.1 Statement of the spectral theorem and related facts

A formal statement of the spectral theorem follows.

Theorem 1.3 (Spectral theorem)**.** *Let $\mathcal{X}$ be a complex Euclidean space, let $A \in \mathrm{L}(\mathcal{X})$ be a normal operator, and assume that the distinct eigenvalues of A are $\lambda_1, \ldots, \lambda_k$. There exists a unique choice of orthogonal projection operators $P_1, \ldots, P_k \in \mathrm{Pos}(\mathcal{X})$, with $P_1 + \cdots + P_k = \mathbb{1}_{\mathcal{X}}$ and $P_i P_j = 0$ for $i \neq j$, such that*

$$A = \sum_{i=1}^{k} \lambda_i P_i. \tag{1.3}$$

For each $i \in \{1, \ldots, k\}$, it holds that the rank of P_i is equal to the multiplicity of λ_i as an eigenvalue of A.

As suggested above, the expression of a normal operator A in the form of the above equation (1.3) is called a *spectral decomposition* of A.

A simple corollary of the spectral theorem follows. It expresses essentially the same fact as the spectral theorem, but in a slightly different form that will be useful to refer to later in the course.

Corollary 1.4. *Let $\mathcal{X}$ be a complex Euclidean space, let $A \in \mathrm{L}(\mathcal{X})$ be a normal operator, and assume that* $\mathrm{spec}(A) = \{\lambda_1, \ldots, \lambda_n\}$*. There exists an orthonormal basis $\{x_1, \ldots, x_n\}$ of $\mathcal{X}$ such that*

$$A = \sum_{i=1}^{n} \lambda_i x_i x_i^*. \tag{1.4}$$

It is clear from the expression (1.4), along with the requirement that the set $\{x_1, \ldots, x_n\}$ is an orthonormal basis, that each x_i is an eigenvector of A whose corresponding eigenvalue is λ_i. It is also clear that any operator A that is expressible in such a form as (1.4) is normal—implying that the condition of normality is equivalent to the existence of an orthonormal basis of eigenvectors.

We will often refer to expressions of operators in the form (1.4) as *spectral decompositions*, despite the fact that it differs slightly from the form (1.3). It must be noted that unlike the form (1.3), the form (1.4) is generally not unique (unless each eigenvalue of A has multiplicity one, in which case the expression is unique up to scalar multiples of the vectors $\{x_1, \ldots, x_n\}$).

Finally, let us mention one more important theorem regarding spectral decompositions of normal operators, which states that the same orthonormal basis of eigenvectors $\{x_1, \ldots, x_n\}$ may be chosen for any two normal operators, provided that they commute.

Theorem 1.5. *Let $\mathcal{X}$ be a complex Euclidean space and let $A, B \in \mathrm{L}(\mathcal{X})$ be normal operators for which $[A, B] = 0$. There exists an orthonormal basis $\{x_1, \ldots, x_n\}$ of $\mathcal{X}$ such that*

$$A = \sum_{i=1}^{n} \lambda_i x_i x_i^* \qquad \text{and} \qquad B = \sum_{i=1}^{n} \mu_i x_i x_i^*$$

are spectral decompositions of A and B, respectively.

1.5.2 Functions of normal operators

Every function of the form $f : \mathbb{C} \to \mathbb{C}$ may be extended to the set of normal operators in $\mathrm{L}(\mathcal{X})$, for a given complex Euclidean space $\mathcal{X}$, by means of the spectral theorem. In particular, if $A \in \mathrm{L}(\mathcal{X})$ is normal and has the spectral decomposition (1.3), then one defines

$$f(A) = \sum_{i=1}^{k} f(\lambda_i) P_i.$$

Naturally, functions defined only on subsets of scalars may be extended to normal operators whose eigenvalues are restricted accordingly. A few examples of scalar functions extended to operators that will be important later in the course follow.

The exponential function of an operator

The exponential function $\alpha \mapsto \exp(\alpha)$ is defined for all $\alpha \in \mathbb{C}$, and may therefore be extended to a function $A \mapsto \exp(A)$ for any normal operator $A \in \mathrm{L}(\mathcal{X})$ by defining

$$\exp(A) = \sum_{i=1}^{k} \exp(\lambda_i) P_i,$$

assuming that the spectral decomposition of A is given by (1.3).

The exponential function may, in fact, be defined for all operators $A \in \mathrm{L}(\mathcal{X})$ by considering its usual Taylor series. In particular, the series

$$\exp(A) = \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

can be shown to converge for all operators $A \in \mathrm{L}(\mathcal{X})$, and agrees with the above notion based on the spectral decomposition in the case that A is normal.

Non-integer powers of operators

For $r > 0$ the function $\lambda \mapsto \lambda^r$ is defined for nonnegative real values $\lambda \in [0, \infty)$. For a given positive semidefinite operator $Q \in \mathrm{Pos}(\mathcal{X})$ having spectral decomposition (1.3), for which we necessarily have that $\lambda_i \geq 0$ for $1 \leq i \leq k$, we may therefore define

$$Q^r = \sum_{i=1}^{k} \lambda_i^r P_i.$$

For integer values of r, it is clear that Q^r coincides with the usual meaning of this expression given by the multiplication of operators. The case that $r = 1/2$ is particularly common, and in

this case we also write $\sqrt{Q}$ to denote $Q^{1/2}$. The operator $\sqrt{Q}$ is the unique positive semidefinite operator that satisfies

$$\sqrt{Q}\sqrt{Q} = Q.$$

Along similar lines, for any real number $r < 0$, the function $\lambda \mapsto \lambda^r$ is defined for positive real values $\lambda \in (0, \infty)$. For a given positive definite operator $Q \in \mathrm{Pd}(\mathcal{X})$, one defines Q^r in a similar way to above.

The logarithm of an operator

The function $\lambda \mapsto \log(\lambda)$ is defined for every positive real number $\lambda \in (0, \infty)$. For a given positive definite operator $Q \in \mathrm{Pd}(\mathcal{X})$, having a spectral decomposition (1.3) as above, one defines

$$\log(Q) = \sum_{i=1}^{k} \log(\lambda_i) P_i.$$

Logarithms of operators will be important during our discussion of von Neumann entropy.

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

Lecture 2: Mathematical preliminaries (part 2)

This lecture represents the second half of the discussion that we started in the previous lecture concerning basic mathematical concepts and tools used throughout the course.

2.1 The singular-value theorem

The spectral theorem, discussed in the previous lecture, is a valuable tool in quantum information theory. The fact that it is limited to normal operators can, however, restrict its applicability.

The *singular value theorem*, which we will now discuss, is closely related to the spectral theorem, but holds for arbitrary operators—even those of the form $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ for different spaces $\mathcal{X}$ and $\mathcal{Y}$. Like the spectral theorem, we will find that the singular value decomposition is an indispensable tool in quantum information theory. Let us begin with a statement of the theorem.

Theorem 2.1 (Singular value theorem)**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ be a nonzero operator, and let $r = \mathrm{rank}(A)$. There exist positive real numbers $s_1, \ldots, s_r$ and orthonormal sets $\{x_1, \ldots, x_r\} \subset \mathcal{X}$ and $\{y_1, \ldots, y_r\} \subset \mathcal{Y}$ such that*

$$A = \sum_{j=1}^{r} s_j y_j x_j^*. \tag{2.1}$$

An expression of a given matrix A in the form of (2.1) is said to be a *singular value decomposition* of A. The numbers $s_1, \ldots, s_r$ are called *singular values* and the vectors $x_1, \ldots, x_r$ and $y_1, \ldots, y_r$ are called *right* and *left singular vectors*, respectively.

The singular values $s_1, \ldots, s_r$ of an operator A are uniquely determined, up to their ordering. Hereafter we will assume, without loss of generality, that the singular values are ordered from largest to smallest: $s_1 \geq \cdots \geq s_r$. When it is necessary to indicate the dependence of these singular values on A, we denote them $s_1(A), \ldots, s_r(A)$. Although technically speaking 0 is not usually considered a singular value of any operator, it will be convenient to also define $s_k(A) = 0$ for $k > \mathrm{rank}(A)$. The notation $s(A)$ is used to refer to the vector of singular values $s(A) = (s_1(A), \ldots, s_r(A))$, or to an extension of this vector $s(A) = (s_1(A), \ldots, s_k(A))$ for $k > r$ when it is convenient to view it as an element of $\mathbb{R}^k$ for $k > \mathrm{rank}(A)$.

There is a close relationship between singular value decompositions of an operator A and spectral decompositions of the operators A^*A and AA^*. In particular, it will necessarily hold that

$$s_k(A) = \sqrt{\lambda_k(AA^*)} = \sqrt{\lambda_k(A^*A)} \tag{2.2}$$

for $1 \leq k \leq \mathrm{rank}(A)$, and moreover the right singular vectors of A will be eigenvectors of A^*A and the left singular vectors of A will be eigenvectors of AA^*. One is free, in fact, to choose the left singular vectors of A to be any orthonormal collection of eigenvectors of AA^* for which the corresponding eigenvalues are nonzero—and once this is done the right singular vectors will be uniquely determined. Alternately, the right singular vectors of A may be chosen to be

any orthonormal collection of eigenvectors of A^*A for which the corresponding eigenvalues are nonzero, which uniquely determines the left singular vectors.

In the case that $\mathcal{Y} = \mathcal{X}$ and A is a normal operator, it is essentially trivial to derive a singular value decomposition from a spectral decomposition. In particular, suppose that

$$A = \sum_{j=1}^{n} \lambda_j x_j x_j^*$$

is a spectral decomposition of A, and assume that we have chosen to label the eigenvalues of A in such a way that $\lambda_j \neq 0$ for $1 \leq j \leq r = \operatorname{rank}(A)$. A singular value decomposition of the form (2.1) is obtained by setting

$$s_j = |\lambda_j| \qquad \text{and} \qquad y_j = \frac{\lambda_j}{|\lambda_j|} x_j$$

for $1 \leq j \leq r$. Note that this shows, for normal operators, that the singular values are simply the absolute values of the nonzero eigenvalues.

2.1.1 The Moore-Penrose pseudo-inverse

Later in the course we will occasionally refer to the *Moore-Penrose pseudo-inverse* of an operator, which is closely related to its singular value decompositions. For any given operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$, we define the Moore-Penrose pseudo-inverse of A, denoted $A^+ \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$, as the unique operator satisfying these properties:

1. $AA^+A = A$,
2. $A^+AA^+ = A^+$, and
3. AA^+ and A^+A are both Hermitian.

It is clear that there is at least one such choice of A^+, for if

$$A = \sum_{j=1}^{r} s_j y_j x_j^*$$

is a singular value decomposition of A, then

$$A^+ = \sum_{j=1}^{r} \frac{1}{s_j} x_j y_j^*$$

satisfies the three properties above.

The fact that A^+ is uniquely determined by the above equations is easily verified, for suppose that $X, Y \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ both satisfy the above properties:

1. $AXA = A = AYA$,
2. $XAX = X$ and $YAY = Y$, and
3. AX, XA, AY, and YA are all Hermitian.

Using these properties, we observe that

$$\begin{aligned} X &= XAX = (XA)^*X = A^*X^*X = (AYA)^*X^*X = A^*Y^*A^*X^*X \\ &= (YA)^*(XA)^*X = YAXAX = YAX = YAYAX = Y(AY)^*(AX)^* \\ &= YY^*A^*X^*A^* = YY^*(AXA)^* = YY^*A^* = Y(AY)^* = YAY = Y, \end{aligned}$$

which shows that $X = Y$.

2.2 Linear mappings on operator algebras

Linear mappings of the form

$$\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}),$$

where $\mathcal{X}$ and $\mathcal{Y}$ are complex Euclidean spaces, play an important role in the theory of quantum information. The set of all such mappings is sometimes denoted $\mathrm{T}(\mathcal{X}, \mathcal{Y})$, or $\mathrm{T}(\mathcal{X})$ when $\mathcal{X} = \mathcal{Y}$, and is itself a linear space when addition of mappings and scalar multiplication are defined in the straightforward way:

1. Addition: given $\Phi, \Psi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, the mapping $\Phi + \Psi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is defined by

   $$(\Phi + \Psi)(A) = \Phi(A) + \Psi(A)$$

   for all $A \in \mathrm{L}(\mathcal{X})$.
2. Scalar multiplication: given $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ and $\alpha \in \mathbb{C}$, the mapping $\alpha\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is defined by

   $$(\alpha\Phi)(A) = \alpha(\Phi(A))$$

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

For a given mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, the *adjoint* of Φ is defined to be the unique mapping $\Phi^* \in \mathrm{T}(\mathcal{Y}, \mathcal{X})$ that satisfies

$$\langle \Phi^*(B), A \rangle = \langle B, \Phi(A) \rangle$$

for all $A \in \mathrm{L}(\mathcal{X})$ and $B \in \mathrm{L}(\mathcal{Y})$.

The transpose

$$T : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{X}) : A \mapsto A^{\mathsf{T}}$$

is a simple example of a mapping of this type, as is the trace

$$\mathrm{Tr} : \mathrm{L}(\mathcal{X}) \to \mathbb{C} : A \mapsto \mathrm{Tr}(A),$$

provided we make the identification $\mathrm{L}(\mathbb{C}) = \mathbb{C}$.

2.2.1 Remark on tensor products of operators and mappings

Tensor products of operators can be defined in concrete terms using the same sort of Kronecker product construction that we considered for vectors, as well as in more abstract terms connected with the notion of multilinear functions. We will briefly discuss these definitions now, as well as their extension to tensor products of mappings on operator algebras.

First, suppose $A_1 \in \mathrm{L}(\mathcal{X}_1, \mathcal{Y}_1), \ldots, A_n \in \mathrm{L}(\mathcal{X}_n, \mathcal{Y}_n)$ are operators, for complex Euclidean spaces

$$\mathcal{X}_1 = \mathbb{C}^{\Sigma_1}, \ldots, \mathcal{X}_n = \mathbb{C}^{\Sigma_n} \quad \text{and} \quad \mathcal{Y}_1 = \mathbb{C}^{\Gamma_1}, \ldots, \mathcal{Y}_n = \mathbb{C}^{\Gamma_n}.$$

We define a new operator

$$A_1 \otimes \cdots \otimes A_n \in \mathrm{L}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n),$$

in terms of its matrix representation, as

$$(A_1 \otimes \cdots \otimes A_n)((a_1, \ldots, a_n), (b_1, \ldots, b_n)) = A_1(a_1, b_1) \cdots A_n(a_n, b_n)$$

(for all $a_1 \in \Gamma_1, \ldots, a_n \in \Gamma_n$ and $b_1 \in \Sigma_1, \ldots, b_n \in \Gamma_n$).

It is not difficult to check that the operator $A_1 \otimes \cdots \otimes A_n$ just defined satisfies the equation

$$(A_1 \otimes \cdots \otimes A_n)(u_1 \otimes \cdots \otimes u_n) = (A_1 u_1) \otimes \cdots \otimes (A_n u_n) \tag{2.3}$$

for all choices of $u_1 \in \mathcal{X}_1, \ldots, u_n \in \mathcal{X}_n$. Given that $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$ is spanned by the set of all elementary tensors $u_1 \otimes \cdots \otimes u_n$, it is clear that $A_1 \otimes \cdots \otimes A_n$ is the only operator that can satisfy this equation (again, for all choices of $u_1 \in \mathcal{X}_1, \ldots, u_n \in \mathcal{X}_n$). We could, therefore, have considered the equation (2.3) to have been the defining property of $A_1 \otimes \cdots \otimes A_n$.

When considering operator spaces as vector spaces, similar identities to the ones in the previous lecture for tensor products of vectors become apparent. For example,

$$\begin{aligned} A_1 \otimes \cdots \otimes A_{k-1} \otimes (A_k + B_k) \otimes A_{k+1} \otimes \cdots \otimes A_n & \\ = A_1 \otimes \cdots \otimes A_{k-1} \otimes A_k \otimes A_{k+1} \otimes \cdots \otimes A_n & \\ + A_1 \otimes \cdots \otimes A_{k-1} \otimes B_k \otimes A_{k+1} \otimes \cdots \otimes A_n. & \end{aligned}$$

In addition, for all choices of complex Euclidean spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$, $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$, and $\mathcal{Z}_1, \ldots, \mathcal{Z}_n$, and all operators $A_1 \in \mathrm{L}(\mathcal{X}_1, \mathcal{Y}_1), \ldots, A_n \in \mathrm{L}(\mathcal{X}_n, \mathcal{Y}_n)$ and $B_1 \in \mathrm{L}(\mathcal{Y}_1, \mathcal{Z}_1), \ldots, B_n \in \mathrm{L}(\mathcal{Y}_n, \mathcal{Z}_n)$, it holds that

$$(B_1 \otimes \cdots \otimes B_n)(A_1 \otimes \cdots \otimes A_n) = (B_1 A_1) \otimes \cdots \otimes (B_n A_n).$$

Also note that spectral and singular value decompositions of tensor products of operators are very easily obtained from those of the individual operators. This allows one to quickly conclude that

$$\|A_1 \otimes \cdots \otimes A_n\|_p = \|A_1\|_p \cdots \|A_n\|_p,$$

along with a variety of other facts that may be derived by similar reasoning.

Tensor products of linear mappings on operator algebras may be defined in a similar way to those of operators. At this point we have not yet considered concrete representations of such mappings, to which a Kronecker product construction could be applied, but we will later discuss such representations. For now let us simply define the linear mapping

$$\Phi_1 \otimes \cdots \otimes \Phi_n : \mathrm{L}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n) \to \mathrm{L}(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n),$$

for any choice of linear mappings $\Phi_1 : \mathrm{L}(\mathcal{X}_1) \to \mathrm{L}(\mathcal{Y}_1), \ldots, \Phi_n : \mathrm{L}(\mathcal{X}_n) \to \mathrm{L}(\mathcal{Y}_n)$, to be the unique mapping that satisfies the equation

$$(\Phi_1 \otimes \cdots \otimes \Phi_n)(A_1 \otimes \cdots \otimes A_n) = \Phi_1(A_1) \otimes \cdots \otimes \Phi_n(A_n)$$

for all operators $A_1 \in \mathrm{L}(\mathcal{X}_1), \ldots, A_n \in \mathrm{L}(\mathcal{X}_n)$.

Example 2.2 (The partial trace)**.** Let $\mathcal{X}$ be a complex Euclidean space. As mentioned above, we may view the trace as taking the form $\mathrm{Tr} : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathbb{C})$ by making the identification $\mathbb{C} = \mathrm{L}(\mathbb{C})$. For a second complex Euclidean space $\mathcal{Y}$, we may therefore consider the mapping

$$\mathrm{Tr} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})} : \mathrm{L}(\mathcal{X} \otimes \mathcal{Y}) \to \mathrm{L}(\mathcal{Y}).$$

This is the unique mapping that satisfies

$$(\mathrm{Tr} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})})(A \otimes B) = \mathrm{Tr}(A) B$$

for all $A \in \mathrm{L}(\mathcal{X})$ and $B \in \mathrm{L}(\mathcal{Y})$. This mapping is called the *partial trace*, and is more commonly denoted $\mathrm{Tr}_{\mathcal{X}}$. In general, the subscript refers to the space to which the trace is applied, while the space or spaces that remains ($\mathcal{Y}$ in the case above) are implicit from the context in which the mapping is used.

One may alternately express the partial trace on $\mathcal{X}$ as follows, assuming that $\{x_a : a \in \Sigma\}$ is any orthonormal basis of $\mathcal{X}$:

$$\mathrm{Tr}_{\mathcal{X}}(A) = \sum_{a \in \Sigma} (x_a^* \otimes \mathbb{1}_{\mathcal{Y}}) A (x_a \otimes \mathbb{1}_{\mathcal{Y}})$$

for all $A \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$. An analogous expression holds for $\mathrm{Tr}_{\mathcal{Y}}$.

2.3 Norms of operators

The next topic for this lecture concerns norms of operators. As is true more generally, a *norm* on the space of operators $\mathrm{L}(\mathcal{X}, \mathcal{Y})$, for any choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, is a function $\|\cdot\|$ satisfying the following properties:

1. Positive definiteness: $\|A\| \geq 0$ for all $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$, with $\|A\| = 0$ if and only if $A = 0$.
2. Positive scalability: $\|\alpha A\| = |\alpha| \, \|A\|$ for all $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ and $\alpha \in \mathbb{C}$.
3. The triangle inequality: $\|A + B\| \leq \|A\| + \|B\|$ for all $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$.

Many interesting and useful norms can be defined on spaces of operators, but in this course we will mostly be concerned with a single family of norms called *Schatten p-norms*. This family includes the three most commonly used norms in quantum information theory: the *spectral norm*, the *Frobenius norm*, and the *trace norm*.

2.3.1 Definition and basic properties of Schatten norms

For any operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ and any real number $p \geq 1$, one defines the Schatten p-norm of A as

$$\|A\|_p = \left[\mathrm{Tr}\left((A^* A)^{p/2}\right)\right]^{1/p}.$$

We also define

$$\|A\|_\infty = \max\{\|Au\| : u \in \mathcal{X}, \ \|u\| = 1\}, \tag{2.4}$$

which happens to coincide with $\lim_{p \to \infty} \|A\|_p$ and therefore explains why the subscript ∞ is used.

An equivalent way to define these norms is to consider the the vector $s(A)$ of singular values of A, as discussed at the beginning of the lecture. For each $p \in [1, \infty]$, it holds that the Schatten p-norm of A coincides with the ordinary (vector) p-norm of $s(A)$:

$$\|A\|_p = \|s(A)\|_p.$$

The Schatten p-norms satisfy many nice properties, some of which are summarized in the following list:

1. The Schatten p-norms are non-increasing in p. In other words, for any operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ and for $1 \leq p \leq q \leq \infty$ we have
$$\|A\|_p \geq \|A\|_q.$$

2. For every $p \in [1,\infty]$, the Schatten p-norm is isometrically invariant (and therefore unitarily invariant). This means that
$$\|A\|_p = \|UAV^*\|_p$$
for any choice of linear isometries U and V (which include unitary operators U and V) for which the product UAV^* makes sense.
3. For each $p \in [1,\infty]$, one defines $p^* \in [1,\infty]$ by the equation
$$\frac{1}{p} + \frac{1}{p^*} = 1.$$
For every operator $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$, it holds that
$$\|A\|_p = \max\left\{ |\langle B, A\rangle| \,:\, B \in \mathrm{L}(\mathcal{X},\mathcal{Y}),\ \|B\|_{p^*} \leq 1 \right\}.$$
This implies that
$$|\langle B, A\rangle| \leq \|A\|_p \|B\|_{p^*},$$
which is *Hölder's inequality* for Schatten norms.
4. For any choice of linear operators $A \in \mathrm{L}(\mathcal{X}_1,\mathcal{X}_2)$, $B \in \mathrm{L}(\mathcal{X}_2,\mathcal{X}_3)$, and $C \in \mathrm{L}(\mathcal{X}_3,\mathcal{X}_4)$, and any choice of $p \in [1,\infty]$, we have
$$\|CBA\|_p \leq \|C\|_\infty \|B\|_p \|A\|_\infty.$$
It follows that
$$\|AB\|_p \leq \|A\|_p \|B\|_p \tag{2.5}$$
for all choices of $p \in [1,\infty]$ and operators A and B for which the product AB exists. The property (2.5) is known as *submultiplicativity*.
5. It holds that
$$\|A\|_p = \|A^*\|_p = \|A^{\mathsf{T}}\|_p = \|\overline{A}\|_p$$
for every $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$.

2.3.2 The trace norm, Frobenius norm, and spectral norm

The Schatten 1-norm is more commonly called the *trace norm*, the Schatten 2-norm is also known as the *Frobenius norm*, and the Schatten ∞-norm is called the *spectral norm* or *operator norm*. A common notation for these norms is:
$$\|\cdot\|_{\mathrm{tr}} = \|\cdot\|_1, \quad \|\cdot\|_{\mathrm{F}} = \|\cdot\|_2, \quad \text{and} \quad \|\cdot\| = \|\cdot\|_\infty.$$
In this course we will generally write $\|\cdot\|$ rather than $\|\cdot\|_\infty$, but will not use the notation $\|\cdot\|_{\mathrm{tr}}$ and $\|\cdot\|_{\mathrm{F}}$.

Let us note a few special properties of these three particular norms:

1. *The spectral norm.* The spectral norm $\|\cdot\| = \|\cdot\|_\infty$, also called the *operator norm*, is special in several respects. It is the norm *induced* by the Euclidean norm, which is its defining property (2.4). It satisfies the property
$$\|A^*A\| = \|A\|^2$$
for every $A \in \mathrm{L}(\mathcal{X},\mathcal{Y})$.

2. *The Frobenius norm.* Substituting $p = 2$ into the definition of $\|\cdot\|_p$ we see that the Frobenius norm $\|\cdot\|_2$ is given by

$$\|A\|_2 = [\mathrm{Tr}\,(A^*A)]^{1/2} = \sqrt{\langle A, A\rangle}.$$

It is therefore the norm defined by the inner product on $\mathrm{L}\,(\mathcal{X}, \mathcal{Y})$. In essence, it is the norm that one obtains by thinking of elements of $\mathrm{L}\,(\mathcal{X}, \mathcal{Y})$ as ordinary vectors and forgetting that they are operators:

$$\|A\|_2 = \sqrt{\sum_{a,b} |A(a,b)|^2},$$

where a and b range over the indices of the matrix representation of A.

3. *The trace norm.* Substituting $p = 1$ into the definition of $\|\cdot\|_p$ we see that the trace norm $\|\cdot\|_1$ is given by

$$\|A\|_1 = \mathrm{Tr}\left(\sqrt{A^*A}\right).$$

A convenient expression of $\|A\|_1$, for any operator of the form $A \in \mathrm{L}\,(\mathcal{X})$, is

$$\|A\|_1 = \max\{|\langle A, U\rangle| \,:\, U \in \mathrm{U}\,(\mathcal{X})\}.$$

Another useful fact about the trace norm is that it is *monotonic*:

$$\|\mathrm{Tr}_{\mathcal{Y}}(A)\|_1 \leq \|A\|_1$$

for all $A \in \mathrm{L}\,(\mathcal{X} \otimes \mathcal{Y})$. This is because

$$\|\mathrm{Tr}_{\mathcal{Y}}(A)\|_1 = \max\left\{|\langle A, U \otimes \mathbb{1}_{\mathcal{Y}}\rangle| \,:\, U \in \mathrm{U}\,(\mathcal{X})\right\}$$

while

$$\|A\|_1 = \max\left\{|\langle A, U\rangle| \,:\, U \in \mathrm{U}\,(\mathcal{X} \otimes \mathcal{Y})\right\};$$

and the inequality follows from the fact that the first maximum is taken over a subset of the unitary operators for the second.

Example 2.3. Consider a complex Euclidean space $\mathcal{X}$ and any choice of unit vectors $u, v \in \mathcal{X}$. We have

$$\|uu^* - vv^*\|_p = 2^{1/p}\sqrt{1 - |\langle u, v\rangle|^2}. \tag{2.6}$$

To see this, we note that the operator $A = uu^* - vv^*$ is Hermitian and therefore normal, so its singular values are the absolute values of its nonzero eigenvalues. It will therefore suffice to prove that the eigenvalues of A are $\pm\sqrt{1 - |\langle u, v\rangle|^2}$, along with the eigenvalue 0 occurring with multiplicity $n - 2$, where $n = \dim(\mathcal{X})$. Given that $\mathrm{Tr}(A) = 0$ and $\mathrm{rank}(A) \leq 2$, it is evident that the eigenvalues of A are of the form $\pm\lambda$ for some $\lambda \geq 0$, along with eigenvalue 0 with multiplicity $n - 2$. As

$$2\lambda^2 = \mathrm{Tr}(A^2) = 2 - 2|\langle u, v\rangle|^2$$

we conclude $\lambda = \sqrt{1 - |\langle u, v\rangle|^2}$, from which (2.6) follows:

$$\|uu^* - vv^*\|_p = \left(2\left(1 - |\langle u, v\rangle|^2\right)^{p/2}\right)^{1/p} = 2^{1/p}\sqrt{1 - |\langle u, v\rangle|^2}.$$

2.4 The operator-vector correspondence

It will be helpful throughout this course to make use of a simple correspondence between the spaces $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ and $\mathcal{Y} \otimes \mathcal{X}$, for given complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$.

We define the mapping

$$\mathrm{vec} : \mathrm{L}(\mathcal{X}, \mathcal{Y}) \to \mathcal{Y} \otimes \mathcal{X}$$

to be the linear mapping that represents a change of bases from the standard basis of $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ to the standard basis of $\mathcal{Y} \otimes \mathcal{X}$. Specifically, we define

$$\mathrm{vec}(E_{b,a}) = e_b \otimes e_a$$

for all $a \in \Sigma$ and $b \in \Gamma$, at which point the mapping is determined for every $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ by linearity. In the Dirac notation, this mapping amounts to flipping a bra to a ket:

$$\mathrm{vec}(|b\rangle \langle a|) = |b\rangle |a\rangle .$$

(Note that it is only standard basis elements that are flipped in this way.)

The vec mapping is a linear bijection, which implies that every vector $u \in \mathcal{Y} \otimes \mathcal{X}$ uniquely determines an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ that satisfies $\mathrm{vec}(A) = u$. It is also an isometry, in the sense that

$$\langle A, B \rangle = \langle \mathrm{vec}(A), \mathrm{vec}(B) \rangle$$

for all $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$. The following properties of the vec mapping are easily verified:

1. For every choice of complex Euclidean spaces $\mathcal{X}_1$, $\mathcal{X}_2$, $\mathcal{Y}_1$, and $\mathcal{Y}_2$, and every choice of operators $A \in \mathrm{L}(\mathcal{X}_1, \mathcal{Y}_1)$, $B \in \mathrm{L}(\mathcal{X}_2, \mathcal{Y}_2)$, and $X \in \mathrm{L}(\mathcal{X}_2, \mathcal{X}_1)$, it holds that

$$(A \otimes B)\,\mathrm{vec}(X) = \mathrm{vec}(AXB^{\mathsf{T}}). \tag{2.7}$$

2. For every choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, and every choice of operators $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$, the following equations hold:

$$\mathrm{Tr}_{\mathcal{X}} \left(\mathrm{vec}(A)\,\mathrm{vec}(B)^*\right) = AB^*, \tag{2.8}$$

$$\mathrm{Tr}_{\mathcal{Y}} \left(\mathrm{vec}(A)\,\mathrm{vec}(B)^*\right) = \left(B^* A\right)^{\mathsf{T}}. \tag{2.9}$$

3. For $u \in \mathcal{X}$ and $v \in \mathcal{Y}$ we have

$$\mathrm{vec}(uv^*) = u \otimes \overline{v}. \tag{2.10}$$

   This includes the special cases $\mathrm{vec}(u) = u$ and $\mathrm{vec}(v^*) = \overline{v}$, which we obtain by setting $v = 1$ and $u = 1$, respectively.

Example 2.4 (The Schmidt decomposition)**.** Suppose $u \in \mathcal{Y} \otimes \mathcal{X}$ for given complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$. Let $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ be the unique operator for which $u = \mathrm{vec}(A)$. There exists a singular value decomposition

$$A = \sum_{i=1}^{r} s_i y_i x_i^*$$

of A. Consequently

$$u = \mathrm{vec}(A) = \mathrm{vec}\left(\sum_{i=1}^{r} s_i y_i x_i^*\right) = \sum_{i=1}^{r} s_i\,\mathrm{vec}\left(y_i x_i^*\right) = \sum_{i=1}^{r} s_i y_i \otimes \overline{x_i}.$$

The fact that $\{x_1, \ldots, x_r\}$ is orthonormal implies that $\{\overline{x_1}, \ldots, \overline{x_r}\}$ is orthonormal as well.

We have therefore established the validity of the *Schmidt decomposition*, which states that every vector $u \in \mathcal{Y} \otimes \mathcal{X}$ can be expressed in the form

$$u = \sum_{i=1}^{r} s_i y_i \otimes z_i$$

for positive real numbers $s_1, \ldots, s_r$ and orthonormal sets $\{y_1, \ldots, y_r\} \subset \mathcal{Y}$ and $\{z_1, \ldots, z_r\} \subset \mathcal{X}$.

2.5 Analysis

Mathematical analysis is concerned with notions of limits, continuity, differentiation, integration and measure, and so on. As some of the proofs that we will encounter in the course will require arguments based on these notions, it is appropriate to briefly review some of the necessary concepts here.

It will be sufficient for our needs that this summary is narrowly focused on Euclidean spaces (as opposed to infinite dimensional spaces). As a result, these notes do not treat analytic concepts in the sort of generality that would be typical of a standard analysis book or course. If you are interested in such a book, the following one is considered a classic:

- W. Rudin. *Principles of Mathematical Analysis*. McGraw–Hill, 1964.

2.5.1 Basic notions of analysis

Let $\mathcal{V}$ be a real or complex Euclidean space, and (for this section only) let us allow $\|\cdot\|$ to be any choice of a fixed norm on $\mathcal{V}$. We may take $\|\cdot\|$ to be the Euclidean norm, but nothing changes if we choose a different norm. (The validity of this assumption rests on the fact that Euclidean spaces are finite-dimensional.)

The *open ball* of radius r around a vector $u \in \mathcal{X}$ is defined as

$$\mathcal{B}_r(u) = \{v \in \mathcal{X} : \|u - v\| < r\},$$

and the *sphere* of radius r around u is defined as

$$\mathcal{S}_r(u) = \{v \in \mathcal{X} : \|u - v\| = r\}.$$

The *closed ball* of radius r around u is the union $\mathcal{B}_r(u) \cup \mathcal{S}_r(u)$.

A set $\mathcal{A} \subseteq \mathcal{X}$ is *open* if, for every $u \in \mathcal{A}$ there exists a choice of $\epsilon > 0$ such that $\mathcal{B}_\epsilon(u) \subseteq \mathcal{A}$. Equivalently, $\mathcal{A} \subseteq \mathcal{X}$ is open if it is the union of some collection of open balls. (This can be an empty, finite, or countably or uncountably infinite collections of open balls.) A set $\mathcal{A} \subseteq \mathcal{X}$ is *closed* if it is the complement of an open set.

Given subsets $\mathcal{B} \subseteq \mathcal{A} \subseteq \mathcal{X}$, we say that $\mathcal{B}$ is open or closed *relative to* $\mathcal{A}$ if $\mathcal{B}$ is the intersection of $\mathcal{A}$ and some open or closed set in $\mathcal{X}$, respectively.

Let $\mathcal{A}$ and $\mathcal{B}$ be subsets of a Euclidean space $\mathcal{X}$ that satisfy $\mathcal{B} \subseteq \mathcal{A}$. Then the *closure* of $\mathcal{B}$ relative to $\mathcal{A}$ is the intersection of all subsets $\mathcal{C}$ for which $\mathcal{B} \subseteq \mathcal{C}$ and $\mathcal{C}$ is closed relative to $\mathcal{A}$. In other words, this is the smallest set that contains $\mathcal{B}$ and is closed relative to $\mathcal{A}$. The set $\mathcal{B}$ is *dense* in $\mathcal{A}$ if the closure of $\mathcal{B}$ relative to $\mathcal{A}$ is $\mathcal{A}$ itself.

Suppose $\mathcal{X}$ and $\mathcal{Y}$ are Euclidean spaces and $f : \mathcal{A} \to \mathcal{Y}$ is a function defined on some subset $\mathcal{A} \subseteq \mathcal{X}$. For any point $u \in \mathcal{A}$, the function f is said to be *continuous* at u if the following holds: for every $\varepsilon > 0$ there exists $\delta > 0$ such that

$$\|f(v) - f(u)\| < \varepsilon$$

for all $v \in \mathcal{B}_\delta(u) \cap \mathcal{A}$. An alternate way of writing this condition is

$$(\forall \varepsilon > 0)(\exists \delta > 0)[f(\mathcal{B}_\delta(u) \cap \mathcal{A}) \subseteq \mathcal{B}_\varepsilon(f(u))].$$

If f is continuous at every point in $\mathcal{A}$, then we just say that f is *continuous on* $\mathcal{A}$.

The *preimage* of a set $\mathcal{B} \subseteq \mathcal{Y}$ under a function $f : \mathcal{A} \to \mathcal{Y}$ defined on some subset $\mathcal{A} \subseteq \mathcal{X}$ is defined as

$$f^{-1}(\mathcal{B}) = \{u \in \mathcal{A} \,:\, f(u) \in \mathcal{B}\}.$$

Such a function f is continuous on $\mathcal{A}$ if and only if the preimage of every open set in $\mathcal{Y}$ is open relative to $\mathcal{A}$. Equivalently, f is continuous on $\mathcal{A}$ if and only if the preimage of every closed set in $\mathcal{Y}$ is closed relative to $\mathcal{A}$.

A *sequence* of vectors in a subset $\mathcal{A}$ of a Euclidean space $\mathcal{X}$ is a function $s : \mathbb{N} \to \mathcal{A}$, where $\mathbb{N}$ denotes the set of natural numbers $\{1, 2, \ldots\}$. We usually denote a general sequence by $(u_n)_{n\in\mathbb{N}}$ or (u_n), and it is understood that the function s in question is given by $s : n \mapsto u_n$. A sequence $(u_n)_{n\in\mathbb{N}}$ in $\mathcal{X}$ *converges* to $u \in \mathcal{X}$ if, for all $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that $\|u_n - u\| < \varepsilon$ for all $n \geq N$.

A sequence (v_n) is a *sub-sequence* of (u_n) if there is a strictly increasing sequence of nonnegative integers $(k_n)_{n\in\mathbb{N}}$ such that $v_n = u_{k_n}$ for all $n \in \mathbb{N}$. In other words, you get a sub-sequence from a sequence by skipping over whichever vectors you want, provided that you still have infinitely many vectors left.

2.5.2 Compact sets

A set $\mathcal{A} \subseteq \mathcal{X}$ is *compact* if every sequence (u_n) in $\mathcal{A}$ has a sub-sequence (v_n) that converges to a point $v \in \mathcal{A}$. In any Euclidean space $\mathcal{X}$, a set $\mathcal{A}$ is compact if and only if it is closed and bounded (which means it is contained in $\mathcal{B}_r(0)$ for some real number $r > 0$). This fact is known as the *Heine-Borel Theorem*.

Compact sets have some nice properties. Two properties that are noteworthy for the purposes of this course are following:

1. If $\mathcal{A}$ is compact and $f : \mathcal{A} \to \mathbb{R}$ is continuous on $\mathcal{A}$, then f achieves both a maximum and minimum value on $\mathcal{A}$.
2. Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces. If $\mathcal{A} \subset \mathcal{X}$ is compact and $f : \mathcal{X} \to \mathcal{Y}$ is continuous on $\mathcal{A}$, then $f(\mathcal{A}) \subset \mathcal{Y}$ is also compact.

2.6 Convexity

Many sets of interest in the theory of quantum information are *convex sets*, and when reasoning about some of these sets we will make use of various facts from the the theory of convexity (or convex analysis). Two books on convexity theory that you may find helpful are these:

- R. T. Rockafellar. *Convex Analysis*. Princeton University Press, 1970.
- A. Barvinok. *A Course in Convexity*. Volume 54 of *Graduate Studies in Mathematics*, American Mathematical Society, 2002.

2.6.1 Basic notions of convexity

Let $\mathcal{X}$ be any Euclidean space. A set $\mathcal{A} \subseteq \mathcal{X}$ is *convex* if, for all choices of $u, v \in \mathcal{A}$ and $\lambda \in [0,1]$, we have

$$\lambda u + (1-\lambda)v \in \mathcal{A}.$$

Another way to say this is that $\mathcal{A}$ is convex if and only if you can always draw the straight line between any two points of $\mathcal{A}$ without going outside $\mathcal{A}$.

A point $w \in \mathcal{A}$ in a convex set $\mathcal{A}$ is said to be an *extreme point* of $\mathcal{A}$ if, for every expression

$$w = \lambda u + (1-\lambda)v$$

for $u, v \in \mathcal{A}$ and $\lambda \in (0,1)$, it holds that $u = v = w$. These are the points that do not lie *properly* between two other points in $\mathcal{A}$.

A set $\mathcal{A} \subseteq \mathcal{X}$ is a *cone* if, for all choices of $u \in \mathcal{A}$ and $\lambda \geq 0$, we have that $\lambda u \in \mathcal{A}$. A *convex cone* is simply a cone that is also convex. A cone $\mathcal{A}$ is convex if and only if, for all $u, v \in \mathcal{A}$, it holds that $u + v \in \mathcal{A}$.

The intersection of any collection of convex sets is also convex. Also, if $\mathcal{A}, \mathcal{B} \subseteq \mathcal{X}$ are convex, then their sum and difference

$$\mathcal{A} + \mathcal{B} = \{u + v \,:\, u \in \mathcal{A},\, v \in \mathcal{B}\} \quad \text{and} \quad \mathcal{A} - \mathcal{B} = \{u - v \,:\, u \in \mathcal{A},\, v \in \mathcal{B}\}$$

are also convex.

Example 2.5. For any $\mathcal{X}$, the set $\mathrm{Pos}(\mathcal{X})$ is a convex cone. This is so because it follows easily from the definition of positive semidefinite operators that $\mathrm{Pos}(\mathcal{X})$ is a cone and $A + B \in \mathrm{Pos}(\mathcal{X})$ for all $A, B \in \mathrm{Pos}(\mathcal{X})$. The only extreme point of this set is $0 \in \mathrm{L}(\mathcal{X})$. The set $\mathrm{D}(\mathcal{X})$ of density operators on $\mathcal{X}$ is convex, but it is not a cone. Its extreme points are precisely those density operators having rank 1, i.e., those of the form uu^* for $u \in \mathcal{X}$ being a unit vector.

For any finite, nonempty set Σ, we say that a vector $p \in \mathbb{R}^\Sigma$ is a *probability vector* if it holds that $p(a) \geq 0$ for all $a \in \Sigma$ and $\sum_{a \in \Sigma} p(a) = 1$. A *convex combination* of points in $\mathcal{A}$ is any finite sum of the form

$$\sum_{a \in \Sigma} p(a) u_a$$

for $\{u_a \,:\, a \in \Sigma\} \subset A$ and $p \in \mathbb{R}^\Sigma$ a probability vector. Notice that we are speaking only of *finite* sums when we refer to convex combinations.

The *convex hull* of a set $\mathcal{A} \subseteq \mathcal{X}$, denoted $\mathrm{conv}(\mathcal{A})$, is the intersection of all convex sets containing $\mathcal{A}$. Equivalently, it is precisely the set of points that can be written as convex combinations of points in $\mathcal{A}$. This is true even in the case that $\mathcal{A}$ is infinite. The convex hull $\mathrm{conv}(\mathcal{A})$ of a closed set $\mathcal{A}$ need not itself be closed. However, if $\mathcal{A}$ is compact, then so too is $\mathrm{conv}(\mathcal{A})$. The *Krein-Milman theorem* states that every compact, convex set $\mathcal{A}$ is equal to the convex hull of its extreme points.

2.6.2 A few theorems about convex analysis in real Euclidean spaces

It will be helpful later for us to make use of the following three theorems about convex sets. These theorems concern just *real* Euclidean spaces $\mathbb{R}^\Sigma$, but this will not limit their applicability to quantum information theory: we will use them when considering spaces $\mathrm{Herm}\left(\mathbb{C}^\Gamma\right)$ of Hermitian operators, which may be considered as real Euclidean spaces taking the form $\mathbb{R}^{\Gamma \times \Gamma}$ (as discussed in the previous lecture).

The first theorem is *Carathéodory's theorem*. It implies that every element in the convex hull of a subset $\mathcal{A} \subseteq \mathbb{R}^\Sigma$ can always be written as a convex combination of a small number of points in $\mathcal{A}$ (where *small* means at most $|\Sigma| + 1$). This is true regardless of the size or any other properties of the set $\mathcal{A}$.

Theorem 2.6 (Carathéodory's theorem)**.** *Let $\mathcal{A}$ be any subset of a real Euclidean space $\mathbb{R}^\Sigma$, and let $m = |\Sigma| + 1$. For every element $u \in \operatorname{conv}(\mathcal{A})$, there exist m (not necessarily distinct) points $u_1, \ldots, u_m \in \mathcal{A}$, such that u may be written as a convex combination of $u_1, \ldots, u_m$.*

The second theorem is an example of a *minmax* theorem that is attributed to Maurice Sion. In general, minmax theorems provide conditions under which a minimum and a maximum can be reversed without changing the value of the expression in which they appear.

Theorem 2.7 (Sion's minmax theorem)**.** *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are compact and convex subsets of a real Euclidean space $\mathbb{R}^\Sigma$. It holds that*

$$\min_{u \in \mathcal{A}} \max_{v \in \mathcal{B}} \langle u, v \rangle = \max_{v \in \mathcal{B}} \min_{u \in \mathcal{A}} \langle u, v \rangle .$$

This theorem is not actually as general as the one proved by Sion, but it will suffice for our needs. One of the ways it can be generalized is to drop the condition that one of the two sets is compact (which generally requires either the minimum or the maximum to be replaced by an infimum or supremum).

Finally, let us state one version of a *separating hyperplane* theorem, which essentially states that if one has a closed, convex subset $\mathcal{A} \subset \mathbb{R}^\Sigma$ and a point $u \in \mathbb{R}^\Sigma$ that is not contained in $\mathcal{A}$, then it is possible to cut $\mathbb{R}^\Sigma$ into two separate (open) half-spaces so that one contains $\mathcal{A}$ and the other contains u.

Theorem 2.8 (Separating hyperplane theorem)**.** *Suppose that $\mathcal{A}$ is a closed and convex subset of a real Euclidean space $\mathbb{R}^\Sigma$ and $u \in \mathbb{R}^\Sigma$ not contained in $\mathcal{A}$. There exists a vector $v \in \mathbb{R}^\Sigma$ for which*

$$\langle v, w \rangle > \langle v, u \rangle$$

for all choices of $w \in \mathcal{A}$.

There are other separating hyperplane theorems that are similar in spirit to this one, but this one will be sufficient for us.

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

Lecture 3: States, measurements, and channels

We begin our discussion of quantum information in this lecture, starting with an overview of three mathematical objects that provide a basic foundation for the theory: states, measurements, and channels. We will also begin to discuss important notions connected with these objects, and will continue with this discussion in subsequent lectures.

3.1 Overview of states, measurements, and channels

The theory of quantum information is concerned with properties of abstract, idealized physical systems that will be called *registers* throughout this course. In particular, one defines the notions of *states* of registers; of *measurements* of registers, which produce classical information concerning their states; and of *channels*, which transform states of one register into states of another. Taken together, these definitions provide the basic model with which quantum information theory is concerned.

3.1.1 Registers

The term *register* is intended to be suggestive of a component inside a computer in which some finite amount of data can be stored and manipulated. While this is a reasonable picture to keep in mind, it should be understood that any physical system in which a finite amount of data may be stored, and whose state may change over time, could be modeled as a register. Examples include the entire memory of a computer, or a collection of computers, or any medium used for the transmission of information from one source to another. At an intuitive level, what is most important is that registers are viewed as a physical objects, or parts of a physical objects, that store information.

It is not difficult to formulate a precise mathematical definition of registers, but we will not take the time to do this in this course. It will suffice for our needs to state two simple assumptions about registers:

1. Every register has a unique name that distinguishes it from other registers.
2. Every register has associated to it a finite and nonempty set of *classical states*.

Typical names for registers in these notes are capital letters written in a *sans serif* font, such as X, Y, and Z, as well as subscripted variants of these names like $\mathsf{X}_1, \ldots, \mathsf{X}_n$, Y_A, and Y_B. In every situation we will encounter in this course, there will be a finite (but not necessarily bounded) number of registers under consideration.

There may be legitimate reasons, both mathematical and physical, to object to the assumption that registers have specified classical state sets associated to them. In essence, this assumption amounts to the selection of a preferred basis from which to develop the theory, as opposed to opting for a basis-independent theory. From a computational or information processing point of view, however, it is quite natural to assume the existence of a preferred basis, and little (or

perhaps nothing) is lost by making this assumption in the finite-dimensional setting in which we will work.

Suppose that X is a register whose classical state set is Σ. We then associate the complex Euclidean space $\mathcal{X} = \mathbb{C}^{\Sigma}$ with the register X. States, measurements, and channels connected with X will then be described in linear-algebraic terms that refer to this space. As a general convention, we will always name the complex Euclidean space associated with a given register with the same letter as the register, but in a scripted font rather than a *sans serif* font. For instance, the complex Euclidean spaces associated with registers Y_j and Z_A are denoted $\mathcal{Y}_j$ and $\mathcal{Z}_A$, respectively. This is done throughout these notes without explicit mention.

For any finite sequence $\mathsf{X}_1, \ldots, \mathsf{X}_n$ of distinct registers, we may view that the n-tuple

$$\mathsf{Y} = (\mathsf{X}_1, \ldots, \mathsf{X}_n)$$

is itself a register. Assuming that the classical state sets of the registers $\mathsf{X}_1, \ldots, \mathsf{X}_n$ are given by $\Sigma_1, \ldots, \Sigma_n$, respectively, we naturally take the classical state set of Y to be $\Sigma_1 \times \cdots \times \Sigma_n$. The complex Euclidean space associated with Y is therefore

$$\mathcal{Y} = \mathbb{C}^{\Sigma_1 \times \cdots \times \Sigma_n} = \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n.$$

3.1.2 States

A *quantum state* (or simply a *state*) of a register X is an element of the set

$$\mathrm{D}(\mathcal{X}) = \{\rho \in \mathrm{Pos}(\mathcal{X}) : \mathrm{Tr}(\rho) = 1\}$$

of *density operators* on $\mathcal{X}$. Every element of this set is to be considered a valid state of X.

A state $\rho \in \mathrm{D}(\mathcal{X})$ is said to be *pure* if it takes the form

$$\rho = uu^*$$

for some vector $u \in \mathcal{X}$. (Given that $\mathrm{Tr}(uu^*) = \|u\|^2$, any such vector is necessarily a unit vector.) An equivalent condition is that $\mathrm{rank}(\rho) = 1$. The term *mixed state* is sometimes used to refer to a state that is either not pure or not necessarily pure, but we will generally not use this terminology: it will be our default assumption that states are not necessarily pure, provided it has not been explicitly stated otherwise.

Three simple observations (the first two of which were mentioned briefly in the previous lecture) about the set of states $\mathrm{D}(\mathcal{X})$ of a register X are as follows.

1. The set $\mathrm{D}(\mathcal{X})$ is *convex*: if $\rho, \sigma \in \mathrm{D}(\mathcal{X})$ and $\lambda \in [0,1]$, then $\lambda\rho + (1-\lambda)\sigma \in \mathrm{D}(\mathcal{X})$.
2. The *extreme points* of $\mathrm{D}(\mathcal{X})$ are precisely the pure states uu^* for $u \in \mathcal{X}$ ranging over all unit vectors.
3. The set $\mathrm{D}(\mathcal{X})$ is *compact*.

One way to argue that $\mathrm{D}(\mathcal{X})$ is compact, starting from the assumption that the unit sphere $\mathcal{S} = \{u \in \mathcal{X} : \|u\| = 1\}$ in $\mathcal{X}$ is compact, is as follows. We first note that the function $f : \mathcal{S} \to \mathrm{D}(\mathcal{X}) : u \mapsto uu^*$ is continuous, so the set of pure states $f(\mathcal{S}) = \{uu^* : u \in \mathcal{X}, \|u\| = 1\}$ is compact (as continuous functions always map compact sets to compact sets). By the spectral theorem it is clear that $\mathrm{D}(\mathcal{X})$ is the convex hull of this set: $\mathrm{D}(\mathcal{X}) = \mathrm{conv}\{uu^* : u \in \mathcal{X}, \|u\| = 1\}$. As the convex hull of every compact set is compact, it follows that $\mathrm{D}(\mathcal{X})$ is compact.

Let $\mathsf{X}_1, \ldots, \mathsf{X}_n$ be distinct registers, and let Y be the register formed by viewing these n registers as a single, compound register: $\mathsf{Y} = (\mathsf{X}_1, \ldots, \mathsf{X}_n)$. A state of Y taking the form

$$\rho_1 \otimes \cdots \otimes \rho_n \in \mathrm{D}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right),$$

for density operators $\rho_1 \in \mathrm{D}\left(\mathcal{X}_1\right), \ldots, \rho_n \in \mathrm{D}\left(\mathcal{X}_n\right)$, is said to be a *product state*. It represents the situation that $\mathsf{X}_1, \ldots, \mathsf{X}_n$ are *independent*, or that their states are independent, at a particular moment. If the state of Y cannot be expressed as product state, it is said that $\mathsf{X}_1, \ldots, \mathsf{X}_n$ are *correlated*. This includes the possibility that $\mathsf{X}_1, \ldots, \mathsf{X}_n$ are *entangled*, which is a phenomenon that we will discuss in detail later in the course. Registers can, however, be correlated without being entangled.

3.1.3 Measurements

A *measurement* of a register X (or a measurement on a complex Euclidean space $\mathcal{X}$) is a function of the form

$$\mu : \Gamma \to \mathrm{Pos}\left(\mathcal{X}\right),$$

where Γ is a finite, nonempty set of *measurement outcomes*. To be considered a valid measurement, such a function must satisfy the constraint

$$\sum_{a \in \Gamma} \mu(a) = \mathbb{1}_{\mathcal{X}}.$$

It is common that one identifies the measurement μ with the collection of operators $\{P_a : a \in \Gamma\}$, where $P_a = \mu(a)$ for each $a \in \Gamma$. Each operator P_a is called the *measurement operator* associated with the outcome $a \in \Gamma$.

When a measurement of the form $\mu : \Gamma \to \mathrm{Pos}\left(\mathcal{X}\right)$ is applied to a register X whose state is $\rho \in \mathrm{D}\left(\mathcal{X}\right)$, two things happen:

1. An element of Γ is randomly selected as the outcome of the measurement. The probability associated with each possible outcome $a \in \Gamma$ is given by

$$p(a) = \langle \mu(a), \rho \rangle .$$

2. The register X ceases to exist.

This definition of measurements guarantees that the vector $p \in \mathbb{R}^{\Gamma}$ of outcome probabilities will indeed be a probability vector, for every choice of $\rho \in \mathrm{D}\left(\mathcal{X}\right)$. In particular, each $p(a)$ is a nonnegative real number because the inner product of two positive semidefinite operators is necessarily a nonnegative real number, and the probabilities sum to 1 due to the constraint $\sum_{a \in \Gamma} \mu(a) = \mathbb{1}_{\mathcal{X}}$. In more detail,

$$\sum_{a \in \Gamma} p(a) = \sum_{a \in \Gamma} \langle \mu(a), \rho \rangle = \langle \mathbb{1}_{\mathcal{X}}, \rho \rangle = \mathrm{Tr}(\rho) = 1.$$

It can be sown that *every* linear function that maps $\mathrm{D}\left(\mathcal{X}\right)$ to the set of probability vectors in $\mathbb{R}^{\Gamma}$ is induced by some measurement μ as we have just discussed. It is therefore not an arbitrary choice to define measurements as they are defined, but rather a reflection of the idea that every linear function mapping density operators to probability vectors is to be considered a valid measurement.

Note that the assumption that the register that is measured ceases to exist is not necessarily standard: you will find definitions of measurements in books and papers that do not make this assumption, and provide a description of the state that is left in the register after the measurement. No generality is lost, however, in making the assumption that registers cease to exist upon being measured. This is because standard notions of *nondestructive measurements*, which specify the states of registers after they are measured, can be described by composing channels with measurements (as we have defined them).

A measurement of the form

$$\mu : \Gamma_1 \times \cdots \times \Gamma_n \to \mathrm{Pos}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right),$$

defined on a register of the form $\mathsf{Y} = (\mathsf{X}_1, \ldots, \mathsf{X}_n)$, is called a *product measurement* if there exist measurements

$$\begin{gathered} \mu_1 : \Gamma_1 \to \mathrm{Pos}\left(\mathcal{X}_1\right), \\ \vdots \\ \mu_n : \Gamma_n \to \mathrm{Pos}\left(\mathcal{X}_n\right) \end{gathered}$$

such that

$$\mu(a_1, \ldots, a_n) = \mu_1(a_1) \otimes \cdots \otimes \mu_n(a_n)$$

for all $(a_1, \ldots, a_n) \in \Gamma_1 \times \cdots \times \Gamma_n$. Similar to the interpretation of a product state, a product measurement describes the situation in which the measurements $\mu_1, \ldots, \mu_n$ are independently applied to registers $\mathsf{X}_1, \ldots, \mathsf{X}_n$, and the n-tuple of measurement outcomes is interpreted as a single measurement outcome of the compound measurement μ.

A *projective measurement* $\mu : \Gamma \to \mathrm{Pos}\left(\mathcal{X}\right)$ is one for which $\mu(a)$ is a projection operator for each $a \in \Gamma$. The only way this can happen in the presence of the constraint $\sum_{a \in \Gamma} \mu(a) = \mathbb{1}_{\mathcal{X}}$ is for the measurement operators $\{P_a : a \in \Gamma\}$ to be projections onto mutually orthogonal subspaces of $\mathcal{X}$. When $\{x_a : a \in \Sigma\}$ is an orthonormal basis of $\mathcal{X}$, the projective measurement

$$\mu : \Sigma \to \mathrm{Pos}\left(\mathcal{X}\right) : a \mapsto x_a x_a^*$$

is referred to as the measurement with respect to the basis $\{x_a : a \in \Sigma\}$.

3.1.4 Channels

Quantum channels represent idealized physical operations that transform states of one register into states of another. In mathematical terms, a *quantum channel* from a register X to a register Y is a linear mapping of the form

$$\Phi : \mathrm{L}\left(\mathcal{X}\right) \to \mathrm{L}\left(\mathcal{Y}\right)$$

that satisfies two restrictions:

1. Φ must be *trace-preserving*, and
2. Φ must be *completely positive*.

These restrictions will be explained shortly.

When a quantum channel from X to Y is applied to X, it is to be viewed that the register X ceases to exist, having been replaced by or transformed into the register Y. The state of Y is determined by applying the mapping Φ to the state $\rho \in \mathrm{D}\left(\mathcal{X}\right)$ of X, yielding $\Phi(\rho) \in \mathrm{D}\left(\mathcal{Y}\right)$.

There is nothing that precludes the choice that $\mathsf{X} = \mathsf{Y}$, and in this case one simply views that the state of the register X has been changed according to the mapping $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{X})$. A simple example of a channel of this form is the *identity channel* $\mathbb{1}_{\mathrm{L}(\mathcal{X})}$, which leaves each $X \in \mathrm{L}(\mathcal{X})$ unchanged. Intuitively speaking, this channel represents an ideal communication channel or a perfect component in a quantum computer memory, which causes no modification of the register it acts upon.

Along the same lines as states and measurements, tensor products of channels represent independently applied channels, collectively viewed as a single channel. More specifically, if $\mathsf{X}_1, \ldots, \mathsf{X}_n$ and $\mathsf{Y}_1, \ldots, \mathsf{Y}_n$ are registers, and

$$\begin{aligned} \Phi_1 &: \mathrm{L}(\mathcal{X}_1) \to \mathrm{L}(\mathcal{Y}_1) \\ &\vdots \\ \Phi_n &: \mathrm{L}(\mathcal{X}_n) \to \mathrm{L}(\mathcal{Y}_n) \end{aligned}$$

are channels, the channel

$$\Phi_1 \otimes \cdots \otimes \Phi_n : \mathrm{L}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n) \to \mathrm{L}(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n)$$

is said to be a *product channel*. It is the channel that represents the action of channels $\Phi_1, \ldots, \Phi_n$ being independently applied to $\mathsf{X}_1, \ldots, \mathsf{X}_n$.

Now let us return to the restrictions of trace preservation and complete positivity mentioned in the definition of channels. Obviously, if we wish to consider that the output $\Phi(\rho)$ of a given channel $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ is a valid state of Y for every possible state $\rho \in \mathrm{D}(\mathcal{X})$ of X, it must hold that Φ maps density operators to density operators. What is more, this must be so for tensor products of channels: it must hold that

$$(\Phi_1 \otimes \cdots \otimes \Phi_n)(\rho) \in \mathrm{D}(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n)$$

for every choice of $\rho \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$, given any choice of channels $\Phi_1, \ldots, \Phi_n$ transforming registers $\mathsf{X}_1, \ldots, \mathsf{X}_n$ into registers $\mathsf{Y}_1, \ldots, \mathsf{Y}_n$. In addition, we make the assumption that the identity channel $\mathbb{1}_{\mathrm{L}(\mathcal{Z})}$ is a valid channel for every register Z.

In particular, for every legitimate channel $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$, it must hold that $\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}$ is also a legitimate channel, for every choice of a register Z. Thus,

$$(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(\rho) \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{Z})$$

for every choice of $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Z})$. This is equivalent to the two conditions stated before: it must hold that Φ is *completely positive*, which means that $(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(P) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z})$ for every $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Z})$, and Φ must preserve trace: $\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X)$ for every $X \in \mathrm{L}(\mathcal{X})$.

Once we have imposed the condition of complete positivity on channels, it is not difficult to see that any tensor product $\Phi_1 \otimes \cdots \otimes \Phi_n$ of such channels will also map density operators to density operators. We may view tensor products like this as a composition of the channels $\Phi_1, \ldots, \Phi_n$ tensored with identity channels like this:

$$\Phi_1 \otimes \cdots \otimes \Phi_n = (\Phi_1 \otimes \mathbb{1}_{\mathcal{X}_2} \otimes \cdots \otimes \mathbb{1}_{\mathcal{X}_n}) \cdots (\mathbb{1}_{\mathcal{Y}_1} \otimes \cdots \otimes \mathbb{1}_{\mathcal{Y}_{n-1}} \otimes \Phi_n).$$

On the right hand side, we have a composition of tensor products of channels, defined in the usual way that one composes mappings. Each one of these tensor products of channels maps density operators to density operators, by the definitions of complete positivity and trace-preservation, and so the same thing is true of the product channel on the left hand side.

We will study the condition of complete positivity (as well as trace-preservation) in much greater detail in a couple of lectures.

3.2 Information complete measurements

In the remainder of this lecture we will discuss a couple of basic facts about states and measurements. The first fact is that states of registers are uniquely determined by the measurement statistics they generate. More precisely, if one knows the probability associated with every outcome of every measurement that could possibly be performed on a given register, then that registers state has been uniquely determined.

In fact, something stronger may be said: for any choice of a register X, there are choices of measurements on X that uniquely determine every possible state of X by the measurement statistics that they alone generate. Such measurements are called *information-complete* measurements. They are characterized by the property that their measurement operators span the space $\mathrm{L}(\mathcal{X})$.

Proposition 3.1. *Let $\mathcal{X}$ be a complex Euclidean space, and let*

$$\mu : \Gamma \to \mathrm{Pos}(\mathcal{X}) : a \mapsto P_a$$

be a measurement on $\mathcal{X}$ with the property that the collection $\{P_a : a \in \Gamma\}$ spans all of $\mathrm{L}(\mathcal{X})$. The mapping $\phi : \mathrm{L}(\mathcal{X}) \to \mathbb{C}^\Gamma$, defined by

$$(\phi(X))(a) = \langle P_a, X \rangle$$

for all $X \in \mathrm{L}(\mathcal{X})$ and $a \in \Gamma$, is one-to-one on $\mathrm{L}(\mathcal{X})$.

Remark 3.2. Of course the fact that ϕ is one-to-one on $\mathrm{L}(\mathcal{X})$ implies that it is one-to-one on $\mathrm{D}(\mathcal{X})$, which is all we really care about for the sake of this discussion. It is no harder to prove the proposition for all of $\mathrm{L}(\mathcal{X})$, however, so it is stated in the more general way.

Proof. It is clear that ϕ is linear, so we must only prove $\ker(\phi) = \{0\}$. Assume $\phi(X) = 0$, meaning that $(\phi(X))(a) = \langle P_a, X \rangle = 0$ for all $a \in \Gamma$, and write

$$X = \sum_{a \in \Gamma} \alpha_a P_a$$

for some choice of $\{\alpha_a : a \in \Gamma\} \subset \mathbb{C}$. This is possible because $\{P_a : a \in \Gamma\}$ spans $\mathrm{L}(\mathcal{X})$. It follows that

$$\|X\|_2^2 = \langle X, X \rangle = \sum_{a \in \Gamma} \overline{\alpha_a} \langle P_a, X \rangle = 0,$$

and therefore $X = 0$ by the positive definiteness of the Frobenius norm. This implies $\ker(\phi) = \{0\}$, as required. □

Let us now construct a simple example of an information-complete measurement, for any choice of a complex Euclidean space $\mathcal{X} = \mathbb{C}^\Sigma$. We will assume that the elements of Σ have been ordered in some fixed way. For each pair $(a, b) \in \Sigma \times \Sigma$, define an operator $Q_{a,b} \in \mathrm{L}(\mathcal{X})$ as follows:

$$Q_{a,b} = \begin{cases} E_{a,a} & \text{if } a = b \\ E_{a,a} + E_{a,b} + E_{b,a} + E_{b,b} & \text{if } a < b \\ E_{a,a} + iE_{a,b} - iE_{b,a} + E_{b,b} & \text{if } a > b. \end{cases}$$

Each operator $Q_{a,b}$ is positive semidefinite, and the set $\{Q_{a,b} : (a, b) \in \Sigma \times \Sigma\}$ spans the space $\mathrm{L}(\mathcal{X})$. With the exception of the trivial case $|\Sigma| = 1$, the operator

$$Q = \sum_{(a,b) \in \Sigma \times \Sigma} Q_{a,b}$$

differs from the identity operator, which means that $\{Q_{a,b} : (a,b) \in \Sigma \times \Sigma\}$ is not generally a measurement. The operator Q is, however, positive definite, and by defining

$$P_{a,b} = Q^{-1/2} Q_{a,b} Q^{-1/2}$$

we have that $\mu : \Sigma \times \Sigma \to \mathrm{Pos}(\mathcal{X}) : (a,b) \mapsto P_{a,b}$ is an information-complete measurement.

It also holds that every state of an n-tuple of registers $(\mathsf{X}_1, \ldots, \mathsf{X}_n)$ is uniquely determined by the measurement statistics of all product measurements on $(\mathsf{X}_1, \ldots, \mathsf{X}_n)$. This follows from the simple observation that for any choice of information-complete measurements

$$\begin{gathered} \mu_1 : \Gamma_1 \to \mathrm{Pos}(\mathcal{X}_1) \\ \vdots \\ \mu_n : \Gamma_n \to \mathrm{Pos}(\mathcal{X}_n) \end{gathered}$$

defined on $\mathsf{X}_1, \ldots, \mathsf{X}_n$, the product measurement given by

$$\mu(a_1, \ldots, a_n) = \mu_1(a_1) \otimes \cdots \otimes \mu_n(a_n)$$

is also necessarily information-complete.

3.3 Partial measurements

A natural notion concerning measurements is that of a *partial measurement*. This is the situation in which we have a collection of registers $(\mathsf{X}_1, \ldots, \mathsf{X}_n)$ in some state $\rho \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$, and we perform measurements on just a subset of these registers. These measurements will yield results as normal, but the remaining registers will continue to exist and have some state (which generally will depend on the particular measurement outcomes that resulted from the measurements).

For simplicity let us consider this situation for just a pair of registers (X, Y). Assume the pair has the state $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$, and a measurement $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$ is performed on X. Conditioned on the outcome $a \in \Gamma$ resulting from this measurement, the state of Y will become

$$\frac{\mathrm{Tr}_{\mathcal{X}}\left[(\mu(a) \otimes \mathbb{1}_{\mathcal{Y}})\rho\right]}{\langle \mu(a) \otimes \mathbb{1}_{\mathcal{Y}}, \rho \rangle}.$$

One way to see that this must indeed be the state of Y conditioned on the measurement outcome a is that it is the only state that is consistent with every possible measurement $\nu : \Sigma \to \mathrm{Pos}(\mathcal{Y})$ that could independently be performed on Y.

To explain this in greater detail, let us write $\mathsf{A} = a$ to denote the event that the original measurement μ on X results in the outcome $a \in \Gamma$, and let us write $\mathsf{B} = b$ to denote the event that the new, hypothetical measurement ν on Y results in the outcome $b \in \Sigma$. We have

$$\Pr[(\mathsf{A} = a) \wedge (\mathsf{B} = b)] = \langle \mu(a) \otimes \nu(b), \rho \rangle$$

and

$$\Pr[\mathsf{A} = a] = \langle \mu(a) \otimes \mathbb{1}_{\mathcal{Y}}, \rho \rangle,$$

so by the rule of conditional probabilities we have

$$\Pr[\mathsf{B} = b | \mathsf{A} = a] = \frac{\Pr[(\mathsf{A} = a) \wedge (\mathsf{B} = b)]}{\Pr[\mathsf{A} = a]} = \frac{\langle \mu(a) \otimes \nu(b), \rho \rangle}{\langle \mu(a) \otimes \mathbb{1}_{\mathcal{Y}}, \rho \rangle}.$$

Noting that

$$\langle X \otimes Y, \rho \rangle = \langle Y, \mathrm{Tr}_{\mathcal{X}} \left[(X^* \otimes \mathbb{1}_{\mathcal{Y}}) \rho \right] \rangle$$

for all X, Y, and ρ, we see that

$$\frac{\langle \mu(a) \otimes \nu(b), \rho \rangle}{\langle \mu(a) \otimes \mathbb{1}_{\mathcal{Y}}, \rho \rangle} = \langle \nu(b), \xi_a \rangle$$

for

$$\xi_a = \frac{\mathrm{Tr}_{\mathcal{X}} \left[(\mu(a) \otimes \mathbb{1}_{\mathcal{Y}}) \rho \right]}{\langle \mu(a) \otimes \mathbb{1}_{\mathcal{Y}}, \rho \rangle}.$$

As states are uniquely determined by their measurement statistics, as we have just discussed, we see that $\xi_a \in \mathrm{D}(\mathcal{Y})$ must indeed be the state of Y, conditioned on the measurement μ having resulted in outcome $a \in \Gamma$. (Of course ξ_a is not well-defined when $\Pr[\mathsf{A} = a] = 0$, but we do not need to worry about conditioning on an event that will never happen.)

3.4 Observable differences between states

A natural way to measure the distance between probability vectors $p, q \in \mathbb{R}^{\Gamma}$ is by the 1-norm:

$$\| p - q \|_1 = \sum_{a \in \Gamma} | p(a) - q(a) | .$$

It is easily verified that

$$\| p - q \|_1 = 2 \max_{\Delta \subseteq \Gamma} \left(\sum_{a \in \Delta} p(a) - \sum_{a \in \Delta} q(a) \right).$$

This is a natural measure of distance because it quantifies the optimal probability that two known probability vectors can be distinguished, given a single sample from the distributions they specify.

As an example, let us consider a thought experiment involving two hypothetical people: Alice and Bob. Two probability vectors $p_0, p_1 \in \mathbb{R}^{\Gamma}$ are fixed, and are considered to be known to both Alice and Bob. Alice privately chooses a random bit $a \in \{0, 1\}$, uniformly at random, and uses the value a to randomly choose an element $b \in \Gamma$: if $a = 0$, she samples b according to p_0, and if $a = 1$, she samples b according to p_1. The sampled element $b \in \Gamma$ is given to Bob, whose goal is to identify the value of Alice's random bit a. Bob may only use the value of b, along with his knowledge of p_0 and p_1, when making his guess.

It is clear from Bayes' theorem what Bob should do to maximize his probability to correctly guess the value of a: if $p_0(b) > p_1(b)$, he should guess that $a = 0$, while if $p_0(b) < p_1(b)$ he should guess that $a = 1$. In case $p_0(b) = p_1(b)$, Bob may as well guess that $a = 0$ or $a = 1$ arbitrarily, for he has learned nothing at all about the value of a from such an element $b \in \Gamma$. Bob's probability to correctly identify the value of a using this strategy is

$$\frac{1}{2} + \frac{1}{4} \| p_0 - p_1 \|_1 ,$$

which can be verified by a simple calculation. This is an optimal strategy.

A slightly more general situation is one in which $a \in \{0, 1\}$ is not chosen uniformly, but rather

$$\Pr[a = 0] = \lambda \qquad \text{and} \qquad \Pr[a = 1] = 1 - \lambda$$

for some value of $\lambda \in [0,1]$. In this case, an optimal strategy for Bob is to guess that $a = 0$ if $\lambda p_0(b) > (1-\lambda)p_1(b)$, to guess that $a = 1$ if $\lambda p_0(b) < (1-\lambda)p_1(b)$, and to guess arbitrarily if $\lambda p_0(b) = (1-\lambda)p_1(b)$. His probability of correctness will be

$$\frac{1}{2} + \frac{1}{2} \left\| \lambda p_0 - (1-\lambda) p_1 \right\|.$$

Naturally, this generalizes the expression for the case $\lambda = 1/2$.

Now consider a similar scenario, except with quantum states $\rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})$ in place of probability vectors $p_0, p_1 \in \mathbb{R}^\Gamma$. More specifically, Alice chooses a random bit $a = \{0,1\}$ according to the distribution

$$\Pr[a = 0] = \lambda \qquad \text{and} \qquad \Pr[a = 1] = 1 - \lambda,$$

for some choice of $\lambda \in [0,1]$ (which is known to both Alice and Bob). She then hands Bob a register X that has been prepared in the quantum state $\rho_a \in \mathrm{D}(\mathcal{X})$. This time, Bob has the freedom to choose whatever measurement he wants in trying to guess the value of a.

Note that there is no generality lost in assuming Bob makes a measurement having outcomes 0 and 1. If he were to make any other measurement, perhaps with many outcomes, and then process the outcome in some way to arrive at a guess for the value of a, we could simply combine his measurement with the post-processing phase to arrive at the description of a measurement with outcomes 0 and 1.

The following theorem states, in mathematical terms, that Bob's optimal strategy correctly identifies a with probability

$$\frac{1}{2} + \frac{1}{2} \left\| \lambda \rho_0 - (1-\lambda) \rho_1 \right\|_1,$$

which is a similar expression to the one we had in the classical case. The proof of the theorem also makes clear precisely what strategy Bob should employ for optimality.

Theorem 3.3 (Helstrom)**.** *Let $\rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})$ be states and let $\lambda \in [0,1]$. For every choice of positive semidefinite operators $P_0, P_1 \in \mathrm{Pos}(\mathcal{X})$ for which $P_0 + P_1 = \mathbb{1}_\mathcal{X}$, it holds that*

$$\lambda \langle P_0, \rho_0 \rangle + (1-\lambda) \langle P_1, \rho_1 \rangle \leq \frac{1}{2} + \frac{1}{2} \left\| \lambda \rho_0 - (1-\lambda) \rho_1 \right\|_1.$$

Moreover, equality is achieved for some choice of projection operators $P_0, P_1 \in \mathrm{Pos}(\mathcal{X})$ with $P_0 + P_1 = \mathbb{1}_\mathcal{X}$.

Proof. First, note that

$$\begin{aligned}
&(\lambda \langle P_0, \rho_0 \rangle + (1-\lambda) \langle P_1, \rho_1 \rangle) - (\lambda \langle P_1, \rho_0 \rangle + (1-\lambda) \langle P_0, \rho_1 \rangle) = \langle P_0 - P_1, \lambda \rho_0 - (1-\lambda) \rho_1 \rangle \\
&(\lambda \langle P_0, \rho_0 \rangle + (1-\lambda) \langle P_1, \rho_1 \rangle) + (\lambda \langle P_1, \rho_0 \rangle + (1-\lambda) \langle P_0, \rho_1 \rangle) = 1,
\end{aligned}$$

and therefore

$$\lambda \langle P_0, \rho_0 \rangle + (1-\lambda) \langle P_1, \rho_1 \rangle = \frac{1}{2} + \frac{1}{2} \langle P_0 - P_1, \lambda \rho_0 - (1-\lambda) \rho_1 \rangle, \tag{3.1}$$

for any choice of $P_0, P_1 \in \mathrm{Pos}(\mathcal{X})$ with $P_0 + P_1 = \mathbb{1}_\mathcal{X}$.

Now, for every unit vector $u \in \mathcal{X}$ we have

$$|u^*(P_0 - P_1)u| = |u^* P_0 u - u^* P_1 u| \leq u^* P_0 u + u^* P_1 u = u^*(P_0 + P_1)u = 1,$$

and therefore (as $P_0 - P_1$ is Hermitian) it holds that $\|P_0 - P_1\| \leq 1$. By Hölder's inequality (for Schatten p-norms) we therefore have

$$\langle P_0 - P_1, \lambda\rho_0 - (1-\lambda)\rho_1 \rangle \leq \|P_0 - P_1\| \, \|\lambda\rho_0 - (1-\lambda)\rho_1\|_1 \leq \|\lambda\rho_0 - (1-\lambda)\rho_1\|_1 ,$$

and so the inequality in the theorem follows from (3.1).

To prove equality can be achieved for projection operators $P_0, P_1 \in \mathrm{Pos}(\mathcal{X})$ with $P_0 + P_1 = \mathbb{1}_{\mathcal{X}}$, we consider a spectral decomposition

$$\lambda\rho_0 - (1-\lambda)\rho_1 = \sum_{j=1}^{n} \eta_j x_j x_j^* .$$

Defining

$$P_0 = \sum_{j:\, \eta_j \geq 0} x_j x_j^* \qquad \text{and} \qquad P_1 = \sum_{j:\, \eta_j < 0} x_j x_j^* ,$$

we have that P_0 and P_1 are projections with $P_0 + P_1 = \mathbb{1}_{\mathcal{X}}$, and moreover

$$(P_0 - P_1)(\lambda\rho_0 - (1-\lambda)\rho_1) = \sum_{j=1}^{n} \big|\eta_j\big| \, x_j x_j^* .$$

It follows that

$$\langle P_0 - P_1, \lambda\rho_0 - (1-\lambda)\rho_1 \rangle = \sum_{j=1}^{n} \big|\eta_j\big| = \|\lambda\rho_0 - (1-\lambda)\rho_1\|_1 ,$$

and by (3.1) we obtain the desired equality. □

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

Lecture 4: Purifications and fidelity

Throughout this lecture we will be discussing pairs of registers of the form (X, Y), and the relationships among the states of X, Y, and (X, Y).

The situation generalizes to collections of three or more registers, provided we are interested in bipartitions. For instance, if we have a collection of registers $(\mathsf{X}_1, \ldots, \mathsf{X}_n)$, and we wish to consider the state of a subset of these registers in relation to the state of the whole, we can effectively group the registers into two disjoint collections and relabel them as X and Y to apply the conclusions to be drawn. Other, multipartite relationships can become more complicated, such as relationships between states of $(\mathsf{X}_1, \mathsf{X}_2)$, $(\mathsf{X}_2, \mathsf{X}_3)$, and $(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$, but this is not the topic of this lecture.

4.1 Reductions, extensions, and purifications

Suppose that a pair of registers (X, Y) has the state $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$. The states of X and Y individually are then given by

$$\rho^{\mathsf{X}} = \mathrm{Tr}_{\mathcal{Y}}(\rho) \qquad \text{and} \qquad \rho^{\mathsf{Y}} = \mathrm{Tr}_{\mathcal{X}}(\rho).$$

You could regard this as a definition, but these are the only choices that are consistent with the interpretation that disregarding Y should have no influence on the outcomes of any measurements performed on X alone, and likewise for X and Y reversed. The states ρ^{X} and ρ^{Y} are sometimes called the *reduced states* of X and Y, or the *reductions* of ρ to X and Y.

We may also go in the other direction. If a state $\sigma \in \mathrm{D}(\mathcal{X})$ of X is given, we may consider the possible states $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ that are consistent with σ on X, meaning that $\sigma = \mathrm{Tr}_{\mathcal{Y}}(\rho)$. Unless Y is a trivial register with just a single classical state, there are always multiple choices for ρ that are consistent with σ. Any such state ρ is said to be an *extension* of σ. For instance, $\rho = \sigma \otimes \xi$, for any density operator $\xi \in \mathrm{D}(\mathcal{Y})$, is always an extension of σ, because

$$\mathrm{Tr}_{\mathcal{Y}}(\sigma \otimes \xi) = \sigma \otimes \mathrm{Tr}(\xi) = \sigma.$$

If σ is pure, this is the only possible form for an extension. This is a mathematically simple statement, but it is nevertheless important at an intuitive level: it says that a register in a pure state cannot be correlated with any other registers.

A special type of extension is one in which the state of (X, Y) is pure: if $\rho = uu^* \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ is a pure state for which

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = \sigma,$$

it is said that ρ is a *purification* of σ. One also often refers to the vector u, as opposed to the operator uu^*, as being a purification of σ.

The notions of reductions, extensions, and purifications are easily extended to arbitrary positive semidefinite operators, as opposed to just density operators. For instance, if $P \in \mathrm{Pos}(\mathcal{X})$ is

a positive semidefinite operator and $u \in \mathcal{X} \otimes \mathcal{Y}$ is a vector for which

$$P = \mathrm{Tr}_{\mathcal{Y}}(uu^*),$$

it is said that u (or uu^*) is a purification of P.

For example suppose $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} = \mathbb{C}^{\Sigma}$, for some arbitrary (finite and nonempty) set Σ. The vector

$$u = \sum_{a \in \Sigma} e_a \otimes e_a$$

satisfies the equality

$$\mathbb{1}_{\mathcal{X}} = \mathrm{Tr}_{\mathcal{Y}}(uu^*),$$

and so u is a purification of $\mathbb{1}_{\mathcal{X}}$.

4.2 Existence and properties of purifications

A study of the properties of purifications is greatly simplified by the following observation. The vec mapping defined in Lecture 2 is a one-to-one and onto linear correspondence between $\mathcal{X} \otimes \mathcal{Y}$ and $\mathrm{L}(\mathcal{Y}, \mathcal{X})$; and for any choice of $u \in \mathcal{X} \otimes \mathcal{Y}$ and $A \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ satisfying $u = \mathrm{vec}(A)$ it holds that

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = \mathrm{Tr}_{\mathcal{Y}}(\mathrm{vec}(A)\,\mathrm{vec}(A)^*) = AA^*.$$

Therefore, for every choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, and for any given operator $P \in \mathrm{Pos}(\mathcal{X})$, the following two properties are equivalent:

1. There exists a purification $u \in \mathcal{X} \otimes \mathcal{Y}$ of P.
2. There exists an operator $A \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ such that $P = AA^*$.

The following theorem, whose proof is based on this observation, establishes necessary and sufficient conditions for the existence of a purification of a given operator.

Theorem 4.1. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, and let $P \in \mathrm{Pos}(\mathcal{X})$ be a positive semidefinite operator. There exists a purification $u \in \mathcal{X} \otimes \mathcal{Y}$ of P if and only if* $\dim(\mathcal{Y}) \geq \mathrm{rank}(P)$.

Proof. As discussed above, the existence of a purification $u \in \mathcal{X} \otimes \mathcal{Y}$ of P is equivalent to the existence of an operator $A \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ satisfying $P = AA^*$. Under the assumption that such an operator A exists, it is clear that

$$\mathrm{rank}(P) = \mathrm{rank}(AA^*) = \mathrm{rank}(A) \leq \dim(\mathcal{Y})$$

as claimed.

Conversely, under the assumption that $\dim(\mathcal{Y}) \geq \mathrm{rank}(P)$, there must exist operator $B \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ for which $BB^* = \Pi_{\mathrm{im}(P)}$ (the projection onto the image of P). To obtain such an operator B, let $r = \mathrm{rank}(P)$, use the spectral theorem to write

$$P = \sum_{j=1}^{r} \lambda_j(P) x_j x_j^*,$$

and let

$$B = \sum_{j=1}^{r} x_j y_j^*$$

for any choice of an orthonormal set $\{y_1, \ldots, y_r\} \subset \mathcal{Y}$. Now, for $A = \sqrt{P}B$ it holds that $AA^* = P$ as required. □

Corollary 4.2. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces such that* $\dim(\mathcal{Y}) \geq \dim(\mathcal{X})$. *For every choice of $P \in \mathrm{Pos}(\mathcal{X})$, there exists a purification $u \in \mathcal{X} \otimes \mathcal{Y}$ of P.*

Having established a simple condition under which purifications exist, the next step is to prove the following important relationship among all purifications of a given operator within a given space.

Theorem 4.3 (Unitary equivalence of purifications)**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, and suppose that vectors $u, v \in \mathcal{X} \otimes \mathcal{Y}$ satisfy*

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = \mathrm{Tr}_{\mathcal{Y}}(vv^*).$$

There exists a unitary operator $U \in \mathrm{U}(\mathcal{Y})$ such that $v = (\mathbb{1}_{\mathcal{X}} \otimes U)u$.

Proof. Let $P \in \mathrm{Pos}(\mathcal{X})$ satisfy $\mathrm{Tr}_{\mathcal{Y}}(uu^*) = P = \mathrm{Tr}_{\mathcal{Y}}(vv^*)$, and let $A, B \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ be the unique operators satisfying $u = \mathrm{vec}(A)$ and $v = \mathrm{vec}(B)$. It therefore holds that $AA^* = P = BB^*$. Letting $r = \mathrm{rank}(P)$, it follows that $\mathrm{rank}(A) = r = \mathrm{rank}(B)$.

Now, let $\{x_1, \ldots, x_r\} \subset \mathcal{X}$ be any orthonormal collection of eigenvectors of P with corresponding eigenvalues $\lambda_1(P), \ldots, \lambda_r(P)$. By the singular value theorem, it is possible to write

$$A = \sum_{j=1}^{r} \sqrt{\lambda_j(P)}\, x_j y_j^* \qquad \text{and} \qquad B = \sum_{j=1}^{r} \sqrt{\lambda_j(P)}\, x_j z_j^*$$

for some choice of orthonormal sets $\{y_1, \ldots, y_r\}$ and $\{z_1, \ldots, z_r\}$.

Finally, let $V \in \mathrm{U}(\mathcal{Y})$ be any unitary operator satisfying $Vz_j = y_j$ for every $j = 1, \ldots, r$. It follows that $AV = B$, and by taking $U = V^{\mathsf{T}}$ one has

$$(\mathbb{1}_{\mathcal{X}} \otimes U)u = (\mathbb{1}_{\mathcal{X}} \otimes V^{\mathsf{T}})\,\mathrm{vec}(A) = \mathrm{vec}(AV) = \mathrm{vec}(B) = v$$

as required. □

Theorem 4.3 will have significant value throughout the course, as a tool for proving a variety of results. It is also important at an intuitive level that the following example aims to illustrate.

Example 4.4. Suppose X and Y are distinct registers, and that Alice holds X and Bob holds Y in separate locations. Assume moreover that the pair (X, Y) is in a pure state uu^*.

Now imagine that Bob wishes to transform the state of (X, Y) so that it is in a different pure state vv^*. Assuming that Bob is able to do this without any interaction with Alice, it must hold that

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = \mathrm{Tr}_{\mathcal{Y}}(vv^*). \tag{4.1}$$

This equation expresses the assumption that Bob does not touch X.

Theorem 4.3 implies that not only is (4.1) a necessary condition for Bob to transform uu^* into vv^*, but in fact it is sufficient. In particular, there must exist a unitary operator $U \in \mathrm{U}(\mathcal{Y})$ for which $v = (\mathbb{1}_{\mathcal{X}} \otimes U)u$, and Bob can implement the transformation from uu^* into vv^* by applying the unitary operation described by U to his register Y.

4.3 The fidelity function

There are different ways that one may quantify the similarity or difference between density operators. One way that relates closely to the notion of purifications is the *fidelity* between states. It is used extensively in the theory of quantum information.

4.3.1 Definition of the fidelity function

Given positive semidefinite operators $P, Q \in \mathrm{Pos}(\mathcal{X})$, we define the fidelity between P and Q as

$$\mathrm{F}(P, Q) = \left\| \sqrt{P}\sqrt{Q} \right\|_1.$$

Equivalently,

$$\mathrm{F}(P, Q) = \mathrm{Tr}\sqrt{\sqrt{P}Q\sqrt{P}}.$$

Similar to purifications, it is common to see the fidelity defined only for density operators as opposed to arbitrary positive semidefinite operators. It is, however, useful to extend the definition to all positive semidefinite operators as we have done, and it incurs little or no additional effort.

4.3.2 Basic properties of the fidelity

There are many interesting properties of the fidelity function. Let us begin with a few simple ones. First, the fidelity is symmetric: $\mathrm{F}(P, Q) = \mathrm{F}(Q, P)$ for all $P, Q \in \mathrm{Pos}(\mathcal{X})$. This is clear from the definition, given that $\|A\|_1 = \|A^*\|_1$ for all operators A.

Next, suppose that $u \in \mathcal{X}$ is a vector and $Q \in \mathrm{Pos}(\mathcal{X})$ is a positive semidefinite operator. It follows from the observation that $\sqrt{uu^*} = \frac{uu^*}{\|u\|}$ whenever $u \neq 0$ that

$$\mathrm{F}(uu^*, Q) = \sqrt{u^*Qu}.$$

In particular, $\mathrm{F}(uu^*, vv^*) = |\langle u, v\rangle|$ for any choice of vectors $u, v \in \mathcal{X}$.

One nice property of the fidelity that we will utilize several times is that it is multiplicative with respect to tensor products. This fact is stated in the following proposition (which can be easily extended from tensor products of two operators to any finite number of operators by induction).

Proposition 4.5. *Let $P_1, Q_1 \in \mathrm{Pos}(\mathcal{X}_1)$ and $P_2, Q_2 \in \mathrm{Pos}(\mathcal{X}_2)$ be positive semidefinite operators. It holds that*

$$\mathrm{F}(P_1 \otimes P_2, Q_1 \otimes Q_2) = \mathrm{F}(P_1, Q_1)\,\mathrm{F}(P_2, Q_2).$$

Proof. We have

$$\begin{aligned}\mathrm{F}(P_1 \otimes P_2, Q_1 \otimes Q_2) &= \left\| \sqrt{P_1 \otimes P_2}\sqrt{Q_1 \otimes Q_2} \right\|_1 = \left\| \left(\sqrt{P_1} \otimes \sqrt{P_2}\right)\left(\sqrt{Q_1} \otimes \sqrt{Q_2}\right) \right\|_1 \\ &= \left\| \sqrt{P_1}\sqrt{Q_1} \otimes \sqrt{P_2}\sqrt{Q_2} \right\|_1 = \left\| \sqrt{P_1}\sqrt{Q_1} \right\|_1 \left\| \sqrt{P_2}\sqrt{Q_2} \right\|_1 = \mathrm{F}(P_1, Q_1)\,\mathrm{F}(P_2, Q_2)\end{aligned}$$

as claimed. □

4.3.3 Uhlmann's theorem

Next we will prove a fundamentally important theorem about the fidelity, known as Uhlmann's theorem, which relates the fidelity to the notion of purifications.

Theorem 4.6 (Uhlmann's theorem)**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $P, Q \in \mathrm{Pos}(\mathcal{X})$ be positive semidefinite operators, both having rank at most $\dim(\mathcal{Y})$, and let $u \in \mathcal{X} \otimes \mathcal{Y}$ be any purification of P. It holds that*

$$\mathrm{F}(P, Q) = \max\left\{ |\langle u, v\rangle| \,:\, v \in \mathcal{X} \otimes \mathcal{Y},\ \mathrm{Tr}_{\mathcal{Y}}(vv^*) = Q \right\}.$$

Proof. Given that the rank of both P and Q is at most $\dim(\mathcal{Y})$, there must exist operators $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ for which $A^*A = \Pi_{\mathrm{im}(P)}$ and $B^*B = \Pi_{\mathrm{im}(Q)}$. The equations

$$\mathrm{Tr}_{\mathcal{Y}}\left(\mathrm{vec}\left(\sqrt{P}A^*\right)\mathrm{vec}\left(\sqrt{P}A^*\right)^*\right) = \sqrt{P}A^*A\sqrt{P} = P$$
$$\mathrm{Tr}_{\mathcal{Y}}\left(\mathrm{vec}\left(\sqrt{Q}B^*\right)\mathrm{vec}\left(\sqrt{Q}B^*\right)^*\right) = \sqrt{Q}B^*B\sqrt{Q} = Q$$

follow, demonstrating that

$$\mathrm{vec}\left(\sqrt{P}A^*\right) \quad \text{and} \quad \mathrm{vec}\left(\sqrt{Q}B^*\right)$$

are purifications of P and Q, respectively. By Theorem 4.3 it follows that every choice of a purification $u \in \mathcal{X} \otimes \mathcal{Y}$ of P must take the form

$$u = (\mathbb{1}_{\mathcal{X}} \otimes U)\,\mathrm{vec}\left(\sqrt{P}A^*\right) = \mathrm{vec}\left(\sqrt{P}A^*U^{\mathsf{T}}\right),$$

for some unitary operator $U \in \mathrm{U}(\mathcal{Y})$, and likewise every purification $v \in \mathcal{X} \otimes \mathcal{Y}$ of Q must take the form

$$v = (\mathbb{1}_{\mathcal{X}} \otimes V)\,\mathrm{vec}\left(\sqrt{Q}B^*\right) = \mathrm{vec}\left(\sqrt{Q}B^*V^{\mathsf{T}}\right)$$

for some unitary operator $V \in \mathrm{U}(\mathcal{Y})$.

The maximization in the statement of the theorem is therefore equivalent to

$$\max_{V \in \mathrm{U}(\mathcal{Y})} \left|\left\langle \mathrm{vec}\left(\sqrt{P}A^*U^{\mathsf{T}}\right), \mathrm{vec}\left(\sqrt{Q}B^*V^{\mathsf{T}}\right)\right\rangle\right|,$$

which may alternately be written as

$$\max_{V \in \mathrm{U}(\mathcal{Y})} \left|\left\langle U^{\mathsf{T}}\overline{V}, A\sqrt{P}\sqrt{Q}B^*\right\rangle\right| \tag{4.2}$$

for some choice of $U \in \mathrm{U}(\mathcal{Y})$. As $V \in \mathrm{U}(\mathcal{Y})$ ranges over all unitary operators, so too does $U^{\mathsf{T}}\overline{V}$, and therefore the quantity represented by equation (4.2) is given by

$$\left\| A\sqrt{P}\sqrt{Q}B^* \right\|_1.$$

Finally, given that A^*A and B^*B are projection operators, A and B must both have spectral norm at most 1. It therefore holds that

$$\left\| \sqrt{P}\sqrt{Q} \right\|_1 = \left\| A^*A\sqrt{P}\sqrt{Q}B^*B \right\|_1 \leq \left\| A\sqrt{P}\sqrt{Q}B^* \right\|_1 \leq \left\| \sqrt{P}\sqrt{Q} \right\|_1$$

so that

$$\left\| A\sqrt{P}\sqrt{Q}B^* \right\|_1 = \left\| \sqrt{P}\sqrt{Q} \right\|_1 = \mathrm{F}(P, Q).$$

The equality in the statement of the theorem therefore holds. □

Various properties of the fidelity follow from Uhlmann's theorem. For example, it is clear from the theorem that $0 \leq \mathrm{F}(\rho, \xi) \leq 1$ for density operators ρ and ξ. Moreover $\mathrm{F}(\rho, \xi) = 1$ if and only if $\rho = \xi$. It is also evident (from the definition) that $\mathrm{F}(\rho, \xi) = 0$ if and only if $\sqrt{\rho}\sqrt{\xi} = 0$, which is equivalent to $\rho\xi = 0$ (i.e., to ρ and ξ having orthogonal images).

Another property of the fidelity that follows from Uhlmann's theorem is as follows.

Proposition 4.7. *Let $P_1, \ldots, P_k, Q_1, \ldots, Q_k \in \mathrm{Pos}(\mathcal{X})$ be positive semidefinite operators. It holds that*

$$\mathrm{F}\left(\sum_{i=1}^{k} P_i, \sum_{i=1}^{k} Q_i\right) \geq \sum_{i=1}^{k} \mathrm{F}\left(P_i, Q_i\right).$$

Proof. Let $\mathcal{Y}$ be a complex Euclidean space having dimension at least that of $\mathcal{X}$, and choose vectors $u_1, \ldots, u_k, v_1, \ldots, v_k \in \mathcal{X} \otimes \mathcal{Y}$ satisfying $\mathrm{Tr}_{\mathcal{Y}}\left(u_i u_i^*\right) = P_i$, $\mathrm{Tr}_{\mathcal{Y}}\left(v_i v_i^*\right) = Q_i$, and $\langle u_i, v_i \rangle = \mathrm{F}(P_i, Q_i)$ for each $i = 1, \ldots, k$. Such vectors exist by Uhlmann's theorem. Let $\mathcal{Z} = \mathbb{C}^k$ and define $u, v \in \mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z}$ as

$$u = \sum_{i=1}^{k} u_i \otimes e_i \qquad \text{and} \qquad v = \sum_{i=1}^{k} v_i \otimes e_i.$$

We have

$$\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}\left(uu^*\right) = \sum_{i=1}^{k} P_i \qquad \text{and} \qquad \mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}\left(vv^*\right) = \sum_{i=1}^{k} Q_i.$$

Thus, again using Uhlmann's theorem, we have

$$\mathrm{F}\left(\sum_{i=1}^{k} P_i, \sum_{i=1}^{k} Q_i\right) \geq \left|\langle u, v \rangle\right| = \sum_{i=1}^{k} \mathrm{F}\left(P_i, Q_i\right)$$

as required. □

It follows from this proposition is that the fidelity function is *concave* in the first argument:

$$\mathrm{F}(\lambda\rho_1 + (1-\lambda)\rho_2, \xi) \geq \lambda\, \mathrm{F}(\rho_1, \xi) + (1-\lambda)\, \mathrm{F}(\rho_2, \xi)$$

for all $\rho_1, \rho_2, \xi \in \mathrm{D}(\mathcal{X})$ and $\lambda \in [0,1]$, and by symmetry it is concave in the second argument as well. In fact, the fidelity is *jointly concave*:

$$\mathrm{F}(\lambda\rho_1 + (1-\lambda)\rho_2, \lambda\xi_1 + (1-\lambda)\xi_2) \geq \lambda\, \mathrm{F}(\rho_1, \xi_1) + (1-\lambda)\, \mathrm{F}(\rho_2, \xi_2).$$

for all $\rho_1, \rho_2, \xi_1, \xi_2 \in \mathrm{D}(\mathcal{X})$ and $\lambda \in [0,1]$.

4.3.4 Alberti's theorem

A different characterization of the fidelity function is given by Alberti's theorem, which is as follows.

Theorem 4.8 (Alberti)**.** *Let $\mathcal{X}$ be a complex Euclidean space and let $P, Q \in \mathrm{Pos}(\mathcal{X})$ be positive semidefinite operators. It holds that*

$$\left(\mathrm{F}(P, Q)\right)^2 = \inf_{R \in \mathrm{Pd}(\mathcal{X})} \langle R, P \rangle \, \langle R^{-1}, Q \rangle.$$

When we study semidefinite programming later in the course, we will see that this theorem is in fact closely related to Uhlmann's theorem through semidefinite programming duality. For now we will make due with a different proof. It is more complicated, but it has the value that it illustrates some useful tricks from matrix analysis. To prove the theorem, it is helpful to start first with the special case that $P = Q$, which is represented by the following lemma.

Lemma 4.9. *Let $P \in \mathrm{Pos}(\mathcal{X})$. It holds that*

$$\inf_{R \in \mathrm{Pd}(\mathcal{X})} \langle R, P \rangle \langle R^{-1}, P \rangle = (\mathrm{Tr}(P))^2.$$

Proof. It is clear that

$$\inf_{R \in \mathrm{Pd}(\mathcal{X})} \langle R, P \rangle \langle R^{-1}, P \rangle \leq (\mathrm{Tr}(P))^2,$$

given that $R = \mathbb{1}$ is positive definite. To establish the reverse inequality, it suffices to prove that

$$\langle R, P \rangle \langle R^{-1}, P \rangle \geq (\mathrm{Tr}(P))^2$$

for any choice of $R \in \mathrm{Pd}(\mathcal{X})$. This will follow from the simple observation that, for any choice of positive real numbers α and β, we have $\alpha^2 + \beta^2 \geq 2\alpha\beta$ and therefore $\alpha\beta^{-1} + \beta\alpha^{-1} \geq 2$. With this fact in mind, consider a spectral decomposition

$$R = \sum_{i=1}^{n} \lambda_i u_i u_i^*.$$

We have

$$\begin{aligned}
\langle R, P \rangle \langle R^{-1}, P \rangle &= \sum_{1 \leq i,j \leq n} \lambda_i \lambda_j^{-1} (u_i^* P u_i)(u_j^* P u_j) \\
&= \sum_{1 \leq i \leq n} (u_i^* P u_i)^2 + \sum_{1 \leq i < j \leq n} (\lambda_i \lambda_j^{-1} + \lambda_j \lambda_i^{-1})(u_i^* P u_i)(u_j^* P u_j) \\
&\geq \sum_{1 \leq i \leq n} (u_i^* P u_i)^2 + 2 \sum_{1 \leq i < j \leq n} (u_i^* P u_i)(u_j^* P u_j) \\
&= (\mathrm{Tr}(P))^2
\end{aligned}$$

as required. □

Proof of Theorem 4.8. We will first prove the theorem for P and Q positive definite. Let us define $S \in \mathrm{Pd}(\mathcal{X})$ to be

$$S = \left(\sqrt{P}Q\sqrt{P}\right)^{-1/4} \sqrt{P}R\sqrt{P} \left(\sqrt{P}Q\sqrt{P}\right)^{-1/4}.$$

Notice that as R ranges over all positive definite operators, so too does S. We have

$$\begin{aligned}
\left\langle S, \left(\sqrt{P}Q\sqrt{P}\right)^{1/2} \right\rangle &= \langle R, P \rangle, \\
\left\langle S^{-1}, \left(\sqrt{P}Q\sqrt{P}\right)^{1/2} \right\rangle &= \langle R^{-1}, Q \rangle.
\end{aligned}$$

Therefore, by Lemma 4.9, we have

$$\begin{aligned}
\inf_{R \in \mathrm{Pd}(\mathcal{X})} \langle R, P \rangle \langle R^{-1}, Q \rangle &= \inf_{S \in \mathrm{Pd}(\mathcal{X})} \left\langle S, \left(\sqrt{P}Q\sqrt{P}\right)^{1/2} \right\rangle \left\langle S^{-1}, \left(\sqrt{P}Q\sqrt{P}\right)^{1/2} \right\rangle \\
&= \left(\mathrm{Tr}\sqrt{\sqrt{P}Q\sqrt{P}}\right)^2 \\
&= (\mathrm{F}(P, Q))^2.
\end{aligned}$$

To prove the general case, let us first note that, for any choice of $R \in \mathrm{Pd}(\mathcal{X})$ and $\varepsilon > 0$, we have

$$\langle R, P \rangle \langle R^{-1}, Q \rangle \leq \langle R, P + \varepsilon \mathbb{1} \rangle \langle R^{-1}, Q + \varepsilon \mathbb{1} \rangle.$$

Thus,

$$\inf_{R \in \mathrm{Pd}(\mathcal{X})} \langle R, P \rangle \langle R^{-1}, Q \rangle \leq \left(\mathrm{F}(P + \varepsilon \mathbb{1}, Q + \varepsilon \mathbb{1})\right)^2$$

for all $\varepsilon > 0$. As

$$\lim_{\varepsilon \to 0^+} \mathrm{F}(P + \varepsilon \mathbb{1}, Q + \varepsilon \mathbb{1}) = \mathrm{F}(P, Q)$$

we have

$$\inf_{R \in \mathrm{Pd}(\mathcal{X})} \langle R, P \rangle \langle R^{-1}, Q \rangle \leq \left(\mathrm{F}(P, Q)\right)^2.$$

On the other hand, for any choice of $R \in \mathrm{Pd}(\mathcal{X})$ we have

$$\langle R, P + \varepsilon \mathbb{1} \rangle \langle R^{-1}, Q + \varepsilon \mathbb{1} \rangle \geq \left(\mathrm{F}(P + \varepsilon \mathbb{1}, Q + \varepsilon \mathbb{1})\right)^2 \geq \left(\mathrm{F}(P, Q)\right)^2$$

for all $\varepsilon > 0$, and therefore

$$\langle R, P \rangle \langle R^{-1}, Q \rangle \geq \left(\mathrm{F}(P, Q)\right)^2.$$

As this holds for all $R \in \mathrm{Pd}(\mathcal{X})$ we have

$$\inf_{R \in \mathrm{Pd}(\mathcal{X})} \langle R, P \rangle \langle R^{-1}, Q \rangle \geq \left(\mathrm{F}(P, Q)\right)^2,$$

which completes the proof. □

4.4 The Fuchs–van de Graaf inequalities

We will now state and prove the Fuchs–van de Graaf inequalities, which establish a close relationship between the trace norm of the difference between two density operators and their fidelity. The inequalities are as stated in the following theorem.

Theorem 4.10 (Fuchs–van de Graaf)**.** *Let $\mathcal{X}$ be a complex Euclidean space and assume that $\rho, \xi \in \mathrm{D}(\mathcal{X})$ are density operators on $\mathcal{X}$. It holds that*

$$1 - \frac{1}{2} \|\rho - \xi\|_1 \leq \mathrm{F}(\rho, \xi) \leq \sqrt{1 - \frac{1}{4} \|\rho - \xi\|_1^2}.$$

To prove this theorem we first need the following lemma relating the trace norm and Frobenius norm. Once we have it in hand, the theorem will be easy to prove.

Lemma 4.11. *Let $\mathcal{X}$ be a complex Euclidean space and let $P, Q \in \mathrm{Pos}(\mathcal{X})$ be positive semidefinite operators on $\mathcal{X}$. It holds that*

$$\|P - Q\|_1 \geq \left\| \sqrt{P} - \sqrt{Q} \right\|_2^2.$$

Proof. Let

$$\sqrt{P} - \sqrt{Q} = \sum_{i=1}^{n} \lambda_i u_i u_i^*$$

be a spectral decomposition of $\sqrt{P} - \sqrt{Q}$. Given that $\sqrt{P} - \sqrt{Q}$ is Hermitian, it follows that

$$\sum_{i=1}^{n} |\lambda_i|^2 = \left\| \sqrt{P} - \sqrt{Q} \right\|_2^2.$$

Now, define

$$U = \sum_{i=1}^{n} \operatorname{sign}(\lambda_i) u_i u_i^*$$

where

$$\operatorname{sign}(\lambda) = \begin{cases} 1 & \text{if } \lambda \geq 0 \\ -1 & \text{if } \lambda < 0 \end{cases}$$

for every real number λ. It follows that

$$U\left(\sqrt{P} - \sqrt{Q}\right) = \left(\sqrt{P} - \sqrt{Q}\right) U = \sum_{i=1}^{n} |\lambda_i| \, u_i u_i^* = \left| \sqrt{P} - \sqrt{Q} \right|.$$

Using the operator identity

$$A^2 - B^2 = \frac{1}{2}((A - B)(A + B) + (A + B)(A - B)),$$

along with the fact that U is unitary, we have

$$\begin{aligned} \|P - Q\|_1 &\geq |\operatorname{Tr}((P - Q)U)| \\ &= \left| \frac{1}{2} \operatorname{Tr}\left((\sqrt{P} - \sqrt{Q})(\sqrt{P} + \sqrt{Q})U\right) + \frac{1}{2} \operatorname{Tr}\left((\sqrt{P} + \sqrt{Q})(\sqrt{P} - \sqrt{Q})U\right) \right| \\ &= \operatorname{Tr}\left(\left| \sqrt{P} - \sqrt{Q} \right| \left(\sqrt{P} + \sqrt{Q} \right) \right). \end{aligned}$$

Now, by the triangle inequality (for real numbers), we have that

$$u_i^* \left(\sqrt{P} + \sqrt{Q} \right) u_i \geq \left| u_i^* \sqrt{P} u_i - u_i^* \sqrt{Q} u_i \right| = |\lambda_i|$$

for every $i = 1, \ldots, n$. Thus

$$\operatorname{Tr}\left(\left| \sqrt{P} - \sqrt{Q} \right| \left(\sqrt{P} + \sqrt{Q} \right) \right) = \sum_{i=1}^{n} |\lambda_i| \, u_i^* \left(\sqrt{P} + \sqrt{Q} \right) u_i \geq \sum_{i=1}^{n} |\lambda_i|^2 = \left\| \sqrt{P} - \sqrt{Q} \right\|_2^2$$

as required. □

Proof of Theorem 4.10. The operators ρ and ξ have unit trace, and therefore

$$\left\| \sqrt{\rho} - \sqrt{\xi} \right\|_2^2 = \operatorname{Tr}\left(\sqrt{\rho} - \sqrt{\xi} \right)^2 = 2 - 2 \operatorname{Tr}\left(\sqrt{\rho} \sqrt{\xi} \right) \geq 2 - 2 \operatorname{F}(\rho, \xi).$$

The first inequality therefore follows from Lemma 4.11.

To prove the second inequality, let $\mathcal{Y}$ be a complex Euclidean space with $\dim(\mathcal{Y}) = \dim(\mathcal{X})$, and let $u, v \in \mathcal{X} \otimes \mathcal{Y}$ satisfy $\operatorname{Tr}_{\mathcal{Y}}(uu^*) = \rho$, $\operatorname{Tr}_{\mathcal{Y}}(vv^*) = \xi$, and $\operatorname{F}(\rho, \xi) = |\langle u, v \rangle|$. Such vectors exist as a consequence of Uhlmann's theorem. By the monotonicity of the trace norm we have

$$\|\rho - \xi\|_1 \leq \|uu^* - vv^*\|_1 = 2\sqrt{1 - |\langle u, v \rangle|^2} = 2\sqrt{1 - \operatorname{F}(\rho, \xi)^2},$$

and therefore

$$\operatorname{F}(\rho, \xi) \leq \sqrt{1 - \frac{1}{4} \|\rho - \xi\|_1^2}$$

as required. □

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

Lecture 5: Naimark's theorem; characterizations of channels

5.1 Naimark's Theorem

The following theorem expresses a fundamental relationship between ordinary measurements and projective measurements. It is known as Naimark's theorem, although one should understand that it is really a simple, finite-dimensional case of a more general theorem known by the same name that is important in operator theory. The theorem is also sometimes called *Neumark's Theorem*: the two names refer to the same individual, Mark Naimark, whose name has been transliterated in these two different ways.

Theorem 5.1 (Naimark's theorem)**.** *Let $\mathcal{X}$ be a complex Euclidean space, let*

$$\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$$

be a measurement on $\mathcal{X}$, and let $\mathcal{Y} = \mathbb{C}^{\Gamma}$. There exists a linear isometry $A \in \mathrm{U}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$ such that

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

for every $a \in \Gamma$.

Proof. Define $A \in \mathrm{L}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$ as

$$A = \sum_{a \in \Gamma} \sqrt{\mu(a)} \otimes e_a.$$

It holds that

$$A^*A = \sum_{a \in \Sigma} \mu(a) = \mathbb{1}_{\mathcal{X}},$$

so A is a linear isometry, and $A^*(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a})A = \mu(a)$ for each $a \in \Gamma$ as required. □

One may interpret this theorem as saying that an arbitrary measurement

$$\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$$

on a register X can be simulated by a projective measurement on a pair of registers (X, Y). In particular, we take $\mathcal{Y} = \mathbb{C}^{\Gamma}$, and by the theorem we conclude that there exists a linear isometry $A \in \mathrm{U}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$ such that

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

for every $a \in \Gamma$. For an arbitrary, but fixed, choice of a unit vector $u \in \mathcal{Y}$, we may choose a unitary operator $U \in \mathrm{U}(\mathcal{X} \otimes \mathcal{Y})$ for which

$$A = U(\mathbb{1}_{\mathcal{X}} \otimes u).$$

Consider the projective measurement $\nu : \Gamma \to \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ defined as

$$\nu(a) = U^*(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a})U$$

for each $a \in \Gamma$. If a density operator $\rho \in \mathrm{D}(\mathcal{X})$ is given, and the registers (X, Y) are prepared in the state $\rho \otimes uu^*$, then this projective measurement results in each outcome $a \in \Gamma$ with probability

$$\langle \nu(a), \rho \otimes uu^* \rangle = \langle A^*(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a})A, \rho \rangle = \langle \mu(a), \rho \rangle .$$

The probability for each measurement outcome is therefore in agreement with the original measurement μ.

5.2 Representations of quantum channels

Next, we will move on to a discussion of linear mappings of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$. Recall that we write $\mathrm{T}(\mathcal{X}, \mathcal{Y})$ to denote the space of all linear mappings taking this form. Mappings of this sort are important in quantum information theory because (among other reasons) channels take this form.

In this section we will discuss four different ways to represent such mappings, as well as a relationship among these representations. Throughout this section, and the remainder of the lecture, we assume that $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} = \mathbb{C}^{\Gamma}$ are arbitrary fixed complex Euclidean spaces.

5.2.1 The natural representation

For every mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, it is clear that the mapping

$$\mathrm{vec}(X) \mapsto \mathrm{vec}(\Phi(X))$$

is linear, as it can be represented as a composition of linear mappings. To be precise, there must exist a linear operator $K(\Phi) \in \mathrm{L}(\mathcal{X} \otimes \mathcal{X}, \mathcal{Y} \otimes \mathcal{Y})$ that satisfies

$$K(\Phi)\,\mathrm{vec}(X) = \mathrm{vec}(\Phi(X))$$

for all $X \in \mathrm{L}(\mathcal{X})$. The operator $K(\Phi)$ is the *natural representation* of Φ. A concrete expression for $K(\Phi)$ is as follows:

$$K(\Phi) = \sum_{a,b \in \Sigma} \sum_{c,d \in \Gamma} \langle E_{c,d}, \Phi(E_{a,b}) \rangle \, E_{c,a} \otimes E_{d,b}. \tag{5.1}$$

To verify that the above equation (5.1) holds, one may simply compute:

$$K(\Phi)\,\mathrm{vec}(E_{a,b}) = \mathrm{vec}\left(\sum_{c,d \in \Gamma} \langle E_{c,d}, \Phi(E_{a,b}) \rangle \, E_{c,d} \right) = \mathrm{vec}(\Phi(E_{a,b})),$$

from which it follows that $K(\Phi)\,\mathrm{vec}(X) = \mathrm{vec}(\Phi(X))$ for all X by linearity.

Notice that the mapping $K : \mathrm{T}(\mathcal{X}, \mathcal{Y}) \to \mathrm{L}(\mathcal{X} \otimes \mathcal{X}, \mathcal{Y} \otimes \mathcal{Y})$ is itself linear:

$$K(\alpha\Phi + \beta\Psi) = \alpha K(\Phi) + \beta K(\Psi)$$

for all choices of $\alpha, \beta \in \mathbb{C}$ and $\Phi, \Psi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$. In fact, K is a linear bijection, as the above form (5.1) makes clear that for every operator $A \in \mathrm{L}(\mathcal{X} \otimes \mathcal{X}, \mathcal{Y} \otimes \mathcal{Y})$ there exists a unique choice of $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ for which $A = K(\Phi)$.

The natural representation respects the notion of adjoints, meaning that

$$K(\Phi^*) = (K(\Phi))^*$$

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

5.2.2 The Choi-Jamiołkowski representation

The natural representation of mappings specifies a straightforward way that an operator can be associated with a mapping. There is a different and somewhat less straightforward way that such an association can be made that turns out to be very important in understanding completely positive mappings in particular. Specifically, let us define a mapping $J : \mathrm{T}(\mathcal{X}, \mathcal{Y}) \to \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$ as

$$J(\Phi) = \sum_{a,b \in \Sigma} \Phi(E_{a,b}) \otimes E_{a,b}$$

for each $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$. Alternately we may write

$$J(\Phi) = (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})}) (\mathrm{vec}(\mathbb{1}_{\mathcal{X}}) \mathrm{vec}(\mathbb{1}_{\mathcal{X}})^*).$$

The operator $J(\Phi)$ is called the *Choi-Jamiołkowski representation* of Φ.

As for the natural representation, it is evident from the definition that J is a linear bijection. Another way to see this is to note that the action of the mapping Φ can be recovered from the operator $J(\Phi)$ by means of the equation

$$\Phi(X) = \mathrm{Tr}_{\mathcal{X}} \left[J(\Phi) (\mathbb{1}_{\mathcal{Y}} \otimes X^{\mathsf{T}}) \right].$$

5.2.3 Kraus representations

Let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be a mapping, and suppose that

$$\{A_a : a \in \Gamma\}, \ \{B_a : a \in \Gamma\} \subset \mathrm{L}(\mathcal{X}, \mathcal{Y})$$

are (finite and nonempty) collections of operators for which the equation

$$\Phi(X) = \sum_{a \in \Gamma} A_a X B_a^* \tag{5.2}$$

holds for all $X \in \mathrm{L}(\mathcal{X})$. The expression (5.2) is said to be a *Kraus representation* of the mapping Φ. It will be established shortly that Kraus representations exist for all mappings. Unlike the natural representation and Choi-Jamiołkowski representation, Kraus representations are never unique.

The term *Kraus representation* is sometimes reserved for the case that $A_a = B_a$ for each $a \in \Gamma$, and in this case the operators $\{A_a : a \in \Gamma\}$ are called *Kraus operators*. Such a representation exists, as we will see shortly, if and only if Φ is completely positive.

Under the assumption that Φ is given by the above equation (5.2), it holds that

$$\Phi^*(Y) = \sum_{a \in \Gamma} A_a^* Y B_a.$$

5.2.4 Stinespring representations

Finally, suppose that $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is a given mapping, $\mathcal{Z}$ is a complex Euclidean space, and $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ are operators such that

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}} (AXB^*) \tag{5.3}$$

for all $X \in \mathrm{L}(\mathcal{X})$. The expression (5.3) is said to be a *Stinespring representation* of Φ. Similar to Kraus representations, Stinespring representations always exists for a given Φ and are never unique.

Similar to Kraus representations, the term *Stinespring representation* is often reserved for the case $A = B$. Once again, as we will see, such a representation exists if and only if Φ is completely positive.

If $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is given by the above equation (5.3), then

$$\Phi^*(Y) = A^*(Y \otimes \mathbb{1}_{\mathcal{Z}})B.$$

(Expressions of this form are also sometimes referred to as Stinespring representations.)

5.2.5 A simple relationship among the representations

The following proposition explains a simple way in which the four representations discussed above relate to one another.

Proposition 5.2. *Let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ and let $\{A_a : a \in \Gamma\}$ and $\{B_a : a \in \Gamma\}$ be collections of operators in $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ for a finite, non-empty set Γ. The following statements are equivalent.*

1. *(Kraus representations.) It holds that*

   $$\Phi(X) = \sum_{a \in \Gamma} A_a X B_a^*$$

   for all $X \in \mathrm{L}(\mathcal{X})$.
2. *(Stinespring representations.) For $\mathcal{Z} = \mathbb{C}^\Gamma$ and $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ defined as*

   $$A = \sum_{a \in \Gamma} A_a \otimes e_a \qquad \text{and} \qquad B = \sum_{a \in \Gamma} B_a \otimes e_a,$$

   it holds that $\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(AXB^*)$ for all $X \in \mathrm{L}(\mathcal{X})$.
3. *(The natural representation.) It holds that*

   $$K(\Phi) = \sum_{a \in \Gamma} A_a \otimes \overline{B_a}.$$

4. *(The Choi-Jamiołkowski representation.) It holds that*

   $$J(\Phi) = \sum_{a \in \Gamma} \mathrm{vec}(A_a)\,\mathrm{vec}(B_a)^*.$$

Proof. The equivalence between items 1 and 2 is a straightforward calculation. The equivalence between items 1 and 3 follows from the identity

$$\mathrm{vec}(A_a X B_a^*) = \left(A_a \otimes \overline{B_a}\right)\mathrm{vec}(X)$$

for each $a \in \Gamma$ and every $X \in \mathrm{L}(\mathcal{X})$. Finally, the equivalence between items 1 and 4 follows from the expression

$$J(\Phi) = (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})\left(\mathrm{vec}(\mathbb{1}_{\mathcal{X}})\,\mathrm{vec}(\mathbb{1}_{\mathcal{X}})^*\right)$$

along with

$$(A_a \otimes \mathbb{1}_{\mathcal{X}})\,\mathrm{vec}(\mathbb{1}_{\mathcal{X}}) = \mathrm{vec}(A_a) \quad \text{and} \quad \mathrm{vec}(\mathbb{1}_{\mathcal{X}})^*(B_a^* \otimes \mathbb{1}_{\mathcal{X}}) = \mathrm{vec}(B_a)^*$$

for each $a \in \Gamma$. □

Various facts may be derived from the above proposition. For instance, it follows that every mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ has a Kraus representation in which $|\Gamma| = \mathrm{rank}(J(\Phi)) \leq \dim(\mathcal{X} \otimes \mathcal{Y})$, and similarly that every such Φ has a Stinespring representation in which $\dim(\mathcal{Z}) = \mathrm{rank}(J(\Phi))$.

5.3 Characterizations of completely positive and trace-preserving maps

Now we are ready to characterize quantum channels in terms of their Choi-Jamiołkowski, Kraus, and Stinespring representations. (The natural representation does not happen to help us with respect to these particular characterizations—which is not surprising because it essentially throws away the operator structure of the inputs and outputs of a given mapping.)

5.3.1 Characterizations of completely positive maps

We will begin with a characterization of completely positive mappings in terms of their Choi-Jamiołkowski, Kraus, and Stinespring representations. Before doing this, let us recall the following terminology: a mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is said to be *positive* if and only if $\Phi(P) \in \mathrm{Pos}(\mathcal{Y})$ for all $P \in \mathrm{Pos}(\mathcal{X})$, and is said to be *completely positive* if and only if $\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}$ is positive for every choice of a complex Euclidean space $\mathcal{Z}$.

Theorem 5.3. *For every mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, the following statements are equivalent.*

1. *Φ is completely positive.*
2. *$\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})}$ is positive.*
3. *$J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$.*
4. *There exists a finite set of operators $\{A_a : a \in \Gamma\} \subset \mathrm{L}(\mathcal{X}, \mathcal{Y})$ such that*
$$\Phi(X) = \sum_{a \in \Gamma} A_a X A_a^* \tag{5.4}$$
for all $X \in \mathrm{L}(\mathcal{X})$.
5. *Item 4 holds for $|\Gamma| = \mathrm{rank}(J(\Phi))$.*
6. *There exists a complex Euclidean space $\mathcal{Z}$ and an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ such that*
$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(AXA^*)$$
for all $X \in \mathrm{L}(\mathcal{X})$.
7. *Item 6 holds for $\mathcal{Z}$ having dimension equal to the rank of $J(\Phi)$.*

Proof. The theorem will be proved by establishing implications among the 7 items that are sufficient to establish their equivalence. The particular implications that will be proved are summarized as follows:

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (5) \Rightarrow (4) \Rightarrow (1)$$
$$(5) \Rightarrow (7) \Rightarrow (6) \Rightarrow (1)$$

Note that some of these implications are immediate: item 1 implies item 2 by the definition of complete positivity, item 5 trivially implies item 4, item 7 trivially implies item 6, and item 5 implies item 7 by Proposition 5.2.

Assume that $\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})}$ is positive. Given that

$$\mathrm{vec}(\mathbb{1}_{\mathcal{X}})\,\mathrm{vec}(\mathbb{1}_{\mathcal{X}})^* \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{X})$$

and

$$J(\Phi) = \left(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})}\right)(\mathrm{vec}(\mathbb{1}_{\mathcal{X}})\,\mathrm{vec}(\mathbb{1}_{\mathcal{X}})^*),$$

it follows that $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$. Item 2 therefore implies item 3.

Next, assume that $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$. By the spectral theorem, along with the fact that every eigenvalue of a positive semidefinite operator is non-negative, we have that it is possible to write

$$J(\Phi) = \sum_{a \in \Gamma} u_a u_a^*,$$

for some choice of vectors $\{u_a : a \in \Gamma\} \subset \mathcal{Y} \otimes \mathcal{X}$ such that $|\Gamma| = \mathrm{rank}(J(\Phi))$. Defining $A_a \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ so that $\mathrm{vec}(A_a) = u_a$ for each $a \in \Gamma$, it follows that

$$J(\Phi) = \sum_{a \in \Gamma} \mathrm{vec}(A_a)\,\mathrm{vec}(A_a)^*.$$

The equation (5.4) therefore holds for every $X \in \mathrm{L}(\mathcal{X})$ by Proposition 5.2, which establishes that item 3 implies item 5.

Finally, note that mappings of the form $X \mapsto AXA^*$ are easily seen to be completely positive, and non-negative linear combinations of completely positive mappings are completely positive as well. Item 4 therefore implies item 1. Along similar lines, the partial trace is completely positive and completely positive mappings are closed under composition. Item 6 therefore implies item 1, which completes the proof. □

5.3.2 Characterizations of trace-preserving maps

Next we will characterize the collection of trace-preserving mappings in terms of their representations. These characterizations are straightforward, but it is nevertheless convenient to state them in a similar style to those of Theorem 5.3.

Before stating the theorem, the following terminology must be mentioned. A mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is said to be *unital* if and only if $\Phi(\mathbb{1}_{\mathcal{X}}) = \mathbb{1}_{\mathcal{Y}}$.

Theorem 5.4. *For every mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, the following statements are equivalent.*

1. *Φ is trace-preserving.*
2. *Φ^* is unital.*
3. *$\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}$.*
4. *There exists a Kraus representation*
$$\Phi(X) = \sum_{a \in \Gamma} A_a X B_a^*$$
of Φ for which the operators $\{A_a : a \in \Gamma\}$, $\{B_a : a \in \Gamma\} \subset \mathrm{L}(\mathcal{X}, \mathcal{Y})$ satisfy
$$\sum_{a \in \Gamma} A_a^* B_a = \mathbb{1}_{\mathcal{X}}.$$
5. *For all Kraus representations*
$$\Phi(X) = \sum_{a \in \Gamma} A_a X B_a^*$$
of Φ, the operators $\{A_a : a \in \Gamma\}$, $\{B_a : a \in \Gamma\} \subset \mathrm{L}(\mathcal{X}, \mathcal{Y})$ satisfy
$$\sum_{a \in \Gamma} A_a^* B_a = \mathbb{1}_{\mathcal{X}}.$$

6. *There exists a Stinespring representation*

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}\left(AXB^*\right)$$

of Φ *for which the operators* $A, B \in \mathrm{L}\left(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z}\right)$ *satisfy* $A^*B = \mathbb{1}_{\mathcal{X}}$.

7. *For all Stinespring representations*

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}\left(AXB^*\right)$$

of Φ, *the operators* $A, B \in \mathrm{L}\left(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z}\right)$ *satisfy* $A^*B = \mathbb{1}_{\mathcal{X}}$.

Proof. Under the assumption that Φ is trace-preserving, it holds that

$$\langle \mathbb{1}_{\mathcal{X}}, X \rangle = \mathrm{Tr}(X) = \mathrm{Tr}(\Phi(X)) = \langle \mathbb{1}_{\mathcal{Y}}, \Phi(X) \rangle = \langle \Phi^*(\mathbb{1}_{\mathcal{Y}}), X \rangle,$$

and thus $\langle \mathbb{1}_{\mathcal{X}} - \Phi^*(\mathbb{1}_{\mathcal{Y}}), X \rangle = 0$ for all $X \in \mathrm{L}\left(\mathcal{X}\right)$. It follows that $\Phi^*(\mathbb{1}_{\mathcal{Y}}) = \mathbb{1}_{\mathcal{X}}$, so Φ^* is unital. Along similar lines, the assumption that Φ^* is unital implies that

$$\mathrm{Tr}(\Phi(X)) = \langle \mathbb{1}_{\mathcal{Y}}, \Phi(X) \rangle = \langle \Phi^*(\mathbb{1}_{\mathcal{Y}}), X \rangle = \langle \mathbb{1}_{\mathcal{X}}, X \rangle = \mathrm{Tr}(X)$$

for every $X \in \mathrm{L}\left(\mathcal{X}\right)$, so Φ is trace-preserving. The equivalence of items 1 and 2 has therefore been established.

Next, suppose that

$$\Phi(X) = \sum_{a \in \Gamma} A_a X B_a^*$$

is a Kraus representation of Φ. It holds that

$$\Phi^*(Y) = \sum_{a \in \Gamma} A_a^* Y B_a$$

for every $Y \in \mathrm{L}\left(\mathcal{Y}\right)$, and in particular it holds that

$$\Phi^*(\mathbb{1}_{\mathcal{Y}}) = \sum_{a \in \Gamma} A_a^* B_a.$$

Thus, if Φ^* is unital, then

$$\sum_{a \in \Gamma} A_a^* B_a = \mathbb{1}_{\mathcal{X}}, \tag{5.5}$$

and so it has been proved that item 2 implies item 5. On the other hand, if (5.5) holds, then it follows that $\Phi^*(\mathbb{1}_{\mathcal{Y}}) = \mathbb{1}_{\mathcal{X}}$, and therefore item 4 implies item 2. Given that every mapping has at least one Kraus representation, item 5 trivially implies item 4, and therefore the equivalence of items 2, 4, and 5 has been established.

Now assume that

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}\left(AXB^*\right)$$

is a Stinespring representation of Φ. It follows that

$$\Phi^*(Y) = A^*\left(Y \otimes \mathbb{1}_{\mathcal{Z}}\right)B$$

for all $Y \in \mathrm{L}\left(\mathcal{Y}\right)$, and in particular $\Phi^*(\mathbb{1}_{\mathcal{Y}}) = A^*B$. The equivalence of items 2, 6 and 7 follows by the same reasoning as for the case of items 2, 4 and 5.

Finally, suppose that $\mathcal{X} = \mathbb{C}^{\Gamma}$, and consider the operator

$$\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \sum_{a,b\in\Gamma} \mathrm{Tr}\left(\Phi(E_{a,b})\right) E_{a,b}. \tag{5.6}$$

If it holds that Φ is trace-preserving, then it follows that

$$\mathrm{Tr}(\Phi(E_{a,b})) = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b, \end{cases} \tag{5.7}$$

and therefore

$$\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \sum_{a\in\Gamma} E_{a,a} = \mathbb{1}_{\mathcal{X}}.$$

Conversely, if it holds that $\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}$, then by the expression (5.6) it follows that (5.7) holds. The mapping Φ is therefore trace-preserving by linearity and the fact that $\{E_{a,b} : a, b \in \Gamma\}$ is a basis of $\mathrm{L}(\mathcal{X})$. The equivalence of items 1 and 3 has therefore been established, which completes the proof. □

5.3.3 Characterizations of channels

The two theorems from above are now easily combined to give the following characterization of quantum channels. For convenience, let us hereafter write $\mathrm{C}(\mathcal{X}, \mathcal{Y})$ to denote the set of all channels from $\mathcal{X}$ to $\mathcal{Y}$, meaning the set of all completely positive and trace-preserving mappings $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$.

Corollary 5.5. *Let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$. The following statements are equivalent.*

1. $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$.
2. $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$ *and* $\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}$.
3. *There exists a finite set of operators $\{A_a : a \in \Gamma\} \subset \mathrm{L}(\mathcal{X}, \mathcal{Y})$ such that*

   $$\Phi(X) = \sum_{a\in\Gamma} A_a X A_a^*$$

   for all $X \in \mathrm{L}(\mathcal{X})$, and such that

   $$\sum_{a\in\Gamma} A_a^* A_a = \mathbb{1}_{\mathcal{X}}.$$

4. *Item 3 holds for Γ satisfying $|\Gamma| = \mathrm{rank}(J(\Phi))$.*
5. *There exists a complex Euclidean space $\mathcal{Z}$ and a linear isometry $A \in \mathrm{U}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$, such that*

   $$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(AXA^*)$$

   for all $X \in \mathrm{L}(\mathcal{X})$.
6. *Item 5 holds for a complex Euclidean space $\mathcal{Z}$ with $\dim(\mathcal{Z}) = \mathrm{rank}(J(\Phi))$.*

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

Lecture 6: Further remarks on measurements and channels

In this lecture we will discuss a few loosely connected topics relating to measurements and channels. These discussions will serve to illustrate some of the concepts we have discussed in previous lectures, and are also an opportunity to introduce a few notions that will be handy in future lectures.

6.1 Measurements as channels and nondestructive measurements

We begin with two simple points concerning measurements. The first explains how measurements may be viewed as special types of channels, and the second introduces the notion of nondestructive measurements (which were commented on briefly in Lecture 3).

6.1.1 Measurements as channels

Suppose that we have a measurement $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$ on a register X. When this measurement is performed, X ceases to exist, and the measurement result is transmitted to some hypothetical observer that we generally think of as being external to the system being described or considered.

We could, however, imagine that the measurement outcome is stored in a new register Y, whose classical state set is chosen to be Γ, rather than imagining that it is transmitted to an external observer. Taking this point of view, the measurement μ corresponds to a channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$, where

$$\Phi(X) = \sum_{a \in \Gamma} \langle \mu(a), X \rangle \, E_{a,a}$$

for every $X \in \mathrm{L}(\mathcal{X})$. For any density operator $\rho \in \mathrm{D}(\mathcal{X})$, the output $\Phi(\rho)$ is "classical" in the sense that it is a convex combination of states of the form $E_{a,a}$, which we identify with the classical state a for each $a \in \Gamma$.

Of course we expect that Φ should be a valid channel, but let us verify that this is so. It is clear that Φ is linear and preserves trace, as

$$\mathrm{Tr}(\Phi(X)) = \sum_{a \in \Gamma} \langle \mu(a), X \rangle \, \mathrm{Tr}(E_{a,a}) = \sum_{a \in \Gamma} \langle \mu(a), X \rangle = \langle \mathbb{1}_{\mathcal{X}}, X \rangle = \mathrm{Tr}(X)$$

for every $X \in \mathrm{L}(\mathcal{X})$. To see that Φ is completely positive we may compute the Choi-Jamiołkowski representation

$$J(\Phi) = \sum_{b,c \in \Sigma} \sum_{a \in \Gamma} \langle \mu(a), E_{b,c} \rangle \, E_{a,a} \otimes E_{b,c} = \sum_{a \in \Gamma} E_{a,a} \otimes \left(\sum_{b,c \in \Sigma} \langle \mu(a), E_{b,c} \rangle \, E_{b,c} \right) = \sum_{a \in \Gamma} E_{a,a} \otimes \mu(a)^{\mathsf{T}},$$

where we have assumed that $\mathcal{X} = \mathbb{C}^{\Sigma}$. Each $\mu(a)$ is positive semidefinite, and so $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, which proves that Φ is completely positive.

An alternate way to see that Φ is indeed a channel is to use Naimark's theorem, which implies that $\mu(a) = A^*(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a})A$ for some isometry $A \in \mathrm{U}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$. It holds that

$$\Phi(X) = \sum_{a \in \Gamma} \langle A^*(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a})A, X \rangle \, E_{a,a} = \sum_{a \in \Gamma} E_{a,a} \, \mathrm{Tr}_{\mathcal{X}} \left(AXA^* \right) E_{a,a},$$

which is the composition of two channels: $\Phi = \Delta\Psi$, where $\Psi(X) = \mathrm{Tr}_{\mathcal{X}}(AXA^*)$ and

$$\Delta(Y) = \sum_{a \in \Gamma} E_{a,a} Y E_{a,a}$$

is the *completely dephasing channel* (which effectively zeroes out all off-diagonal entries of a matrix and leaves the diagonal alone). The composition of two channels is a channel, so we have that Φ is a channel.

6.1.2 Nondestructive measurements

Sometimes it is convenient to consider measurements that do not destroy registers, but rather leave them in some state that may depend on the measurement outcome that is obtained from the measurement. We will refer to such processes as *non-destructive measurements*.

Formally, a non-destructive measurement on a space $\mathcal{X}$ is a function

$$\nu : \Gamma \to \mathrm{L}(\mathcal{X}) : a \mapsto M_a,$$

for some finite, non-empty set of measurement outcomes Γ, that satisfies the constraint

$$\sum_{a \in \Gamma} M_a^* M_a = \mathbb{1}_{\mathcal{X}}.$$

When a non-destructive measurement of this form is applied to a register X that has reduced state $\rho \in \mathrm{D}(\mathcal{X})$, two things happen:

1. Each measurement outcome $a \in \Gamma$ occurs with probability $\langle M_a^* M_a, \rho \rangle$.
2. Conditioned on the measurement outcome $a \in \Gamma$ occurring, the reduced state of the register X becomes
$$\frac{M_a \rho M_a^*}{\langle M_a^* M_a, \rho \rangle}.$$

Let us now observe that non-destructive measurements really do not require new definitions, but can be formed from a composition of an operation and a measurement as we defined them initially. One way to do this is to follow the proof of Naimark's theorem. Specifically, let $\mathcal{Y} = \mathbb{C}^{\Gamma}$ and define an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$ as

$$A = \sum_{a \in \Gamma} M_a \otimes e_a.$$

We have that

$$A^*A = \sum_{a \in \Gamma} M_a^* M_a = \mathbb{1}_{\mathcal{X}},$$

which shows that A is a linear isometry. Therefore, the mapping $X \mapsto AXA^*$ from $\mathrm{L}(\mathcal{X})$ to $\mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$ is a channel. Now consider that this operation is followed by a measurement of $\mathcal{Y}$ with respect to the standard basis. Each outcome $a \in \Gamma$ appears with probability

$$\langle \mathbb{1}_{\mathcal{X}} \otimes E_{a,a}, A\rho A^* \rangle = \langle M_a^* M_a, \rho \rangle,$$

and conditioned on the outcome $a \in \Gamma$ appearing, the state of X becomes

$$\frac{\mathrm{Tr}_{\mathcal{Y}}\left[(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a})A\rho A^*\right]}{\langle \mathbb{1}_{\mathcal{X}} \otimes E_{a,a}, A\rho A^* \rangle} = \frac{M_a \rho M_a^*}{\langle M_a^* M_a, \rho \rangle}$$

as required.

Viewing a nondestructive measurement as a channel, along the same lines as in the previous subsection, we see that it is given by

$$\Phi(X) = \sum_{a\in\Gamma} M_a X M_a^* \otimes E_{a,a} = \sum_{a\in\Gamma} (M_a \otimes e_a) X (M_a \otimes e_a)^*,$$

which is easily seen to be completely positive and trace-preserving using the Kraus representation characterization from the previous lecture.

6.2 Convex combinations of channels

Next we will discuss issues relating to the structure of the set of channels $\mathrm{C}(\mathcal{X},\mathcal{Y})$ for a given choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$.

Let us begin with the simple observation that convex combinations of channels are also channels: for any choice of channels $\Phi_0, \Phi_1 \in \mathrm{C}(\mathcal{X},\mathcal{Y})$, and any real number $\lambda \in [0,1]$, it holds that

$$\lambda\Phi_0 + (1-\lambda)\Phi_1 \in \mathrm{C}(\mathcal{X},\mathcal{Y}).$$

One may verify this in different ways, one of which is to consider the Choi-Jamiołkowski representation:

$$J(\lambda\Phi_0 + (1-\lambda)\Phi_1) = \lambda J(\Phi_0) + (1-\lambda) J(\Phi_1).$$

Given that Φ_0 and Φ_1 are completely positive, we have $J(\Phi_0), J(\Phi_1) \in \mathrm{Pos}(\mathcal{Y}\otimes\mathcal{X})$, and because $\mathrm{Pos}(\mathcal{Y}\otimes\mathcal{X})$ is convex it follows that

$$J(\lambda\Phi_0 + (1-\lambda)\Phi_1) \in \mathrm{Pos}(\mathcal{Y}\otimes\mathcal{X}).$$

Thus, $\lambda\Phi_0 + (1-\lambda)\Phi_1$ is completely positive. The fact that $\lambda\Phi_0 + (1-\lambda)\Phi_1$ preserves trace is immediate by linearity. One could also verify the claim that $\mathrm{C}(\mathcal{X},\mathcal{Y})$ is convex somewhat more directly, by considering the definition of complete positivity.

It is also not difficult to see that the set $\mathrm{C}(\mathcal{X},\mathcal{Y})$ is compact for any choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$. This may be verified by again turning to the Choi-Jamiołkowski representation. First, we observe that the set

$$\{P \in \mathrm{Pos}(\mathcal{Y}\otimes\mathcal{X}) \,:\, \mathrm{Tr}(P) = \dim(\mathcal{X})\}$$

is compact, by essentially the same reasoning (which we have discussed previously) that shows the set $\mathrm{D}(\mathcal{Z})$ to be compact (for every complex Euclidean space $\mathcal{Z}$). Second, the set

$$\{X \in \mathrm{L}(\mathcal{Y}\otimes\mathcal{X}) \,:\, \mathrm{Tr}_{\mathcal{Y}}(X) = \mathbb{1}_{\mathcal{X}}\}$$

is closed, for it is an affine subspace (in this case given by a translation of the kernel of the partial trace on $\mathcal{Y}$). The intersection of a compact set and a closed set is compact, so

$$\{P \in \mathrm{Pos}(\mathcal{Y}\otimes\mathcal{X}) \,:\, \mathrm{Tr}_{\mathcal{Y}}(P) = \mathbb{1}_{\mathcal{X}}\}$$

is compact. Continuous mappings map compact sets to compact sets, and the mapping

$$J^{-1} : \mathrm{L}(\mathcal{Y}\otimes\mathcal{X}) \to \mathrm{T}(\mathcal{X},\mathcal{Y})$$

that takes $J(\Phi)$ to Φ for each $\Phi \in \mathrm{T}(\mathcal{X},\mathcal{Y})$ is continuous, so we have that $\mathrm{C}(\mathcal{X},\mathcal{Y})$ is compact.

6.2.1 Choi's theorem on extremal channels

Let us now consider the extreme points of the set $\mathrm{C}(\mathcal{X},\mathcal{Y})$. These are the channels that cannot be written as proper convex combinations of distinct channels. The extreme points of $\mathrm{C}(\mathcal{X},\mathcal{Y})$ can, in some sense, be viewed as being analogous to the pure states of $\mathrm{D}(\mathcal{X})$, but it turns out that the structure of $\mathrm{C}(\mathcal{X},\mathcal{Y})$ is more complicated than $\mathrm{D}(\mathcal{X})$. A characterization of the extreme points of this set is given by the following theorem.

Theorem 6.1 (Choi). *Let $\{A_a : a \in \Sigma\} \subset \mathrm{L}(\mathcal{X},\mathcal{Y})$ be a linearly independent set of operators and let $\Phi \in \mathrm{C}(\mathcal{X},\mathcal{Y})$ be a quantum channel that is given by*

$$\Phi(X) = \sum_{a\in\Sigma} A_a X A_a^*$$

for all $X \in \mathrm{L}(\mathcal{X})$. The channel Φ is an extreme point of the set $\mathrm{C}(\mathcal{X},\mathcal{Y})$ if and only if

$$\{A_b^* A_a : (a,b) \in \Sigma\times\Sigma\}$$

is a linearly independent set of operators.

Proof. Let $\mathcal{Z} = \mathbb{C}^\Sigma$, and define $M \in \mathrm{L}(\mathcal{Z},\mathcal{Y}\otimes\mathcal{X})$ as

$$M = \sum_{a\in\Sigma} \mathrm{vec}(A_a) e_a^*.$$

Given that $\{A_a : a \in \Sigma\}$ is linearly independent, it holds that $\ker(M) = \{0\}$. It also holds that

$$MM^* = \sum_{a\in\Sigma} \mathrm{vec}(A_a)\,\mathrm{vec}(A_a)^* = J(\Phi).$$

Assume first that Φ is not an extreme point of $\mathrm{C}(\mathcal{X},\mathcal{Y})$. It follows that there exist channels $\Psi_0,\Psi_1 \in \mathrm{C}(\mathcal{X},\mathcal{Y})$, with $\Psi_0 \neq \Psi_1$, such that

$$\Phi = \frac{1}{2}\Psi_0 + \frac{1}{2}\Psi_1.$$

Let $P = J(\Phi)$, $Q_0 = J(\Psi_0)$, and $Q_1 = J(\Psi_1)$. As Φ, Ψ_0, and Ψ_1 are channels, one has that $P, Q_0, Q_1 \in \mathrm{Pos}(\mathcal{Y}\otimes\mathcal{X})$ and

$$\mathrm{Tr}_\mathcal{Y}(P) = \mathrm{Tr}_\mathcal{Y}(Q_0) = \mathrm{Tr}_\mathcal{Y}(Q_1) = \mathbb{1}_\mathcal{X}.$$

Moreover, as $\frac{1}{2}Q_0 \leq P$, it follows that $\mathrm{im}(Q_0) \subseteq \mathrm{im}(P) = \mathrm{im}(M)$, and therefore there exists a positive semidefinite operator $R_0 \in \mathrm{Pos}(\mathcal{Z})$ for which $Q_0 = MR_0M^*$. By similar reasoning, there exists a positive semidefinite operator $R_1 \in \mathrm{Pos}(\mathcal{Z})$ for which $Q_1 = MR_1M^*$. Letting $H = R_0 - R_1$, one finds that

$$0 = \mathrm{Tr}_\mathcal{Y}(Q_0) - \mathrm{Tr}_\mathcal{Y}(Q_1) = \mathrm{Tr}_\mathcal{Y}(MHM^*) = \sum_{a,b\in\Sigma} H(a,b)\,(A_b^*A_a)^\mathsf{T},$$

and therefore

$$\sum_{a,b\in\Sigma} H(a,b) A_b^* A_a = 0.$$

Given that $\Psi_0 \neq \Psi_1$, it holds that $Q_0 \neq Q_1$, so $R_0 \neq R_1$, and thus $H \neq 0$. It has therefore been shown that the set $\left\{A_b^*A_a : (a,b) \in \Sigma\times\Sigma\right\}$ is linearly dependent, as required.

Now assume the set $\left\{A_b^* A_a : (a,b) \in \Sigma \times \Sigma\right\}$ is linearly dependent: there exists a nonzero operator $Z \in \mathrm{L}(\mathcal{Z})$ such that

$$\sum_{a,b\in\Sigma} Z(a,b) A_b^* A_a = 0.$$

It follows that

$$\sum_{a,b\in\Sigma} Z^*(a,b) A_b^* A_a = \left(\sum_{a,b\in\Sigma} Z(a,b) A_b^* A_a\right)^* = 0$$

and therefore

$$\sum_{a,b\in\Sigma} H(a,b) A_b^* A_a = 0 \tag{6.1}$$

for both of the choices $H = Z + Z^*$ and $H = iZ - iZ^*$. At least one of the operators $Z + Z^*$ and $iZ - iZ^*$ must be nonzero when Z is nonzero, so one may conclude that the above equation (6.1) holds for a nonzero Hermitian operator $H \in \mathrm{Herm}(\mathcal{Z})$ that is hereafter taken to be fixed. Given that this equation is invariant under rescaling H, there is no loss of generality in assuming $\|H\| \leq 1$.

As $\|H\| \leq 1$ and H is Hermitian, it follows that $\mathbb{1} + H$ and $\mathbb{1} - H$ are both positive semidefinite, and therefore the operators $M(\mathbb{1} + H)M^*$ and $M(\mathbb{1} - H)M^*$ are positive semidefinite as well. Letting $\Psi_0, \Psi_1 \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be the mappings that satisfy

$$J(\Psi_0) = M(\mathbb{1} + H)M^* \quad \text{and} \quad J(\Psi_1) = M(\mathbb{1} - H)M^*,$$

one therefore has that Ψ_0 and Ψ_1 are completely positive. It holds that

$$\mathrm{Tr}_{\mathcal{Y}}(MHM^*) = \sum_{a,b\in\Sigma} H(a,b)\left(A_b^* A_a\right)^{\mathsf{T}} = \left(\sum_{a,b\in\Sigma} H(a,b) A_b^* A_a\right)^{\mathsf{T}} = 0$$

and therefore

$$\mathrm{Tr}_{\mathcal{Y}}(J(\Psi_0)) = \mathrm{Tr}_{\mathcal{Y}}(MM^*) + \mathrm{Tr}_{\mathcal{Y}}(MHM^*) = \mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}$$

and

$$\mathrm{Tr}_{\mathcal{Y}}(J(\Psi_1)) = \mathrm{Tr}_{\mathcal{Y}}(MM^*) - \mathrm{Tr}_{\mathcal{Y}}(MHM^*) = \mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}.$$

Thus, Ψ_0 and Ψ_1 are channels. Finally, given that $H \neq 0$ and $\ker(M) = \{0\}$ it holds that $J(\Psi_0) \neq J(\Psi_1)$, so that $\Psi_0 \neq \Psi_1$. As

$$\frac{1}{2}J(\Psi_0) + \frac{1}{2}J(\Psi_1) = MM^* = J(\Phi),$$

one has that

$$\Phi = \frac{1}{2}\Psi_0 + \frac{1}{2}\Psi_1,$$

which demonstrates that Φ is not an extreme point of $\mathrm{C}(\mathcal{X}, \mathcal{Y})$. □

6.2.2 Application of Carathéodory's theorem to convex combinations of channels

For an arbitrary channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$, one may always write

$$\Phi = \sum_{a \in \Gamma} p(a) \Phi_a$$

for some finite set Γ, a probability vector $p \in \mathbb{R}^{\Gamma}$, and $\{\Phi_a : a \in \Gamma\}$ being a collection of extremal channels. This is so because $\mathrm{C}(\mathcal{X}, \mathcal{Y})$ is convex and compact, and every compact and convex set is equal to the convex hull of its extreme points (by the Krein-Milman theorem). One natural question is: how large must Γ be for such an expression to exist? Carathéodory's theorem, which you will find stated in the Lecture 2 notes, provides an upper bound.

To explain this bound, let us assume $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} = \mathbb{C}^{\Gamma}$. As explained in Lecture 1, we may view the space of Hermitian operators $\mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X})$ as a real vector space indexed by $(\Gamma \times \Sigma)^2$, and therefore having dimension $|\Sigma|^2 |\Gamma|^2$.

Now, the Choi-Jamiołkowski representation $J(\Phi)$ of any channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ is an element of $\mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, and is therefore an element of $\mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X})$. Taking

$$\mathcal{A} = \{J(\Psi) : \Psi \in \mathrm{C}(\mathcal{X}, \mathcal{Y}) \text{ is extremal}\} \subset \mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X}),$$

and applying Carathéodory's theorem, we have that every element $J(\Phi) \in \mathrm{conv}(\mathcal{A})$ can be written as

$$J(\Phi) = \sum_{j=1}^{m} p_j J(\Psi_j)$$

for some probability vector $p = (p_1, \ldots, p_m)$ and some choice of extremal channels $\Psi_1, \ldots, \Psi_m$, for $m = |\Sigma|^2 |\Gamma|^2 + 1$. Equivalently, every channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ can be written as a convex combination of no more than $m = |\Sigma|^2 |\Gamma|^2 + 1$ extremal channels.

This bound may, in fact, be improved to $m = |\Sigma|^2 |\Gamma|^2 - |\Sigma|^2 + 1$ by observing that the trace-preserving property of channels reduces the dimension of the smallest (affine) subspace in which they may be contained.

6.2.3 Mixed unitary channels

Suppose that $\mathcal{X}$ is a complex Euclidean space and $U \in \mathrm{U}(\mathcal{X})$ is a unitary operator. The mapping $\Psi \in \mathrm{T}(\mathcal{X})$ defined by

$$\Psi(X) = UXU^*$$

for all $X \in \mathrm{L}(\mathcal{X})$ is clearly a channel, and any such channel is called a *unitary channel*. Any channel $\Phi \in \mathrm{C}(\mathcal{X})$ that can be written as a convex combination of unitary channels is said to be a *mixed unitary channel*. (The term *random unitary channel* is more common, but it is easily confused with a different notion whereby one chooses a unitary channel randomly according to some distribution or measure.)

Again let us suppose that $\mathcal{X} = \mathbb{C}^{\Sigma}$. One may perform a similar calculation to the one above to find that every mixed unitary channel can be written as a convex combination of $|\Sigma|^4 - 2|\Sigma|^2 + 2$ unitary channels. The difference between this expression and the one from above comes from considering additional linear constraints satisfied by unitary channels—namely that they are unital in addition to being trace-preserving.

6.3 Discrete Weyl operators and teleportation

Now we will switch gears and discuss something different: the collection of so-called *discrete Weyl operators* and some examples of channels based on them. They also allow us to discuss a straightforward generalization of *quantum teleportation* to high-dimensional systems.

6.3.1 Definition of discrete Weyl operators

For any positive integer n, we define

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\},$$

and view this set as a ring with respect to addition and multiplication defined modulo n. Let us also define

$$\omega_n = \exp(2\pi i/n)$$

to be a principal n-th root of unity, which will typically be denoted ω rather than ω_n when n has been fixed or is clear from the context.

Now, for a fixed choice of n, let $\mathcal{X} = \mathbb{C}^{\mathbb{Z}_n}$, and define two unitary operators $X, Z \in \mathrm{U}(\mathcal{X})$ as follows:

$$X = \sum_{a \in \mathbb{Z}_n} E_{a+1,a} \qquad \text{and} \qquad Z = \sum_{a \in \mathbb{Z}_n} \omega^a E_{a,a}.$$

Here, and throughout this section, the expression $a + 1$ refers to addition in $\mathbb{Z}_n$, and similar for other arithmetic expressions involving elements of $\mathbb{Z}_n$. Finally, for any choice of $(a, b) \in \mathbb{Z}_n^2$ we define

$$W_{a,b} = X^a Z^b.$$

Such operators are known as *discrete Weyl operators* (and also as *generalized Pauli operators*).

Let us note a few basic facts about the collection

$$\{W_{a,b} : (a, b) \in \mathbb{Z}_n^2\}. \tag{6.2}$$

First, we have that each $W_{a,b}$ is unitary, given that X and Z are obviously unitary. Next, it is straightforward to show that

$$\mathrm{Tr}(W_{a,b}) = \begin{cases} n & \text{if } a = b = 0 \\ 0 & \text{otherwise.} \end{cases}$$

This implies that the collection (6.2) forms an orthogonal basis for $\mathrm{L}(\mathcal{X})$, because

$$\langle W_{a,b}, W_{c,d} \rangle = \mathrm{Tr}\left(Z^{-b} X^{-a} X^c Z^d\right) = \mathrm{Tr}\left(X^{c-a} Z^{d-b}\right) = \begin{cases} n & \text{if } (a, b) = (c, d) \\ 0 & \text{otherwise.} \end{cases}$$

Finally, we note the *commutation relation*

$$ZX = \omega XZ,$$

which (for instance) implies

$$W_{a,b} W_{c,d} = (X^a Z^b)(X^c Z^d) = \omega^{bc} X^{a+c} Z^{b+d} = \omega^{bc-ad} (X^c Z^d)(X^a Z^b) = \omega^{bc-ad} W_{c,d} W_{a,b}.$$

6.3.2 Dephasing and depolarizing channels

Two simple examples of mixed unitary channels, where the corresponding unitary operators are chosen to be discrete Weyl operators, are as follows:

$$\Delta(A) = \frac{1}{n} \sum_{a \in \mathbb{Z}_n} W_{0,a} A W_{0,a}^* \qquad \text{and} \qquad \Omega(A) = \frac{1}{n^2} \sum_{a,b \in \mathbb{Z}_n} W_{a,b} A W_{a,b}^*.$$

We have already encountered Δ in this lecture: it is the completely dephasing channel that zeros out off-diagonal entries and leaves the diagonal alone. To see that this is so, we may compute the action on the standard basis of $\mathrm{L}(\mathcal{X})$:

$$\Delta(E_{c,d}) = \frac{1}{n} \sum_{a \in \mathbb{Z}_n} W_{0,a} E_{c,d} W_{0,a}^* = \left(\frac{1}{n} \sum_{a \in \mathbb{Z}_n} \omega^{a(c-d)} \right) E_{c,d} = \begin{cases} E_{c,d} & \text{if } c = d \\ 0 & \text{if } c \neq d. \end{cases}$$

Alternately we may compute the action on the basis of discrete Weyl operators:

$$\Delta(W_{c,d}) = \frac{1}{n} \sum_{a \in \mathbb{Z}_n} W_{0,a} W_{c,d} W_{0,a}^* = \left(\frac{1}{n} \sum_{a \in \mathbb{Z}_n} \omega^{ac} \right) W_{c,d} = \begin{cases} W_{c,d} & \text{if } c = 0 \\ 0 & \text{if } c \neq 0. \end{cases}$$

The discrete Weyl operators of the form $W_{c,d}$ for $c = 0$ span precisely the diagonal operators, so we see that this expression is consistent with the one involving the standard basis.

The channel Ω is known as the *completely depolarizing channel*, or the *maximally noisy channel*. We have

$$\Omega(W_{c,d}) = \frac{1}{n^2} \sum_{a,b \in \mathbb{Z}_n} W_{a,b} W_{c,d} W_{a,b}^* = \left(\frac{1}{n^2} \sum_{a,b \in \mathbb{Z}_n} \omega^{bc-ad} \right) W_{c,d} = \begin{cases} W_{c,d} & \text{if } (c,d) = (0,0) \\ 0 & \text{otherwise.} \end{cases}$$

The output is always a scalar multiple of $W_{0,0} = \mathbb{1}$. We may alternately write

$$\Omega(A) = \frac{\mathrm{Tr}(A)}{n} \mathbb{1}.$$

For every $\rho \in \mathrm{D}(\mathcal{X})$ we therefore have $\Omega(\rho) = \mathbb{1}/n$, which is the maximally mixed state: nothing but noise comes out of this channel.

6.3.3 Weyl covariant channels

The channels Δ and Ω above exhibit an interesting phenomenon, which is that the discrete Weyl operators are eigenvectors of them, in the sense that $\Delta(W_{a,b}) = \lambda_{a,b} W_{a,b}$ for some choice of $\{\lambda_{a,b}\} \subset \mathbb{C}$ (and likewise for Ω). This property holds for all channels given by convex combinations of unitary channels corresponding to the discrete Weyl operators. In general, channels of this form are called *Weyl covariant channels*. This can be demonstrated using the commutation relations noted above.

In greater detail, let us take $M \in \mathrm{L}\left(\mathbb{C}^{\mathbb{Z}_n}\right)$ to be any operator, and consider the mapping

$$\Phi(A) = \sum_{a,b \in \mathbb{Z}_n} M(a,b) W_{a,b} A W_{a,b}^*.$$

We have

$$\Phi(W_{c,d}) = \sum_{a,b\in\mathbb{Z}_n} M(a,b) W_{a,b} W_{c,d} W_{a,b}^* = \left(\sum_{a,b\in\mathbb{Z}_n} M(a,b)\omega^{bc-ad} \right) W_{c,d} = N(c,d) W_{c,d}$$

for

$$N(c,d) = \sum_{a,b\in\mathbb{Z}_n} M(a,b)\omega^{bc-ad}.$$

Alternately, we may write

$$N = V M^{\mathsf{T}} V^*,$$

where

$$V = \sum_{b,c\in\mathbb{Z}_n} \omega^{bc} E_{c,b}$$

is the operator typically associated with the *discrete Fourier transform*.

6.3.4 Teleportation

Suppose that X, $\mathsf{Y_A}$, and $\mathsf{Y_B}$ are registers, all having classical state set $\mathbb{Z}_n$ for some arbitrary choice of a positive integer n (such as $n = 8,675,309$, which is known as *Jenny's number*). Alice is holding X and $\mathsf{Y_A}$, while Bob has $\mathsf{Y_B}$. The pair $(\mathsf{Y_A}, \mathsf{Y_B})$ was long ago prepared in the pure state

$$\frac{1}{\sqrt{n}} \operatorname{vec}(\mathbb{1}) = \frac{1}{\sqrt{n}} \sum_{a\in\mathbb{Z}_n} e_a \otimes e_a,$$

while X was recently acquired by Alice. Alice wishes to *teleport* the state of X to Bob by sending him only classical information. To do this, Alice measures the pair $(\mathsf{X}, \mathsf{Y_A})$ with respect to the *generalized Bell basis*

$$\left\{ \frac{1}{\sqrt{n}} \operatorname{vec}(W_{a,b}) \,:\, (a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n \right\}. \tag{6.3}$$

She transmits to Bob whatever result $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ she obtains from her measurement, and Bob "corrects" $\mathsf{Y_B}$ by applying to it the unitary channel

$$\sigma \mapsto W_{a,b} \sigma W_{a,b}^*.$$

We may express this entire procedure as a channel from X to $\mathsf{Y_B}$, where the preparation of $(\mathsf{Y_A}, \mathsf{Y_B})$ is included in the description so that it makes sense to view $\mathsf{Y_B}$ as having been created in the procedure. This channel is given by

$$\Phi(\rho) = \frac{1}{n} \sum_{(a,b)\in\mathbb{Z}_n\times\mathbb{Z}_n} \left(\operatorname{vec}(W_{a,b})^* \otimes W_{a,b}\right) \left(\rho \otimes \frac{1}{n} \operatorname{vec}(\mathbb{1}) \operatorname{vec}(\mathbb{1})^* \right) \left(\operatorname{vec}(W_{a,b}) \otimes W_{a,b}^*\right).$$

To simplify this expression, it helps to note that

$$\operatorname{vec}(\mathbb{1}) \operatorname{vec}(\mathbb{1})^* = \frac{1}{n} \sum_{c,d} \overline{W_{c,d}} \otimes W_{c,d}.$$

We find that

$$\begin{aligned}
\Phi(W_{e,f}) &= \frac{1}{n^3} \sum_{a,b,c,d \in \mathbb{Z}_n} \left(\mathrm{vec}(W_{a,b})^* \otimes W_{a,b}\right) \left(W_{e,f} \otimes \overline{W_{c,d}} \otimes W_{c,d}\right) \left(\mathrm{vec}(W_{a,b}) \otimes W_{a,b}^*\right) \\
&= \frac{1}{n^3} \sum_{a,b,c,d \in \mathbb{Z}_n} \mathrm{Tr}\left(W_{a,b}^* W_{e,f} W_{a,b} W_{c,d}^*\right) W_{a,b} W_{c,d} W_{a,b}^* \\
&= \frac{1}{n^3} \sum_{a,b,c,d \in \mathbb{Z}_n} \left\langle W_{c,d}, W_{e,f} \right\rangle W_{c,d} \\
&= \frac{1}{n} \sum_{c,d \in \mathbb{Z}_n} \left\langle W_{c,d}, W_{e,f} \right\rangle W_{c,d} \\
&= W_{e,f}
\end{aligned}$$

for all $e, f \in \mathbb{Z}_n$. Thus, Φ is the identity channel—so the teleportation has worked as expected.

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

Lecture 7: Semidefinite programming

This lecture is on semidefinite programming, which is a powerful technique from both an analytic and computational point of view. It is not a technique that is specific to quantum information, and in fact there will be almost nothing in this lecture that directly concerns quantum information, but we will later see that it has several very interesting applications to quantum information theory.

7.1 Definition of semidefinite programs and related terminology

We begin with a formal definition of the notion of a semidefinite program. Various terms connected with semidefinite programs are also defined.

There are two points regarding the definition of semidefinite programs that you should be aware of. The first point is that it represents just one of several formalizations of the semidefinite programming concept, and for this reason definitions found in other sources may differ from the one found here. (The differing formalizations do, however, lead to a common theory.) The second point is that semidefinite programs to be found in applications of the concept are typically not phrased in the precise form presented by the definition: some amount of massaging may be required to fit the semidefinite program to the definition.

These two points are, of course, related in that they concern variations in the forms of semidefinite programs. This issue will be discussed in greater detail later in the lecture, where conversions of semidefinite programs from one form to another are discussed. For now, however, let us consider that semidefinite programs are as given by the definition below.

Before proceeding to the definition, we need to define one term: a mapping $\Phi \in \mathrm{T}(\mathcal{X}, Y)$ is *Hermiticity preserving* if it holds that $\Phi(X) \in \mathrm{Herm}(\mathcal{Y})$ for all choices of $X \in \mathrm{Herm}(\mathcal{X})$. (This condition happens to be equivalent to the three conditions that appear in the third question of Assignment 1.)

Definition 7.1. A semidefinite program is a triple (Φ, A, B), where

1. $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is a Hermiticity-preserving linear map, and
2. $A \in \mathrm{Herm}(\mathcal{X})$ and $B \in \mathrm{Herm}(\mathcal{Y})$ are Hermitian operators,

for some choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$.

We associate with the triple (Φ, A, B) two optimization problems, called the *primal* and *dual* problems, as follows:

Primal problem		Dual problem	
maximize:	$\langle A, X \rangle$	minimize:	$\langle B, Y \rangle$
subject to:	$\Phi(X) = B$,	subject to:	$\Phi^*(Y) \geq A$,
	$X \in \mathrm{Pos}(\mathcal{X})$.		$Y \in \mathrm{Herm}(\mathcal{Y})$.

The primal and dual problems have a special relationship to one another that will be discussed shortly.

An operator $X \in \mathrm{Pos}(\mathcal{X})$ satisfying $\Phi(X) = B$ is said to be *primal feasible*, and we let $\mathcal{A}$ denote the set of all such operators:

$$\mathcal{A} = \{X \in \mathrm{Pos}(\mathcal{X}) \,:\, \Phi(X) = B\}.$$

Following a similar terminology for the dual problem, an operator $Y \in \mathrm{Herm}(\mathcal{Y})$ satisfying $\Phi^*(Y) \geq A$ is said to be *dual feasible*, and we let $\mathcal{B}$ denote the set of all dual feasible operators:

$$\mathcal{B} = \{Y \in \mathrm{Herm}(\mathcal{Y}) \,:\, \Phi^*(Y) \geq A\}.$$

The linear functions $X \mapsto \langle A, X\rangle$ and $Y \mapsto \langle B, Y\rangle$ are referred to as the primal and dual *objective functions*. The *primal optimum* or *optimal primal value* of a semidefinite program is defined as

$$\alpha = \sup_{X \in \mathcal{A}} \langle A, X\rangle$$

and the *dual optimum* or *optimal dual value* is defined as

$$\beta = \inf_{Y \in \mathcal{B}} \langle B, Y\rangle.$$

The values α and β may be finite or infinite, and by convention we define $\alpha = -\infty$ if $\mathcal{A} = \varnothing$ and $\beta = \infty$ if $B = \varnothing$. If an operator $X \in \mathcal{A}$ satisfies $\langle A, X\rangle = \alpha$ we say that X is an *optimal primal solution*, or that X *achieves* the optimal primal value. Likewise, if $Y \in \mathcal{B}$ satisfies $\langle B, Y\rangle = \beta$ then we say that Y is an *optimal dual solution*, or that Y achieves the optimal dual value.

Example 7.2. A simple example of a semidefinite program may be obtained, for an arbitrary choice of a complex Euclidean space $\mathcal{X}$ and a Hermitian operator $A \in \mathrm{Herm}(\mathcal{X})$, by taking $\mathcal{Y} = \mathbb{C}$, $B = 1$, and $\Phi(X) = \mathrm{Tr}(X)$ for all $X \in \mathrm{L}(\mathcal{X})$. The primal and dual problems associated with this semidefinite program are as follows:

Primal problem		Dual problem	
maximize:	$\langle A, X\rangle$	minimize:	y
subject to:	$\mathrm{Tr}(X) = 1,$	subject to:	$y\mathbb{1} \geq A,$
	$X \in \mathrm{Pos}(\mathcal{X}).$		$y \in \mathbb{R}.$

To see that the dual problem is as stated, we note that $\mathrm{Herm}(\mathcal{Y}) = \mathbb{R}$ and that the adjoint mapping to the trace is given by $\mathrm{Tr}^*(y) = y\mathbb{1}$ for all $y \in \mathbb{C}$. The optimal primal and dual values α and β happen to be equal (which is not unexpected, as we will soon see), coinciding with the largest eigenvalue $\lambda_1(A)$ of A.

There can obviously be no optimal primal solution to a semidefinite program when α is infinite, and no optimal dual solution when β is infinite. Even in cases where α and β are finite, however, there may not exist optimal primal and/or optimal dual solutions, as the following example illustrates.

Example 7.3. Let $\mathcal{X} = \mathbb{C}^2$ and $\mathcal{Y} = \mathbb{C}^2$, and define $A \in \mathrm{Herm}(\mathcal{X})$, $B \in \mathrm{Herm}(\mathcal{Y})$, and $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ as

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \Phi(X) = \begin{pmatrix} 0 & X(1,2) \\ X(2,1) & 0 \end{pmatrix}$$

for all $X \in \mathrm{L}(\mathcal{X})$. It holds that $\alpha = 0$, but there does not exist an optimal primal solution to (Φ, A, B).

To establish this fact, suppose first that $X \in \mathrm{Pos}(\mathcal{X})$ is primal-feasible. The condition $\Phi(X) = B$ implies that X takes the form

$$X = \begin{pmatrix} X(1,1) & 1 \\ 1 & X(2,2) \end{pmatrix} \tag{7.1}$$

Given that X is positive semidefinite, it must hold that $X(1,1) \geq 0$ and $X(2,2) \geq 0$, because the diagonal entries of positive semidefinite operators are always nonnegative. Moreover, $\mathrm{Det}(X) = X(1,1)X(2,2) - 1$, and given that the determinant of every positive semidefinite operator is nonnegative it follows that $X(1,1)X(2,2) \geq 1$. It must therefore be the case that $X(1,1) > 0$, so that $\langle A, X \rangle < 0$. On the other hand, one may consider the operator

$$X_n = \begin{pmatrix} \frac{1}{n} & 1 \\ 1 & n \end{pmatrix}$$

for each positive integer n. It holds that $X_n \in \mathcal{A}$ and $\langle A, X_n \rangle = -1/n$, and therefore $\alpha \geq -1/n$, for every positive integer n. Consequently one has that $\alpha = 0$, while no primal-feasible X achieves this supremum value.

7.2 Duality

We will now discuss the special relationship between the primal and dual problems associated with a semidefinite program, known as *duality*. A study of this relationship begins with *weak duality*, which simply states that $\alpha \leq \beta$ for every semidefinite program.

Proposition 7.4 (Weak duality for semidefinite programs)**.** *For every semidefinite program (Φ, A, B) it holds that $\alpha \leq \beta$.*

Proof. The proposition is trivial in case $\mathcal{A} = \varnothing$ (which implies $\alpha = -\infty$) or $\mathcal{B} = \varnothing$ (which implies $\beta = \infty$), so we will restrict our attention to the case that both $\mathcal{A}$ and $\mathcal{B}$ are nonempty. For every primal feasible $X \in \mathcal{A}$ and dual feasible $Y \in \mathcal{B}$ it holds that

$$\langle A, X \rangle \leq \langle \Phi^*(Y), X \rangle = \langle Y, \Phi(X) \rangle = \langle Y, B \rangle = \langle B, Y \rangle .$$

Taking the supremum over all $X \in \mathcal{A}$ and the infimum over all $Y \in \mathcal{B}$ establishes that $\alpha \leq \beta$ as required. □

One implication of weak duality is that every dual-feasible operator $Y \in \mathcal{B}$ establishes an upper bound of $\langle B, Y \rangle$ on the optimal primal value α, and therefore an upper bound on $\langle A, X \rangle$ for every primal-feasible operator $X \in \mathcal{A}$. Likewise, every primal-feasible operator $X \in \mathcal{A}$ establishes a lower-bound of $\langle A, X \rangle$ on the optimal dual value β. In other words, it holds that

$$\langle A, X \rangle \leq \alpha \leq \beta \leq \langle B, Y \rangle ,$$

for every $X \in \mathcal{A}$ and $Y \in \mathcal{B}$. If one finds a primal-feasible operator $X \in \mathcal{A}$ and a dual-feasible operator $Y \in \mathcal{B}$ for which $\langle A, X \rangle = \langle B, Y \rangle$, it therefore follows that $\alpha = \beta$ and both X and Y must be optimal: $\alpha = \langle A, X \rangle$ and $\beta = \langle B, Y \rangle$.

The condition that $\alpha = \beta$ is known as *strong duality*. Unlike weak duality, strong duality does not hold for every semidefinite program, as the following example shows.

Example 7.5. Let $\mathcal{X} = \mathbb{C}^3$ and $\mathcal{Y} = \mathbb{C}^2$, and define

$$A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{and} \quad \Phi(X) = \begin{pmatrix} X(1,1) + X(2,3) + X(3,2) & 0 \\ 0 & X(2,2) \end{pmatrix}$$

for all $X \in \mathrm{L}(\mathcal{X})$. The mapping Φ is Hermiticity-preserving and A and B are Hermitian, so (Φ, A, B) is a semidefinite program.

The primal problem associated with the semidefinite program (Φ, A, B) represents a maximization of $-X(1,1)$ subject to the constraints $X(1,1) + X(2,3) + X(3,2) = 1$, $X(2,2) = 0$, and $X \geq 0$. The constraints $X(2,2) = 0$ and $X \geq 0$ force the equality $X(2,3) = X(3,2) = 0$. It must therefore hold that $X(1,1) = 1$, so $\alpha \leq -1$. The fact that $\alpha = -1$, as opposed to $\alpha = -\infty$, is established by considering the primal feasible operator $X = E_{1,1}$.

To analyze the dual problem, we begin by noting that

$$\Phi^*(Y) = \begin{pmatrix} Y(1,1) & 0 & 0 \\ 0 & Y(2,2) & Y(1,1) \\ 0 & Y(1,1) & 0 \end{pmatrix}.$$

The constraint $\Phi^*(Y) \geq A$ implies that

$$\begin{pmatrix} Y(2,2) & Y(1,1) \\ Y(1,1) & 0 \end{pmatrix} \geq 0,$$

so that $Y(1,1) = 0$, and therefore $\beta \geq 0$. The fact that $\beta = 0$ is established by choosing the dual feasible operator $Y = 0$.

Thus, strong duality fails for this semidefinite program: it holds that $\alpha = -1$ while $\beta = 0$.

While strong duality does not hold for every semidefinite program, it does typically hold for semidefinite programs that arise in applications of the concept. Informally speaking, if one does not *try* to make strong duality fail, it will probably hold. There are various conditions on semidefinite programs that allow for an easy verification that strong duality holds (when it does), with one of the most useful conditions being given by the following theorem.

Theorem 7.6 (Slater's theorem for semidefinite programs)**.** *The following implications hold for every semidefinite program (Φ, A, B).*

1. *If $\mathcal{A} \neq \varnothing$ and there exists a Hermitian operator Y for which $\Phi^*(Y) > A$, then $\alpha = \beta$ and there exists a primal feasible operator $X \in \mathcal{A}$ for which $\langle A, X \rangle = \alpha$.*
2. *If $\mathcal{B} \neq \varnothing$ and there exists a positive semidefinite operator X for which $\Phi(X) = B$ and $X > 0$, then $\alpha = \beta$ and there exists a dual feasible operator $Y \in \mathcal{B}$ for which $\langle B, Y \rangle = \beta$.*

(The condition that $X \in \mathrm{Pd}(\mathcal{X})$ satisfies $\Phi(X) = B$ is called *strict primal feasibility*, while the condition that $Y \in \mathrm{Herm}(\mathcal{Y})$ satisfies $\Phi^*(Y) > A$ is called *strict dual feasibility*. In both cases, the "strictness" concerns the positive semidefinite ordering.)

There are two main ideas behind the proof of this theorem, and the proof (of each of the two implications) splits into two parts based on the two ideas. The ideas are as follows.

1. By the hyperplane separation theorem stated in the notes for Lecture 2, every closed convex set can be separated from any point not in that set by a hyperplane.

2. Linear mappings do not always map closed convex sets to closed sets, but under some conditions they do.

We will not prove the hyperplane separation theorem: you can find a proof in one of the references given in Lecture 2. That theorem is stated for a real Euclidean space of the form $\mathbb{R}^{\Sigma}$, but we will apply it to the space of Hermitian operators $\mathrm{Herm}\left(\mathbb{C}^{\Gamma}\right)$ for some finite and nonempty set Γ. As we have already noted more than once, we may view $\mathrm{Herm}\left(\mathbb{C}^{\Gamma}\right)$ as being isomorphic to $\mathbb{R}^{\Gamma\times\Gamma}$ as a real Euclidean space.

The second idea is quite vague as it has been stated above, so let us now state it more precisely as a lemma.

Lemma 7.7. *Let Σ and Γ be finite, nonempty sets, let $\Psi : \mathbb{R}^{\Sigma} \to \mathbb{R}^{\Gamma}$ be a linear mapping, and let $\mathcal{P} \subseteq \mathbb{R}^{\Sigma}$ be a closed convex cone possessing the property that $\ker(\Psi) \cap \mathcal{P}$ is a linear subspace of $\mathbb{R}^{\Sigma}$. It holds that $\Psi(\mathcal{P})$ is closed.*

To prove this lemma, we will make use of the following simple proposition, which we will take as given. It is straightforward to prove using basic concepts from analysis.

Proposition 7.8. *Let Σ be a finite and nonempty set and let $\mathcal{S} \subset \mathbb{R}^{\Sigma}$ be a compact subset of $\mathbb{R}^{\Sigma}$ such that $0 \notin \mathcal{S}$. It holds that $\mathrm{cone}(\mathcal{S}) \triangleq \{\lambda v : v \in \mathcal{S}, \lambda \geq 0\}$ is closed.*

Proof of Lemma 7.7. First we consider the special case that $\ker(\Psi) \cap \mathcal{P} = \{0\}$. Let

$$\mathcal{R} = \{v \in \mathcal{P} : \|v\| = 1\}.$$

It holds that $\mathcal{P} = \mathrm{cone}(\mathcal{R})$ and therefore $\Psi(\mathcal{P}) = \mathrm{cone}(\Psi(\mathcal{R}))$. The set $\mathcal{R}$ is compact, and therefore $\Psi(\mathcal{R})$ is compact as well. Moreover, it holds that $0 \notin \Psi(\mathcal{R})$, for otherwise there would exist a unit norm (and therefore nonzero) vector $v \in \mathcal{P}$ for which $\Psi(v) = 0$, contradicting the assumption that $\ker(\Psi) \cap \mathcal{P} = \{0\}$. It follows from Proposition 7.8 that $\Psi(\mathcal{P})$ is closed.

For the general case, let us denote $\mathcal{V} = \ker(\Psi) \cap \mathcal{P}$, and define $\mathcal{Q} = \mathcal{P} \cap \mathcal{V}^{\perp}$. It holds that $\mathcal{Q}$ is a closed convex cone, and $\ker(\Psi) \cap \mathcal{Q} = \mathcal{V} \cap \mathcal{V}^{\perp} = \{0\}$. We therefore have that $\Psi(\mathcal{Q})$ is closed by the analysis of the special case above. It remains to prove that $\Psi(\mathcal{Q}) = \Psi(\mathcal{P})$. To this end, choose $u \in \mathcal{P}$, and write $u = v + w$ for $v \in \mathcal{V}$ and $w \in \mathcal{V}^{\perp}$. Given that $\mathcal{V} \subseteq \mathcal{P}$ and $\mathcal{P}$ is a convex cone, it follows that $\mathcal{P} + \mathcal{V} = \mathcal{P}$, so $w = u - v \in \mathcal{P} + \mathcal{V} = \mathcal{P}$. Consequently $w \in \mathcal{Q}$. As $\Psi(w) = \Psi(u) - \Psi(v) = \Psi(u)$, we conclude that $\Psi(\mathcal{P}) \subseteq \Psi(\mathcal{Q})$. The reverse containment $\Psi(\mathcal{Q}) \subseteq \Psi(\mathcal{P})$ is trivial, and so we have proved $\Psi(\mathcal{P}) = \Psi(\mathcal{Q})$ as required. □

Now we are ready to prove Theorem 7.6. The two implications are proved in the same basic way, although there are technical differences in the proofs. Each implication is split into two lemmas, along the lines suggested above, which combine in a straightforward way to prove the theorem.

Lemma 7.9. *Let (Φ, A, B) be a semidefinite program. If $\mathcal{A} \neq \varnothing$ and the set*

$$\mathcal{K} = \left\{ \begin{pmatrix} \Phi(X) & 0 \\ 0 & \langle A, X\rangle \end{pmatrix} : X \in \mathrm{Pos}\left(\mathcal{X}\right) \right\} \subseteq \mathrm{Herm}\left(\mathcal{Y} \oplus \mathbb{C}\right)$$

is closed, then $\alpha = \beta$ and there exists a primal feasible operator $X \in \mathcal{A}$ such that $\langle A, X\rangle = \alpha$.

Proof. Let $\varepsilon > 0$ be chosen arbitrarily. Observe that the operator

$$\begin{pmatrix} B & 0 \\ 0 & \alpha + \varepsilon \end{pmatrix} \tag{7.2}$$

is not contained in $\mathcal{K}$, for there would otherwise exist an operator $X \in \mathrm{Pos}(\mathcal{X})$ with $\Phi(X) = B$ and $\langle A, X \rangle > \alpha$, contradicting the optimality of α. The set $\mathcal{K}$ is convex and (by assumption) closed, and therefore there must exist a hyperplane that separates the operator (7.2) from $\mathcal{K}$ in the sense prescribed by Theorem 2.8 of Lecture 2. It follows that there must exist an operator $Y \in \mathrm{Herm}(\mathcal{Y})$ and a real number λ such that

$$\langle Y, \Phi(X) \rangle + \lambda \langle A, X \rangle > \langle Y, B \rangle + \lambda(\alpha + \varepsilon) \tag{7.3}$$

for all $X \in \mathrm{Pos}(\mathcal{X})$.

The set $\mathcal{A}$ has been assumed to be nonempty, so one may select an operator $X_0 \in \mathcal{A}$. As $\Phi(X_0) = B$, we conclude from (7.3) that

$$\lambda \langle A, X_0 \rangle > \lambda(\alpha + \varepsilon),$$

and therefore $\lambda < 0$. By dividing both sides of (7.3) by $|\lambda|$ and renaming variables, we see that there is no loss of generality in assuming that $\lambda = -1$. Substituting $\lambda = -1$ into (7.3) yields

$$\langle \Phi^*(Y) - A, X \rangle > \langle Y, B \rangle - (\alpha + \varepsilon) \tag{7.4}$$

for every $X \in \mathrm{Pos}(\mathcal{X})$. The quantity on the right-hand-side of this inequality is a real number independent of X, which implies that $\Phi^*(Y) - A$ must be positive semidefinite; for if it were not, one could choose X appropriately to make the quantity on the left-hand-side smaller than $\langle Y, B \rangle - (\alpha + \varepsilon)$ (or any other fixed real number independent of X). It therefore holds that

$$\Phi^*(Y) \geq A,$$

so that Y is a dual-feasible operator. Setting $X = 0$ in (7.4) yields $\langle B, Y \rangle < \alpha + \varepsilon$. It has therefore been shown that for every $\varepsilon > 0$ there exists a dual feasible operator $Y \in \mathcal{B}$ such that $\langle B, Y \rangle < \alpha + \varepsilon$. This implies that $\alpha \leq \beta < \alpha + \varepsilon$ for every $\varepsilon > 0$, from which it follows that $\alpha = \beta$ as claimed.

To prove the second part of the lemma, a similar methodology to the first part of the proof is used, except that ε is set to 0. More specifically, we consider whether the operator

$$\begin{pmatrix} B & 0 \\ 0 & \alpha \end{pmatrix} \tag{7.5}$$

is contained in $\mathcal{K}$. If this operator is in $\mathcal{K}$, then there exists an operator $X \in \mathrm{Pos}(\mathcal{X})$ such that $\Phi(X) = B$ and $\langle A, X \rangle = \alpha$, which is the statement claimed by the lemma.

It therefore suffices to derive a contradiction from the assumption that the operator (7.5) is not contained in $\mathcal{K}$. Under this assumption, there must exist a Hermitian operator $Y \in \mathrm{Herm}(\mathcal{Y})$ and a real number λ such that

$$\langle Y, \Phi(X) \rangle + \lambda \langle A, X \rangle > \langle Y, B \rangle + \lambda\alpha \tag{7.6}$$

for all $X \in \mathrm{Pos}(\mathcal{X})$. As before, one concludes from the existence of a primal feasible operator X_0 that $\lambda < 0$, so there is again no loss of generality in assuming that λ and Y are re-scaled so that $\lambda = -1$. After this re-scaling, one finds that

$$\langle \Phi^*(Y) - A, X \rangle > \langle Y, B \rangle - \alpha \tag{7.7}$$

for every $X \in \mathrm{Pos}(\mathcal{X})$, and therefore $\Phi^*(Y) \geq A$ (i.e., Y is dual-feasible). Setting $X = 0$ in (7.7) implies $\langle Y, B \rangle < \alpha$. This, however, implies $\beta < \alpha$, which is in contradiction with weak duality. It follows that the operator (7.5) is contained in $\mathcal{K}$ as required. □

Lemma 7.10. *Let (Φ, A, B) be a semidefinite program. If there exists an operator $Y \in \mathrm{Herm}(\mathcal{Y})$ for which $\Phi^*(Y) > A$, then the set*

$$\mathcal{K} = \left\{ \begin{pmatrix} \Phi(X) & 0 \\ 0 & \langle A, X \rangle \end{pmatrix} \,:\, X \in \mathrm{Pos}(\mathcal{X}) \right\} \subseteq \mathrm{Herm}(\mathcal{Y} \oplus \mathbb{C})$$

is closed.

Proof. The set $\mathrm{Pos}(\mathcal{X})$ is a closed convex cone, and $\mathcal{K}$ is the image of this set under the linear mapping

$$\Psi(X) = \begin{pmatrix} \Phi(X) & 0 \\ 0 & \langle A, X \rangle \end{pmatrix}.$$

If $X \in \ker(\Psi)$, then $\Phi(X) = 0$ and $\langle A, X \rangle = 0$, and therefore

$$\langle \Phi^*(Y) - A, X \rangle = \langle Y, \Phi(X) \rangle - \langle A, X \rangle = 0.$$

If, in addition, it holds that $X \geq 0$, then $X = 0$ given that $\Phi^*(Y) - A > 0$. Thus, $\ker(\Psi) \cap \mathrm{Pos}(\mathcal{X}) = \{0\}$, so $\mathcal{K}$ is closed by Lemma 7.7. □

The two lemmas above together imply that the first implication of Theorem 7.6 holds. The second implication is proved by combining the following two lemmas, which are closely related to the two lemmas just proved.

Lemma 7.11. *Let (Φ, A, B) be a semidefinite program. If $\mathcal{B} \neq \varnothing$ and the set*

$$\mathcal{L} = \left\{ \begin{pmatrix} \Phi^*(Y) - Z & 0 \\ 0 & \langle B, Y \rangle \end{pmatrix} \,:\, Y \in \mathrm{Herm}(\mathcal{Y}),\, Z \in \mathrm{Pos}(\mathcal{X}) \right\} \subseteq \mathrm{Herm}(\mathcal{X} \oplus \mathbb{C})$$

is closed, then $\alpha = \beta$ and there exists a dual feasible operator $Y \in \mathcal{B}$ such that $\langle B, Y \rangle = \beta$.

Proof. Let $\varepsilon > 0$ be chosen arbitrarily. Along similar lines to the proof of Lemma 7.9, one observes that the operator

$$\begin{pmatrix} A & 0 \\ 0 & \beta - \varepsilon \end{pmatrix} \tag{7.8}$$

is not contained in $\mathcal{L}$; for if it were, there would exist an operator $Y \in \mathrm{Herm}(\mathcal{Y})$ with $\Phi^*(Y) \geq A$ and $\langle B, Y \rangle < \beta$, contradicting the optimality of β. As the set $\mathcal{L}$ is closed (by assumption) and is convex, there must exist a hyperplane that separates the operator (7.8) from $\mathcal{L}$; that is, there must exist a real number λ and an operator $X \in \mathrm{Herm}(\mathcal{X})$ such that

$$\langle X, \Phi^*(Y) - Z \rangle + \lambda \langle B, Y \rangle < \langle X, A \rangle + \lambda(\beta - \varepsilon) \tag{7.9}$$

for all $Y \in \mathrm{Herm}(\mathcal{Y})$ and $Z \in \mathrm{Pos}(\mathcal{X})$.

The set $\mathcal{B}$ has been assumed to be nonempty, so one may select a operator $Y_0 \in \mathcal{B}$. It holds that $\Phi^*(Y_0) \geq A$, and setting $Z = \Phi^*(Y_0) - A$ in (7.9) yields

$$\lambda \langle B, Y_0 \rangle < \lambda(\beta - \varepsilon),$$

implying $\lambda < 0$. There is therefore no loss of generality in re-scaling λ and X in (7.9) so that $\lambda = -1$, which yields

$$\langle \Phi(X) - B, Y \rangle < \langle X, A + Z \rangle - (\beta - \varepsilon) \tag{7.10}$$

for every $Y \in \mathrm{Herm}(\mathcal{Y})$ and $Z \in \mathrm{Pos}(\mathcal{X})$. The quantity on the right-hand-side of this inequality is a real number independent of Y, which implies that $\Phi(X) = B$; for if this were not so, one could choose a Hermitian operator $Y \in \mathrm{Herm}(\mathcal{Y})$ appropriately to make the quantity on the left-hand-side larger than $\langle X, A + Z \rangle - (\beta - \varepsilon)$ (or any other real number independent of Y). It therefore holds that X is a primal-feasible operator. Setting $Y = 0$ and $Z = 0$ in (7.10) yields $\langle A, X \rangle > \beta - \varepsilon$. It has therefore been shown that for every $\varepsilon > 0$ there exists a primal feasible operator $X \in \mathcal{A}$ such that $\langle A, X \rangle > \beta - \varepsilon$. This implies $\beta \geq \alpha > \beta - \varepsilon$ for every $\varepsilon > 0$, and therefore $\alpha = \beta$ as claimed.

To prove the second part of the lemma, we may again use essentially the same methodology as for the first part, but setting $\varepsilon = 0$. That is, we consider whether the operator

$$\begin{pmatrix} A & 0 \\ 0 & \beta \end{pmatrix} \tag{7.11}$$

is in $\mathcal{L}$. If so, there exists an operator $Y \in \mathrm{Herm}(\mathcal{Y})$ for which $\Phi^*(Y) - Z = A$ for some $Z \in \mathrm{Pos}(\mathcal{X})$ (i.e., for which $\Phi^*(Y) \geq A$) and for which $\langle B, Y \rangle = \beta$, which is the statement we aim to prove.

It therefore suffices to derive a contradiction from the assumption the operator (7.11) is not in $\mathcal{L}$. Under this assumption, there must exist a real number λ and a Hermitian operator $X \in \mathrm{Herm}(\mathcal{X})$ such that

$$\langle X, \Phi^*(Y) - Z \rangle + \lambda \langle B, Y \rangle < \langle X, A \rangle + \lambda\beta \tag{7.12}$$

for all $Y \in \mathrm{Herm}(\mathcal{Y})$ and $Z \in \mathrm{Pos}(\mathcal{X})$. We conclude, as before, that it must hold that $\lambda < 0$, and so there is no loss of generality in assuming $\lambda = -1$. Moreover, we have

$$\langle \Phi(X) - B, Y \rangle < \langle X, A + Z \rangle - \beta$$

for every $Y \in \mathrm{Herm}(\mathcal{Y})$ and $Z \in \mathrm{Pos}(\mathcal{X})$, and therefore $\Phi(X) = B$. Finally, taking $Y = 0$ and $Z = 0$ implies $\langle A, X \rangle > \beta$. This, however, implies $\alpha > \beta$, which is in contradiction with weak duality. It follows that the operator (7.11) is contained in $\mathcal{L}$ as required. □

Lemma 7.12. *Let (Φ, A, B) be a semidefinite program. If there exists a operator $X \in \mathrm{Pos}(\mathcal{X})$ for which $\Phi(X) = B$ and $X > 0$, then the set*

$$\mathcal{L} = \left\{ \begin{pmatrix} \Phi^*(Y) - Z & 0 \\ 0 & \langle B, Y \rangle \end{pmatrix} : Y \in \mathrm{Herm}(\mathcal{Y}),\, Z \in \mathrm{Pos}(\mathcal{X}) \right\} \subseteq \mathrm{Herm}(\mathcal{X} \oplus \mathbb{C})$$

is closed.

Proof. The set

$$\mathcal{P} = \left\{ \begin{pmatrix} Y & 0 \\ 0 & Z \end{pmatrix} \,:\, Y \in \mathrm{Herm}\,(\mathcal{Y})\,,\, Z \in \mathrm{Pos}\,(\mathcal{X}) \right\}$$

is a closed, convex cone. For the linear map

$$\Psi \begin{pmatrix} Y & \cdot \\ \cdot & Z \end{pmatrix} = \begin{pmatrix} \Phi^*(Y) - Z & 0 \\ 0 & \langle B, Y \rangle \end{pmatrix}$$

it holds that $\mathcal{L} = \Psi(\mathcal{P})$.

Suppose that

$$\begin{pmatrix} Y & 0 \\ 0 & Z \end{pmatrix} \in \ker(\Psi) \cap \mathcal{P}.$$

It must then hold that

$$0 = \langle B, Y \rangle - \langle X, \Phi^*(Y) - Z \rangle = \langle B - \Phi(X), Y \rangle + \langle X, Z \rangle = \langle X, Z \rangle\,,$$

for X being the positive definite operator assumed by the statement of the lemma, implying that $Z = 0$. It follows that

$$\ker(\Psi) \cap \mathcal{P} = \left\{ \begin{pmatrix} Y & 0 \\ 0 & 0 \end{pmatrix} \,:\, Y \in \{B\}^{\perp} \cap \ker(\Phi^*) \right\},$$

which is a linear subspace of $\mathrm{Herm}\,(\mathcal{Y} \oplus \mathcal{X})$. It follows that $\mathcal{L}$ is closed by Lemma 7.7. □

7.3 Alternate forms of semidefinite programs

As was mentioned earlier in the lecture, semidefinite programs can be specified in ways that differ from the formal definition we have been considering thus far in the lecture. A few such ways will now be discussed.

7.3.1 Semidefinite programs with inequality constraints

Suppose $\Phi \in \mathrm{T}\,(\mathcal{X}, \mathcal{Y})$ is a Hermiticity-preserving map and $A \in \mathrm{Herm}\,(\mathcal{X})$ and $B \in \mathrm{Herm}\,(\mathcal{Y})$ are Hermitian operators, and consider this optimization problem:

$$\begin{aligned} \text{maximize:} \quad & \langle A, X \rangle \\ \text{subject to:} \quad & \Phi(X) \leq B, \\ & X \in \mathrm{Pos}\,(\mathcal{X})\,. \end{aligned}$$

It is different from the primal problem associated with the triple (Φ, A, B) earlier in the lecture because the constraint $\Phi(X) = B$ has been replaced with $\Phi(X) \leq B$. There is now more freedom in the valid choices of $X \in \mathrm{Pos}\,(\mathcal{X})$ in this problem, so its optimum value may potentially be larger.

It is not difficult, however, to phrase the problem above using an equality constraint by using a so-called *slack variable*. That is, the inequality constraint

$$\Phi(X) \leq B$$

is equivalent to the equality constraint

$$\Phi(X) + Z = B \qquad (\text{for some } Z \in \mathrm{Pos}(\mathcal{Y})).$$

With this in mind, let us define a new semidefinite program, by which we mean something that conforms to the precise definition given at the beginning of the lecture, as follows. First, let $\Psi \in \mathrm{T}(\mathcal{X} \oplus \mathcal{Y}, \mathcal{Y})$ be defined as

$$\Psi \begin{pmatrix} X & \cdot \\ \cdot & Z \end{pmatrix} = \Phi(X) + Z$$

for all $X \in \mathrm{L}(\mathcal{X})$ and $Z \in \mathrm{L}(\mathcal{Y})$. (The dots indicate elements of $\mathrm{L}(\mathcal{X}, \mathcal{Y})$ and $\mathrm{L}(\mathcal{Y}, \mathcal{X})$ that we don't care about, because they don't influence the output of the mapping Ψ.) Also define $C \in \mathrm{Herm}(\mathcal{X} \oplus \mathcal{Y})$ as

$$C = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}.$$

The primal and dual problems associated with the semidefinite program (Ψ, C, B) are as follows.

Primal problem

$$\begin{aligned} \text{maximize:} \quad & \left\langle \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} X & \cdot \\ \cdot & Z \end{pmatrix} \right\rangle \\ \text{subject to:} \quad & \Psi \begin{pmatrix} X & \cdot \\ \cdot & Z \end{pmatrix} = B, \\ & \begin{pmatrix} X & \cdot \\ \cdot & Z \end{pmatrix} \in \mathrm{Pos}(\mathcal{X} \oplus \mathcal{Y}). \end{aligned}$$

Dual problem

$$\begin{aligned} \text{minimize:} \quad & \langle B, Y \rangle \\ \text{subject to:} \quad & \Psi^*(Y) \geq \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}, \\ & Y \in \mathrm{Herm}(\mathcal{Y}). \end{aligned}$$

Once again, we are using dots to represent operators we don't care about. The fact that we don't care about these operators in this case is a combination of the fact that Ψ is independent of them and the fact that the objective function is independent of them as well. (Had we made a different choice of C, this might not be so.)

The primal problem simplifies to the problem originally posed above. To simplify the dual problem, we must first calculate Ψ^*. It is given by

$$\Psi^*(Y) = \begin{pmatrix} \Phi^*(Y) & 0 \\ 0 & Y \end{pmatrix}.$$

To verify that this is so, we simply check the required condition:

$$\left\langle \begin{pmatrix} X & W \\ V & Z \end{pmatrix}, \Psi^*(Y) \right\rangle = \langle X, \Phi^*(Y) \rangle + \langle Z, Y \rangle = \langle \Phi(X) + Z, Y \rangle = \left\langle \Psi \begin{pmatrix} X & W \\ V & Z \end{pmatrix}, Y \right\rangle,$$

for all $X \in \mathrm{L}(\mathcal{X})$, $Y, Z \in \mathrm{L}(\mathcal{Y})$, $V \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$, and $W \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$. This condition uniquely determines Ψ^*, so we know we have it right. The inequality

$$\begin{pmatrix} \Phi^*(Y) & 0 \\ 0 & Y \end{pmatrix} \geq \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix},$$

for $Y \in \mathrm{Herm}(\mathcal{Y})$, is equivalent to $\Phi^*(Y) \geq A$ and $Y \geq 0$ (i.e., $Y \in \mathrm{Pos}(\mathcal{Y})$). So, we may simplify the problems above so that they look like this:

Primal problem		Dual problem	
maximize:	$\langle A, X \rangle$	minimize:	$\langle B, Y \rangle$
subject to:	$\Phi(X) \leq B,$	subject to:	$\Phi^*(Y) \geq A,$
	$X \in \mathrm{Pos}(\mathcal{X}).$		$Y \in \mathrm{Pos}(\mathcal{Y}).$

This is an attractive form, because the primal and dual problems have a nice symmetry between them.

Note that we could equally well convert a primal problem having an equality constraint into one with an inequality constraint, by using the simple fact that $\Phi(X) = B$ if and only if

$$\begin{pmatrix} \Phi(X) & 0 \\ 0 & -\Phi(X) \end{pmatrix} \leq \begin{pmatrix} B & 0 \\ 0 & -B \end{pmatrix}.$$

So, it would have been alright had we initially defined the primal and dual problems associated with (Φ, A, B) to be the ones with inequality constraints as just discussed: one can convert back and forth between the two forms. (Note, however, that we are better off with Slater's theorem for semidefinite programs with equality constraints than we would be for a similar theorem for inequality constraints, which is why we have elected to start with equality constraints.)

7.3.2 Equality and inequality constraints

It is sometimes convenient to consider semidefinite programming problems that include both equality and inequality constraints, as opposed to just one type. To be more precise, let $\mathcal{X}$, $\mathcal{Y}_1$, and $\mathcal{Y}_2$ be complex Euclidean spaces, let $\Phi_1 : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}_1)$ and $\Phi_2 : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}_2)$ be Hermiticity-preserving maps, let $A \in \mathrm{Herm}(\mathcal{X})$, $B_1 \in \mathrm{Herm}(\mathcal{Y}_1)$, and $B_2 \in \mathrm{Herm}(\mathcal{Y}_2)$ be Hermitian operators, and consider these optimization problems:

Primal problem		Dual problem	
maximize:	$\langle A, X \rangle$	minimize:	$\langle B_1, Y_1 \rangle + \langle B_2, Y_2 \rangle$
subject to:	$\Phi_1(X) = B_1,$	subject to:	$\Phi_1^*(Y_1) + \Phi_2^*(Y_2) \geq A,$
	$\Phi_2(X) \leq B_2,$		$Y_1 \in \mathrm{Herm}(\mathcal{Y}_1),$
	$X \in \mathrm{Pos}(\mathcal{X}).$		$Y_2 \in \mathrm{Pos}(\mathcal{Y}_2).$

The fact that these problems really are dual may be verified in a similar way to the discussion of inequality constraints in the previous subsection. Specifically, one may define a linear mapping

$$\Psi : \mathrm{Herm}(\mathcal{X} \oplus \mathcal{Y}_2) \to \mathrm{Herm}(\mathcal{Y}_1 \oplus \mathcal{Y}_2)$$

as

$$\Psi \begin{pmatrix} X & \cdot \\ \cdot & Z \end{pmatrix} = \begin{pmatrix} \Phi_1(X) & 0 \\ 0 & \Phi_2(X) + Z \end{pmatrix}$$

for all $X \in \mathrm{L}(\mathcal{X})$ and $Z \in \mathrm{L}(\mathcal{Y}_2)$, and define Hermitian operators $C \in \mathrm{Herm}(\mathcal{X} \oplus \mathcal{Y}_2)$ and $D \in \mathrm{Herm}(\mathcal{Y}_1 \oplus \mathcal{Y}_2)$ as

$$C = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad D = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}.$$

The primal problem above is equivalent to the primal problem associated with the semidefinite program (Ψ, C, D). The dual problem above coincides with the dual problem of (Ψ, C, D), by virtue of the fact that

$$\Psi^* \begin{pmatrix} Y_1 & \cdot \\ \cdot & Y_2 \end{pmatrix} = \begin{pmatrix} \Phi_1^*(Y_1) + \Phi_2^*(Y_2) & 0 \\ 0 & Y_2 \end{pmatrix}$$

for every $Y_1 \in \mathrm{Herm}(\mathcal{Y}_1)$ and $Y_2 \in \mathrm{Herm}(\mathcal{Y}_2)$.

Note that strict primal feasibility of (Ψ, C, D) is equivalent to the condition that $\Phi_1(X) = B_1$ and $\Phi_2(X) < B_2$ for some choice of $X \in \mathrm{Pd}(\mathcal{X})$, while strict dual feasibility of (Ψ, C, D) is equivalent to the condition that $\Phi_1^*(Y_1) + \Phi_2^*(Y_2) > A$ for some choice of $Y \in \mathrm{Herm}(\mathcal{Y}_1)$ and $Y_2 \in \mathrm{Pd}(\mathcal{Y}_2)$. In other words, the "strictness" once again refers to the positive semidefinite ordering—every time it appears.

7.3.3 The standard form

The so-called *standard form* for semidefinite programs is given by the following pair of optimization problems:

Primal problem		Dual problem	
maximize:	$\langle A, X \rangle$	minimize:	$\sum_{j=1}^m \gamma_j y_j$
subject to:	$\langle B_1, X \rangle = \gamma_1$	subject to:	$\sum_{j=1}^m y_j B_j \geq A$
	$\vdots$		$y_1, \ldots, y_m \in \mathbb{R}$
	$\langle B_m, X \rangle = \gamma_m$		
	$X \in \mathrm{Pos}(\mathcal{X})$		

Here, $B_1, \ldots, B_m \in \mathrm{Herm}(\mathcal{X})$ take the place of Φ and $\gamma_1, \ldots, \gamma_m \in \mathbb{R}$ take the place of B in semidefinite programs as we have defined them.

It is not difficult to show that this form is equivalent to our form. First, to convert a semidefinite program in the standard form to our form, we define $\mathcal{Y} = \mathbb{C}^m$,

$$\Phi(X) = \sum_{j=1}^m \langle B_j, X \rangle E_{j,j},$$

and

$$B = \sum_{j=1}^m \gamma_j E_{j,j}.$$

The primal problem above is then equivalent to a maximization of $\langle A, X \rangle$ over all $X \in \mathrm{Pos}(\mathcal{X})$ satisfying $\Phi(X) = B$. The adjoint of Φ is given by

$$\Phi^*(Y) = \sum_{j=1}^m Y(j,j) B_j,$$

and we have that

$$\langle B, Y \rangle = \sum_{j=1}^m \gamma_j Y(j,j).$$

The off-diagonal entries of Y are irrelevant for the sake of this problem, and we find that a minimization of $\langle B, Y \rangle$ subject to $\Phi^*(Y) \geq A$ is equivalent to the dual problem given above.

Working in the other direction, the equality constraint $\Phi(X) = B$ may be represented as

$$\langle H_{a,b}, \Phi(X) \rangle = \langle H_{a,b}, B \rangle ,$$

ranging over the Hermitian operator basis $\{H_{a,b} : a, b \in \Gamma\}$ of $\mathrm{L}(\mathcal{Y})$ defined in Lecture 1, where we have assumed that $\mathcal{Y} = \mathbb{C}^{\Gamma}$. Taking $B_{a,b} = \Phi^*(H_{a,b})$ and $\gamma_{a,b} = \langle H_{a,b}, B \rangle$ allows us to write the primal problem associated with (Φ, A, B) as a semidefinite program in standard form. The standard-form dual problem above simplifies to the dual problem associated with (Φ, A, B).

The standard form has some positive aspects, but for the semidefinite programs to be encountered in this course we will find that it is less convenient to use than the forms we discussed previously.

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

Lecture 8: Semidefinite programs for fidelity and optimal measurements

This lecture is devoted to two examples of semidefinite programs: one is for the fidelity between two positive semidefinite operators, and the other is for optimal measurements for distinguishing ensembles of states. The primary goal in studying these examples at this point in the course is to gain familiarity with the concept of semidefinite programming and how it may be applied to problems of interest. The examples themselves are interesting, but they should not necessarily be viewed as primary reasons for studying semidefinite programming—they are simply examples making use of concepts we have discussed thus far in the course. We will see further applications of semidefinite programming to quantum information theory later in the course, and there are many more applications that we will not discuss.

8.1 A semidefinite program for the fidelity function

We begin with a semidefinite program whose optimal value equals the fidelity between to given positive semidefinite operators. As it represents the first application of semidefinite programming to quantum information theory that we are studying in the course, we will go through it in some detail.

8.1.1 Specification of the semidefinite program

Suppose $P, Q \in \mathrm{Pos}(\mathcal{X})$, where $\mathcal{X}$ is a complex Euclidean space, and consider the following optimization problem:

$$\begin{aligned} \text{maximize:} \quad & \frac{1}{2}\mathrm{Tr}(X) + \frac{1}{2}\mathrm{Tr}(X^*) \\ \text{subject to:} \quad & \begin{pmatrix} P & X \\ X^* & Q \end{pmatrix} \geq 0 \\ & X \in \mathrm{L}(\mathcal{X}). \end{aligned}$$

Although it is not phrased in the precise form of a semidefinite program as we formally defined them in the previous lecture, it can be converted to one, as we will now see.

Let us begin by noting that the matrix

$$\begin{pmatrix} P & X \\ X^* & Q \end{pmatrix}$$

is a block matrix that describes an operator in the space $\mathrm{L}(\mathcal{X} \oplus \mathcal{X})$. To phrase the optimization problem above as a semidefinite program, we will effectively optimize over all positive semidefinite operators in $\mathrm{Pos}(\mathcal{X} \oplus \mathcal{X})$, using linear constraints to force the diagonal blocks to be P and Q.

With this idea in mind, we define a linear mapping $\Phi : \mathrm{L}(\mathcal{X} \oplus \mathcal{X}) \to \mathrm{L}(\mathcal{X} \oplus \mathcal{X})$ as follows:

$$\Phi\begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} = \begin{pmatrix} X_{1,1} & 0 \\ 0 & X_{2,2} \end{pmatrix}$$

for all choices of $X_{1,1}, X_{1,2}, X_{2,1}, X_{2,2} \in \mathrm{L}(\mathcal{X})$, and we define $A, B \in \mathrm{Herm}(\mathcal{X} \oplus \mathcal{X})$ as

$$A = \frac{1}{2}\begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}.$$

Now consider the semidefinite program (Φ, A, B), as defined in the previous lecture. The primal objective function takes the form

$$\left\langle \frac{1}{2}\begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}, \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} \right\rangle = \frac{1}{2}\mathrm{Tr}(X_{1,2}) + \frac{1}{2}\mathrm{Tr}(X_{2,1}).$$

The constraint

$$\Phi\begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}$$

is equivalent to the conditions $X_{1,1} = P$ and $X_{2,2} = Q$. Of course, the condition

$$\begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} \in \mathrm{Pos}(\mathcal{X} \oplus \mathcal{X})$$

forces $X_{2,1} = X_{1,2}^*$, as this follows from the Hermiticity of the operator. So, by writing X in place of $X_{1,2}$, we see that the optimization problem stated at the beginning of the section is equivalent to the primal problem associated with (Φ, A, B).

Now let us examine the dual problem. It is as follows:

$$\begin{aligned} \text{minimize:} \quad & \left\langle \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}, \begin{pmatrix} Y_{1,1} & Y_{1,2} \\ Y_{2,1} & Y_{2,2} \end{pmatrix} \right\rangle \\ \text{subject to:} \quad & \Phi^*\begin{pmatrix} Y_{1,1} & Y_{1,2} \\ Y_{2,1} & Y_{2,2} \end{pmatrix} \geq \frac{1}{2}\begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}, \\ & \begin{pmatrix} Y_{1,1} & Y_{1,2} \\ Y_{2,1} & Y_{2,2} \end{pmatrix} \in \mathrm{Herm}(\mathcal{X} \oplus \mathcal{X}). \end{aligned}$$

As is typical when trying to understand the relationship between the primal and dual problems of a semidefinite program, we must find an expression for Φ^*. This happens to be easy in the present case, for we have

$$\left\langle \begin{pmatrix} Y_{1,1} & Y_{1,2} \\ Y_{2,1} & Y_{2,2} \end{pmatrix}, \Phi\begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} Y_{1,1} & Y_{1,2} \\ Y_{2,1} & Y_{2,2} \end{pmatrix}, \begin{pmatrix} X_{1,1} & 0 \\ 0 & X_{2,2} \end{pmatrix} \right\rangle = \langle Y_{1,1}, X_{1,1} \rangle + \langle Y_{2,2}, X_{2,2} \rangle$$

and

$$\left\langle \Phi\begin{pmatrix} Y_{1,1} & Y_{1,2} \\ Y_{2,1} & Y_{2,2} \end{pmatrix}, \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} Y_{1,1} & 0 \\ 0 & Y_{2,2} \end{pmatrix}, \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} \right\rangle = \langle Y_{1,1}, X_{1,1} \rangle + \langle Y_{2,2}, X_{2,2} \rangle,$$

so it must hold that $\Phi^* = \Phi$. Simplifying the above problem accordingly yields

$$\begin{aligned} \text{minimize:} \quad & \langle P, Y_{1,1} \rangle + \langle Q, Y_{2,2} \rangle \\ \text{subject to:} \quad & \begin{pmatrix} Y_{1,1} & 0 \\ 0 & Y_{2,2} \end{pmatrix} \geq \frac{1}{2} \begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix} \\ & Y_{1,1}, Y_{2,2} \in \mathrm{Herm}\,(\mathcal{X})\,. \end{aligned}$$

The problem has no dependence whatsoever on $Y_{1,2}$ and $Y_{2,1}$, so we can ignore them. Let us write $Y = 2Y_{1,1}$ and $Z = 2Y_{2,2}$, so that the problem becomes

$$\begin{aligned} \text{minimize:} \quad & \frac{1}{2} \langle P, Y \rangle + \frac{1}{2} \langle Q, Z \rangle \\ \text{subject to:} \quad & \begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} \geq 0 \\ & Y, Z \in \mathrm{Herm}\,(\mathcal{X})\,. \end{aligned}$$

There is no obvious reason for including the factor of 2 in the specification of Y and Z; it is simply a change of variables that is designed to put the problem into a nicer form for the analysis to come later. The inclusion of the factor of 2 does not, of course, change the fact that Y and Z are free to range over all Hermitian operators.

In summary, we have this pair of problems:

Primal problem	Dual problem
$\begin{aligned} \text{maximize:} \quad & \frac{1}{2}\mathrm{Tr}(X) + \frac{1}{2}\mathrm{Tr}(X^*) \\ \text{subject to:} \quad & \begin{pmatrix} P & X \\ X^* & Q \end{pmatrix} \geq 0 \\ & X \in \mathrm{L}\,(\mathcal{X})\,. \end{aligned}$	$\begin{aligned} \text{minimize:} \quad & \frac{1}{2} \langle P, Y \rangle + \frac{1}{2} \langle Q, Z \rangle \\ \text{subject to:} \quad & \begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} \geq 0 \\ & Y, Z \in \mathrm{Herm}\,(\mathcal{X})\,. \end{aligned}$

We will make some further simplifications to the dual problem a bit later in the lecture, but let us leave it as it is for the time being.

The statement of the primal and dual problems just given is representative of a typical style for specifying semidefinite programs: generally one does not explicitly refer to Φ, A, and B, or operators and mappings coming from other specific forms of semidefinite programs, in applications of the concept in papers or talks. It would not be unusual to see a pair of primal and dual problems presented like this without any indication of how the dual problem was obtained from the primal problem (or vice-versa). This is because the process is more or less routine, once you know how it is done. (Until you've had some practise doing it, however, it may not seem that way.)

8.1.2 Optimal value

Let us observe that strong duality holds for the semidefinite program above. This is easily established by first observing that the primal problem is feasible and the dual problem is strictly feasible, then applying Slater's theorem. To do this formally, we must refer to the triple (Φ, A, B) discussed above. Setting

$$\begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix} = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}$$

gives a primal feasible operator, so that $\mathcal{A} \neq \varnothing$. Setting

$$\begin{pmatrix} Y_{1,1} & Y_{1,2} \\ Y_{2,1} & Y_{2,2} \end{pmatrix} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & \mathbb{1} \end{pmatrix}$$

gives

$$\Phi^*\begin{pmatrix} Y_{1,1} & Y_{1,2} \\ Y_{2,1} & Y_{2,2} \end{pmatrix} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & \mathbb{1} \end{pmatrix} > \frac{1}{2}\begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix},$$

owing to the fact that

$$\begin{pmatrix} \mathbb{1} & -\frac{1}{2}\mathbb{1} \\ -\frac{1}{2}\mathbb{1} & \mathbb{1} \end{pmatrix} = \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix} \otimes \mathbb{1}$$

is positive definite. By Slater's theorem, we have strong duality, and moreover the optimal primal value is achieved by some choice of X.

It so happens that strict primal feasibility may fail to hold: if either of P or Q is not positive definite, it cannot hold that

$$\begin{pmatrix} P & X \\ X^* & Q \end{pmatrix} > 0.$$

Note, however, that we cannot conclude from this fact that the optimal dual value will not be achieved—but indeed this is the case for some choices of P and Q. If P and Q are positive definite, strict primal feasibility does hold, and the optimal dual value will be achieved, as follows from Slater's theorem.

Now let us prove that the optimal value is equal to $\mathrm{F}(P, Q)$, beginning with the inequality $\alpha \geq \mathrm{F}(P, Q)$. To prove this inequality, it suffices to exhibit a primal feasible X for which

$$\frac{1}{2}\operatorname{Tr}(X) + \frac{1}{2}\operatorname{Tr}(X^*) = \mathrm{F}(P, Q).$$

We have

$$\mathrm{F}(P, Q) = \mathrm{F}(Q, P) = \left\| \sqrt{Q}\sqrt{P} \right\|_1 = \max\left\{ \left| \operatorname{Tr}\left(U\sqrt{Q}\sqrt{P}\right) \right| \,:\, U \in \mathrm{U}\left(\mathcal{X}\right) \right\},$$

and so we may choose a unitary operator $U \in \mathrm{U}\left(\mathcal{X}\right)$ for which

$$\mathrm{F}(P, Q) = \operatorname{Tr}\left(U\sqrt{Q}\sqrt{P}\right) = \operatorname{Tr}\left(\sqrt{P}U\sqrt{Q}\right).$$

(The absolute value can safely be omitted: we are free to multiply any U maximizing the absolute value with a scalar on the unit circle, obtaining a nonnegative real number for the trace.) Now define

$$X = \sqrt{P}U\sqrt{Q}.$$

It holds that

$$0 \leq \begin{pmatrix} \sqrt{P} & U\sqrt{Q} \end{pmatrix}^* \begin{pmatrix} \sqrt{P} & U\sqrt{Q} \end{pmatrix} = \begin{pmatrix} \sqrt{P} \\ \sqrt{Q}U^* \end{pmatrix} \begin{pmatrix} \sqrt{P} & U\sqrt{Q} \end{pmatrix} = \begin{pmatrix} P & \sqrt{P}U\sqrt{Q} \\ \sqrt{Q}U^*\sqrt{P} & Q \end{pmatrix},$$

so X is primal feasible, and we have

$$\frac{1}{2}\operatorname{Tr}(X) + \frac{1}{2}\operatorname{Tr}(X^*) = \mathrm{F}(P, Q)$$

as claimed.

Now let us prove the reverse inequality: $\alpha \leq \mathrm{F}(P,Q)$. Suppose that $X \in \mathrm{L}(\mathcal{X})$ is primal feasible, meaning that

$$R = \begin{pmatrix} P & X \\ X^* & Q \end{pmatrix}$$

is positive semidefinite. We may view that $R \in \mathrm{Pos}(\mathcal{Z} \otimes \mathcal{X})$ for $\mathcal{Z} = \mathbb{C}^2$. (More generally, the m-fold direct sum $\mathbb{C}^\Sigma \oplus \cdots \oplus \mathbb{C}^\Sigma$ may be viewed as being equivalent to the tensor product $\mathbb{C}^m \otimes \mathbb{C}^\Sigma$ by identifying the standard basis element $e_{(j,a)}$ of $\mathbb{C}^\Sigma \oplus \cdots \oplus \mathbb{C}^\Sigma$ with the standard basis element $e_j \otimes e_a$ of $\mathbb{C}^m \otimes \mathbb{C}^\Sigma$, for each $j \in \{1,\ldots,m\}$ and $a \in \Sigma$.) Let $\mathcal{Y}$ be a complex Euclidean space whose dimension is at least $\mathrm{rank}(R)$, and let $u \in \mathcal{Z} \otimes \mathcal{X} \otimes \mathcal{Y}$ be a purification of R:

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = R = E_{1,1} \otimes P + E_{1,2} \otimes X + E_{2,1} \otimes X^* + E_{2,2} \otimes Q.$$

Write

$$u = e_1 \otimes u_1 + e_2 \otimes u_2$$

for $u_1, u_2 \in \mathcal{X}$, and observe that

$$\mathrm{Tr}_{\mathcal{Y}}(u_1 u_1^*) = P, \qquad \mathrm{Tr}_{\mathcal{Y}}(u_2 u_2^*) = Q, \qquad \mathrm{Tr}_{\mathcal{Y}}(u_1 u_2^*) = X, \qquad \text{and} \qquad \mathrm{Tr}_{\mathcal{Y}}(u_2 u_1^*) = X^*.$$

We have

$$\frac{1}{2}\mathrm{Tr}(X) + \frac{1}{2}\mathrm{Tr}(X^*) = \frac{1}{2}\langle u_2, u_1\rangle + \frac{1}{2}\langle u_1, u_2\rangle = \Re(\langle u_1, u_2\rangle) \leq |\langle u_1, u_2\rangle| \leq \mathrm{F}(P,Q),$$

where the last inequality follows from Uhlmann's theorem, along with the fact that u_1 and u_2 purify P and Q, respectively.

8.1.3 Alternate proof of Alberti's theorem

The notes from Lecture 4 include a proof of Alberti's theorem, which states that

$$(\mathrm{F}(P,Q))^2 = \inf_{Y \in \mathrm{Pd}(\mathcal{X})} \langle P, Y\rangle \langle Q, Y^{-1}\rangle,$$

for every choice of positive semidefinite operators $P, Q \in \mathrm{Pos}(\mathcal{X})$. We may use our semidefinite program to obtain an alternate proof of this characterization.

First let us return to the dual problem from above:

$$\begin{aligned} &\underline{\text{Dual problem}} \\ \text{minimize:} \quad & \frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle Q, Z\rangle \\ \text{subject to:} \quad & \begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} \geq 0 \\ & Y, Z \in \mathrm{Herm}(\mathcal{X}). \end{aligned}$$

To simplify the problem further, let us prove the following claim.

Claim 8.1. Let $Y, Z \in \mathrm{Herm}(\mathcal{X})$. It holds that

$$\begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{X})$$

if and only if $Y, Z \in \mathrm{Pd}(\mathcal{X})$ and $Z \geq Y^{-1}$.

Proof. Suppose $Y, Z \in \mathrm{Pd}(\mathcal{X})$ and $Z \geq Y^{-1}$. It holds that

$$\begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} = \begin{pmatrix} \mathbb{1} & 0 \\ -Y^{-1} & \mathbb{1} \end{pmatrix} \begin{pmatrix} Y & 0 \\ 0 & Z - Y^{-1} \end{pmatrix} \begin{pmatrix} \mathbb{1} & -Y^{-1} \\ 0 & \mathbb{1} \end{pmatrix}$$

and therefore

$$\begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{X}).$$

Conversely, suppose that

$$\begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{X}).$$

It holds that

$$0 \leq \begin{pmatrix} u \\ v \end{pmatrix}^* \begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = u^* Y u - u^* v - v^* u + v^* Z v$$

for all $u, v \in \mathcal{X}$. If Y were not positive definite, there would exist a unit vector v for which $v^* Y v = 0$, and one could then set

$$u = \frac{1}{2}(\|Z\| + 1)v$$

to obtain

$$\|Z\| \geq v^* Z v \geq \langle u, v \rangle + \langle v, u \rangle = \|Z\| + 1,$$

which is absurd. Thus, $Y \in \mathrm{Pd}(\mathcal{X})$. Finally, by inverting the expression above, we have

$$\begin{pmatrix} Y & 0 \\ 0 & Z - Y^{-1} \end{pmatrix} = \begin{pmatrix} \mathbb{1} & 0 \\ Y^{-1} & \mathbb{1} \end{pmatrix} \begin{pmatrix} Y & -\mathbb{1} \\ -\mathbb{1} & Z \end{pmatrix} \begin{pmatrix} \mathbb{1} & Y^{-1} \\ 0 & \mathbb{1} \end{pmatrix} \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{X}),$$

which implies $Z \geq Y^{-1}$ (and therefore $Z \in \mathrm{Pd}(\mathcal{X})$) as required. □

Now, given that Q is positive semidefinite, it holds that $\langle Q, Z \rangle \geq \langle Q, Y^{-1} \rangle$ whenever $Z \geq Y^{-1}$, so there would be no point in choosing any Z other than Y^{-1} when aiming to minimize the dual objective function subject to that constraint. The dual problem above can therefore be phrased as follows:

Dual problem

$$\begin{aligned} \text{minimize:} \quad & \frac{1}{2}\langle P, Y \rangle + \frac{1}{2}\langle Q, Y^{-1} \rangle \\ \text{subject to:} \quad & Y \in \mathrm{Pd}(\mathcal{X}). \end{aligned}$$

Given that strong duality holds for our semidefinite program, and that we know the optimal value to be $\mathrm{F}(P, Q)$, we have the following theorem.

Theorem 8.2. *Let $\mathcal{X}$ be a complex Euclidean space and let $P, Q \in \mathrm{Pos}(\mathcal{X})$. It holds that*

$$\mathrm{F}(P, Q) = \inf\left\{ \frac{1}{2}\langle P, Y \rangle + \frac{1}{2}\langle Q, Y^{-1} \rangle \,:\, Y \in \mathrm{Pd}(\mathcal{X}) \right\}.$$

To see that this is equivalent to Alberti's theorem, note that for every $Y \in \mathrm{Pd}(\mathcal{X})$ it holds that

$$\frac{1}{2}\langle P, Y\rangle + \frac{1}{2}\langle Q, Y^{-1}\rangle \geq \sqrt{\langle P, Y\rangle\langle Q, Y^{-1}\rangle},$$

with equality if and only if $\langle P, Y\rangle = \langle Q, Y^{-1}\rangle$ (by the arithmetic-geometric mean inequality). It follows that

$$\inf_{Y \in \mathrm{Pd}(\mathcal{X})} \langle P, Y\rangle \langle Q, Y^{-1}\rangle \leq \left(\mathrm{F}(P, Q)\right)^2.$$

Moreover, for an arbitrary choice of $Y \in \mathrm{Pd}(\mathcal{X})$, one may choose $\lambda > 0$ so that

$$\langle P, \lambda Y\rangle = \langle Q, (\lambda Y)^{-1}\rangle$$

and therefore

$$\frac{1}{2}\langle P, \lambda Y\rangle + \frac{1}{2}\langle Q, (\lambda Y)^{-1}\rangle = \sqrt{\langle P, \lambda Y\rangle\langle Q, (\lambda Y)^{-1}\rangle} = \sqrt{\langle P, Y\rangle\langle Q, Y^{-1}\rangle}.$$

Thus,

$$\inf_{Y \in \mathrm{Pd}(\mathcal{X})} \langle P, Y\rangle \langle Q, Y^{-1}\rangle \geq \left(\mathrm{F}(P, Q)\right)^2.$$

We therefore have that Alberti's theorem (Theorem 4.8) is a corollary to the theorem above, as claimed.

8.2 Optimal measurements

We will now move on to the second example of the lecture of a semidefinite programming application to quantum information theory. This example concerns the notion of optimal measurements for distinguishing elements of an ensemble of states.

Suppose that $\mathcal{X}$ is a complex Euclidean space, Γ is a finite and nonempty set, $p \in \mathbb{R}^{\Gamma}$ is a probability vector, and $\{\rho_a : a \in \Gamma\} \subset \mathrm{D}(\mathcal{X})$ is a collection of density operators. Consider the scenario in which Alice randomly selects $a \in \Gamma$ according to the probability distribution described by p, then prepares a register X in the state ρ_a for whichever element $a \in \Gamma$ she selected. She sends X to Bob, whose goal is to identify the element $a \in \Gamma$ selected by Alice with as high a probability as possible. He must do this by means of a measurement $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X}) : a \mapsto P_a$ on X, without any additional help or input from Alice. Bob's optimal probability is given by the maximum value of

$$\sum_{a \in \Gamma} p(a) \langle P_a, \rho_a\rangle$$

over all measurements $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X}) : a \mapsto P_a$ on $\mathcal{X}$.

It is natural to associate an *ensemble* of states with the process performed by Alice. This is a collection

$$\mathcal{E} = \{(p(a), \rho_a) : a \in \Gamma\},$$

which can be described more succinctly by a mapping

$$\eta : \Gamma \to \mathrm{Pos}(\mathcal{X}) : a \mapsto \sigma_a,$$

where $\sigma_a = p(a)\rho_a$ for each $a \in \Gamma$. In general, any mapping η of the above form represents an ensemble if and only if

$$\sum_{a \in \Gamma} \sigma_a \in \mathrm{D}(\mathcal{X}).$$

To recover the description of a collection $\mathcal{E} = \{(p(a), \rho_a) : a \in \Gamma\}$ representing such an ensemble, one may take $p(a) = \operatorname{Tr}(\sigma_a)$ and $\rho_a = \sigma_a / \operatorname{Tr}(\sigma_a)$. Thus, each σ_a is generally not a density operator, but may be viewed as an unnormalized density operator that describes both a density operator and the probability that it is selected.

Now, let us say that a measurement $\mu : \Gamma \to \operatorname{Pos}(\mathcal{X})$ is an *optimal* measurement for a given ensemble $\eta : \Gamma \to \operatorname{Pos}(\mathcal{X})$ if and only if it holds that

$$\sum_{a \in \Gamma} \langle \mu(a), \eta(a) \rangle$$

is maximal among all possible choices of measurements that could be substituted for μ in this expression. We will prove the following theorem, which provides a simple condition (both necessary and sufficient) for a given measurement to be optimal for a given ensemble.

Theorem 8.3. *Let $\mathcal{X}$ be a complex Euclidean space, let Γ be a finite and nonempty set, let $\eta : \Gamma \to \operatorname{Pos}(\mathcal{X}) : a \mapsto \sigma_a$ be an ensemble of states, and let $\mu : \Gamma \to \operatorname{Pos}(\mathcal{X}) : a \mapsto P_a$ be a measurement. It holds that μ is optimal for η if and only if the operator*

$$Y = \sum_{a \in \Gamma} \sigma_a P_a$$

is Hermitian and satisfies $Y \geq \sigma_a$ for each $a \in \Gamma$.

The following proposition, which states a property known as *complementary slackness* for semidefinite programs, will be used to prove the theorem.

Proposition 8.4 (Complementary slackness for SDPs)**.** *Suppose (Φ, A, B) is a semidefinite program, and that $X \in \mathcal{A}$ and $Y \in \mathcal{B}$ satisfy $\langle A, X \rangle = \langle B, Y \rangle$. It holds that*

$$\Phi^*(Y)X = AX \qquad \text{and} \qquad \Phi(X)Y = BY.$$

Remark 8.5. Note that the second equality stated in the proposition is completely trivial, given that $\Phi(X) = B$ for all $X \in \mathcal{A}$. It is stated nevertheless in the interest of illustrating the symmetry between the primal and dual forms of semidefinite programs.

Proof. It holds that

$$\langle A, X \rangle = \langle B, Y \rangle = \langle \Phi(X), Y \rangle = \langle \Phi^*(Y), X \rangle,$$

so

$$\langle \Phi^*(Y) - A, X \rangle = 0.$$

Both $\Phi^*(Y) - A$ and X are positive semidefinite, given that X and Y are feasible. The inner product of two positive semidefinite operators is zero if and only if their product is zero, and so we obtain

$$(\Phi^*(Y) - A)\, X = 0.$$

This implies the first equality in the proposition, as required. □

Next, we will phrase the problem of maximizing the probability of correctly identifying the states in an ensemble as a semidefinite program. We suppose that an ensemble

$$\eta : \Gamma \to \operatorname{Pos}(\mathcal{X}) : a \mapsto \sigma_a$$

is given, and define a semidefinite program as follows. Let $\mathcal{Y} = \mathbb{C}^{\Gamma}$, let $A \in \mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X})$ be given by

$$A = \sum_{a \in \Gamma} E_{a,a} \otimes \sigma_a,$$

and consider the partial trace $\mathrm{Tr}_{\mathcal{Y}}$ as an element of $\mathrm{T}(\mathcal{Y} \otimes \mathcal{X}, \mathcal{X})$. The semidefinite program to be considered is $(\mathrm{Tr}_{\mathcal{Y}}, A, \mathbb{1}_{\mathcal{X}})$, and with it one associates the following problems:

Primal problem		Dual problem	
maximize:	$\langle A, X \rangle$	minimize:	$\mathrm{Tr}(Y)$
subject to:	$\mathrm{Tr}_{\mathcal{Y}}(X) = \mathbb{1}_{\mathcal{X}}$,	subject to:	$\mathbb{1}_{\mathcal{Y}} \otimes Y \geq A$
	$X \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$.		$Y \in \mathrm{Herm}(\mathcal{X})$.

To see that the primal problem represents the optimization problem we are interested in, which is the maximization of

$$\sum_{a \in \Gamma} \langle P_a, \sigma_a \rangle = \sum_{a \in \Gamma} \langle \sigma_a, P_a \rangle$$

over all measurements $\{P_a : a \in \Gamma\}$, we note that any $X \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$ may be written

$$X = \sum_{a,b \in \Gamma} E_{a,b} \otimes X_{a,b}$$

for $\{X_{a,b} : a, b \in \Gamma\} \subset \mathrm{L}(\mathcal{X})$, that the objective function is then given by

$$\langle A, X \rangle = \sum_{a \in \Gamma} \langle \sigma_a, X_{a,a} \rangle$$

and that the constraint $\mathrm{Tr}_{\mathcal{Y}}(X) = \mathbb{1}_{\mathcal{X}}$ is given by

$$\sum_{a \in \Gamma} X_{a,a} = \mathbb{1}_{\mathcal{X}}.$$

As X ranges over all positive semidefinite operators in $\mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, the operators $X_{a,a}$ individually and independently range over all possible positive semidefinite operators in $\mathrm{Pos}(\mathcal{X})$. The "off-diagonal" operators $X_{a,b}$, for $a \neq b$, have no influence on the problem at all, and can safely be ignored. Writing P_a in place of $X_{a,a}$, we see that the primal problem can alternately be written

$$\begin{array}{ll} & \underline{\text{Primal problem}} \\ \text{maximize:} & \displaystyle\sum_{a \in \Gamma} \langle \sigma_a, P_a \rangle \\ \text{subject to:} & \{P_a : a \in \Gamma\} \subset \mathrm{Pos}(\mathcal{X}) \\ & \displaystyle\sum_{a \in \Gamma} P_a = \mathbb{1}_{\mathcal{X}}, \end{array}$$

which is the optimization problem of interest.

The dual problem can be simplified by noting that the constraint

$$\mathbb{1}_{\mathcal{Y}} \otimes Y \geq A$$

is equivalent to

$$\sum_{a \in \Gamma} E_{a,a} \otimes (Y - \sigma_a) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X}),$$

which in turn is equivalent to $Y \geq \sigma_a$ for each $a \in \Gamma$.

To summarize, we have the following pair of optimization problems:

Primal problem		Dual problem	
maximize:	$\sum_{a\in\Gamma} \langle \sigma_a, P_a \rangle$	minimize:	$\mathrm{Tr}(Y)$
subject to:	$\{P_a : a \in \Gamma\} \subset \mathrm{Pos}(\mathcal{X})$	subject to:	$Y \geq \sigma_a \quad (\text{for all } a \in \Gamma)$
	$\sum_{a\in\Gamma} P_a = \mathbb{1}_{\mathcal{X}},$		$Y \in \mathrm{Herm}(\mathcal{X}).$

Strict feasibility is easy to show for this semidefinite program: we may take

$$X = \frac{1}{|\Gamma|}\mathbb{1}_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{X}} \qquad \text{and} \qquad Y = 2\mathbb{1}_{\mathcal{X}}$$

to obtain strictly feasible primal and dual solutions. By Slater's theorem, we have strong duality, and moreover that optimal values are always achieved in both problems.

We are now in a position to prove Theorem 8.3. Suppose first that the measurement μ is optimal for η, so that $\{P_a : a \in \Gamma\}$ is optimal for the semidefinite program above. Somewhat more formally, we have that

$$X = \sum_{a\in\Gamma} E_{a,a} \otimes P_a$$

is an optimal primal solution to the semidefinite program $(\mathrm{Tr}_{\mathcal{Y}}, A, \mathbb{1}_{\mathcal{X}})$. Take Z to be any optimal solution to the dual problem, which we know exists because the optimal solution is always achievable for both the primal and dual problems. By complementary slackness (i.e., Proposition 8.4) it holds that

$$\mathrm{Tr}_{\mathcal{Y}}^*(Z)X = AX,$$

which expands to

$$\sum_{a\in\Gamma} E_{a,a} \otimes ZP_a = \sum_{a\in\Gamma} E_{a,a} \otimes \sigma_a P_a,$$

implying

$$ZP_a = \sigma_a P_a$$

for each $a \in \Gamma$. Summing over $a \in \Gamma$ yields

$$Z = \sum_{a\in\Gamma} \sigma_a P_a = Y.$$

It therefore holds that Y is dual feasible, implying that Y is Hermitian and satisfies $Y \geq \sigma_a$ for each $a \in \Gamma$.

Conversely, suppose that Y is Hermitian and satisfies $Y \geq \sigma_a$ for each $a \in \Gamma$. This means that Y is dual feasible. Given that

$$\mathrm{Tr}(Y) = \sum_{a\in\Gamma} \langle \sigma_a, P_a \rangle,$$

we find that $\{P_a : a \in \Gamma\}$ must be an optimal primal solution by weak duality, as it equals the value achieved by a dual feasible solution. The measurement μ is therefore optimal for the ensemble η.

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

Lecture 9: Entropy and compression

For the next several lectures we will be discussing the von Neumann entropy and various concepts relating to it. This lecture is intended to introduce the notion of entropy and its connection to compression.

9.1 Shannon entropy

Before we discuss the von Neumann entropy, we will take a few moments to discuss the Shannon entropy. This is a purely classical notion, but it is appropriate to start here. The *Shannon entropy* of a probability vector $p \in \mathbb{R}^{\Sigma}$ is defined as follows:

$$H(p) = -\sum_{\substack{a \in \Sigma \\ p(a) > 0}} p(a) \log(p(a)).$$

Here, and always in this course, the base of the logarithm is 2. (We will write $\ln(\alpha)$ if we wish to refer to the natural logarithm of a real number α.) It is typical to express the Shannon entropy slightly more concisely as

$$H(p) = -\sum_{a \in \Sigma} p(a) \log(p(a)),$$

which is meaningful if we make the interpretation $0 \log(0) = 0$. This is sensible given that

$$\lim_{\alpha \to 0^+} \alpha \log(\alpha) = 0.$$

There is no reason why we cannot extend the definition of the Shannon entropy to arbitrary vectors with nonnegative entries if it is useful to do this—but mostly we will focus on probability vectors.

There are standard ways to interpret the Shannon entropy. For instance, the quantity $H(p)$ can be viewed as a measure of the amount of uncertainty in a random experiment described by the probability vector p, or as a measure of the amount of information one gains by learning the value of such an experiment. Indeed, it is possible to start with simple axioms for what a measure of uncertainty or information should satisfy, and to derive from these axioms that such a measure must be equivalent to the Shannon entropy.

Something to keep in mind, however, when using these interpretations as a guide, is that the Shannon entropy is usually only a meaningful measure of uncertainty in an asymptotic sense—as the number of experiments becomes large. When a small number of samples from some experiment is considered, the Shannon entropy may not conform to your intuition about uncertainty, as the following example is meant to demonstrate.

Example 9.1. Let $\Sigma = \{0, 1, \ldots, 2^{m^2}\}$, and define a probability vector $p \in \mathbb{R}^{\Sigma}$ as follows:

$$p(a) = \begin{cases} 1 - \frac{1}{m} & a = 0, \\ \frac{1}{m} 2^{-m^2} & 1 \leq a \leq 2^{m^2}. \end{cases}$$

It holds that $H(p) > m$, and yet the outcome 0 appears with probability $1 - 1/m$. So, as m grows, we become more and more "certain" that the outcome will be 0, and yet the "uncertainty" (as measured by the entropy) goes to infinity.

The above example does not, of course, represent a paradox. The issue is simply that the Shannon entropy can only be interpreted as measuring uncertainty if the number of random experiments grows and the probability vector remains fixed, which is opposite to the example.

9.2 Classical compression and Shannon's source coding theorem

Let us now focus on an important use of the Shannon entropy, which involves the notion of a *compression scheme*. This will allow us to attach a concrete meaning to the Shannon entropy.

9.2.1 Compression schemes

Let $p \in \mathbb{R}^{\Sigma}$ be a probability vector, and let us take $\Gamma = \{0, 1\}$ to be the binary alphabet. For a positive integer n and real numbers $\alpha > 0$ and $\delta \in (0, 1)$, let us say that a pair of mappings

$$f : \Sigma^n \to \Gamma^m$$
$$g : \Gamma^m \to \Sigma^n,$$

forms an (n, α, δ)-*compression scheme* for p if it holds that $m = \lfloor \alpha n \rfloor$ and

$$\Pr\left[g(f(a_1 \cdots a_n)) = a_1 \cdots a_n\right] > 1 - \delta, \tag{9.1}$$

where the probability is over random choices of $a_1, \ldots, a_n \in \Sigma$, each chosen independently according to the probability vector p.

To understand what a compression scheme means at an intuitive level, let us imagine the following situation between two people: Alice and Bob. Alice has a device of some sort with a button on it, and when she presses the button she gets an element of Σ, distributed according to p, independent of any prior outputs of the device. She presses the button n times, obtaining outcomes $a_1 \cdots a_n$, and she wants to communicate these outcomes to Bob using as few bits of communication as possible. So, what Alice does is to *compress* $a_1 \cdots a_n$ into a string of $m = \lfloor \alpha n \rfloor$ bits by computing $f(a_1 \cdots a_n)$. She sends the resulting bit-string $f(a_1 \cdots a_n)$ to Bob, who then *decompresses* by applying g, therefore obtaining $g(f(a_1 \cdots a_n))$. Naturally they hope that $g(f(a_1 \cdots a_n)) = a_1 \cdots a_n$, which means that Bob will have obtained the correct sequence $a_1 \cdots a_n$.

The quantity δ is a bound on the probability the compression scheme makes an error. We may view that the pair (f, g) *works correctly* for a string $a_1 \cdots a_n \in \Sigma^n$ if $g(f(a_1 \cdots a_n)) = a_1 \cdots a_n$, so the above equation (9.1) is equivalent to the condition that the pair (f, g) works correctly with high probability (assuming δ is small).

9.2.2 Statement of Shannon's source coding theorem

In the discussion above, the number α represents the average number of bits the compression scheme needs in order to represent each sample from the distribution described by p. It is obvious that compression schemes will exist for some numbers α and not others. The particular values of α for which it is possible to come up with a compression scheme are closely related to the Shannon entropy $H(p)$, as the following theorem establishes.

Theorem 9.2 (Shannon's source coding theorem)**.** *Let Σ be a finite, non-empty set, let $p \in \mathbb{R}^{\Sigma}$ be a probability vector, let $\alpha > 0$, and let $\delta \in (0,1)$. The following statements hold.*

1. *If $\alpha > H(p)$, then there exists an (n, α, δ)-compression scheme for p for all but finitely many choices of $n \in \mathbb{N}$.*
2. *If $\alpha < H(p)$, then there exists an (n, α, δ)-compression scheme for p for at most finitely many choices of $n \in \mathbb{N}$.*

It is not a mistake, by the way, that both statements hold for any fixed choice of $\delta \in (0,1)$, regardless of whether it is close to 0 or 1 (for instance). This will make sense when we see the proof.

It should be mentioned that the above statement of Shannon's source coding theorem is specific to the somewhat simplified (fixed-length) notion of compression that we have defined. It is more common, in fact, to consider variable-length compressions and to state Shannon's source coding theorem in terms of the average length of compressed strings. The reason why we restrict our attention to fixed-length compression schemes is that this sort of scheme will be more natural when we turn to the quantum setting.

9.2.3 Typical strings

Before we can prove the above theorem, we will need to develop the notion of a *typical string*. For a given probability vector $p \in \mathbb{R}^{\Sigma}$, positive integer n, and positive real number ε, we say that a string $a_1 \cdots a_n \in \Sigma^n$ is *ϵ-typical (with respect to p)* if

$$2^{-n(H(p)+\varepsilon)} < p(a_1) \cdots p(a_n) < 2^{-n(H(p)-\varepsilon)}.$$

We will need to refer to the set of all ε-typical strings of a given length repeatedly, so let us give this set a name:

$$T_{n,\varepsilon}(p) = \left\{ a_1 \cdots a_n \in \Sigma^n \,:\, 2^{-n(H(p)+\varepsilon)} < p(a_1) \cdots p(a_n) < 2^{-n(H(p)-\varepsilon)} \right\}.$$

When the probability vector p is understood from context we write $T_{n,\varepsilon}$ rather than $T_{n,\varepsilon}(p)$.

The following lemma establishes that a random selection of a string $a_1 \cdots a_n$ is very likely to be ε-typical as n gets large.

Lemma 9.3. *Let $p \in \mathbb{R}^{\Sigma}$ be a probability vector and let $\varepsilon > 0$. It holds that*

$$\lim_{n\to\infty} \sum_{a_1\cdots a_n \in T_{n,\varepsilon}(p)} p(a_1) \cdots p(a_n) = 1$$

Proof. Let $Y_1, \ldots, Y_n$ be independent and identically distributed random variables defined as follows: we choose $a \in \Sigma$ randomly according to the probability vector p, and then let the output value be the real number $-\log(p(a))$ for whichever value of a was selected. It holds that the expected value of each Y_j is

$$E[Y_j] = -\sum_{a\in\Sigma} p(a)\log(p(a)) = H(p).$$

The conclusion of the lemma may now be written

$$\lim_{n\to\infty} \Pr\left[\left| \frac{1}{n} \sum_{j=1}^{n} Y_j - H(p) \right| \geq \varepsilon \right] = 0,$$

which is true by the weak law of large numbers. □

Based on the previous lemma, it is straightforward to place upper and lower bounds on the number of ε-typical strings, as shown in the following lemma.

Lemma 9.4. *Let $p \in \mathbb{R}^{\Sigma}$ be a probability vector and let ε be a positive real number. For all but finitely many positive integers n it holds that*

$$(1-\varepsilon)2^{n(H(p)-\varepsilon)} < |T_{n,\varepsilon}| < 2^{n(H(p)+\varepsilon)}.$$

Proof. The upper bound holds for all n. Specifically, by the definition of ε-typical, we have

$$1 \geq \sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} p(a_1) \cdots p(a_n) > 2^{-n(H(p)+\varepsilon)} \, |T_{n,\varepsilon}|,$$

and therefore $|T_{n,\varepsilon}| < 2^{n(H(p)+\varepsilon)}$.

For the lower bound, let us choose n_0 so that

$$\sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} p(a_1) \cdots p(a_n) > 1 - \varepsilon$$

for all $n \geq n_0$, which is possible by Lemma 9.3. For all $n \geq n_0$ we have

$$1 - \varepsilon < \sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} p(a_1) \cdots p(a_n) < |T_{n,\varepsilon}| \, 2^{-n(H(p)-\varepsilon)},$$

and therefore $|T_{n,\varepsilon}| > (1-\varepsilon)2^{n(H(p)-\varepsilon)}$, which completes the proof. □

9.2.4 Proof of Shannon's source coding theorem

We now have the necessary tools to prove Shannon's source coding theorem. Having developed some basic properties of typical strings, the proof is very simple: a good compression function is obtained by simply assigning a unique binary string to each typical string, with every other string mapped arbitrarily. On the other hand, any compression scheme that fails to account for a large fraction of the typical strings will be shown to fail with very high probability.

Proof of Theorem 9.2. First assume that $\alpha > H(p)$, and choose $\varepsilon > 0$ so that $\alpha > H(p) + 2\varepsilon$. For every choice of $n > 1/\varepsilon$ we therefore have that

$$m = \lfloor \alpha n \rfloor > n(H(p) + \varepsilon).$$

Now, because

$$|T_{n,\varepsilon}| < 2^{n(H(p)+\varepsilon)} < 2^m,$$

we may defined a function $f : \Sigma^n \to \Gamma^m$ that is 1-to-1 when restricted to $T_{n,\varepsilon}$, and we may define $g : \Gamma^m \to \Sigma^n$ appropriately so that $g(f(a_1 \cdots a_n)) = a_1 \cdots a_n$ for every $a_1 \cdots a_n \in T_{n,\varepsilon}$. As

$$\Pr\left[g(f(a_1 \cdots a_n)) = a_1 \cdots a_n\right] \geq \Pr[a_1 \cdots a_n \in T_{n,\varepsilon}] = \sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} p(a_1) \cdots p(a_n),$$

we have that this quantity is greater than $1 - \delta$ for sufficiently large n.

Now let us prove the second item, where we assume $\alpha < H(p)$. It is clear from the definition of an (n, α, δ)-compression scheme that such a scheme can only work correctly for at most $2^{\lfloor \alpha n \rfloor}$

strings $a_1 \cdots a_n$. Let us suppose such a scheme is given for each n, and let $G_n \subseteq \Sigma^n$ be the collection of strings on which the appropriate scheme works correctly. If we can show that

$$\lim_{n\to\infty} \Pr[a_1 \cdots a_n \in G_n] = 0 \tag{9.2}$$

then we will be finished.

Toward this goal, let us note that for every n and ε, we have

$$\begin{aligned}\Pr[a_1 \cdots a_n \in G_n] &\leq \Pr[a_1 \cdots a_n \in G_n \cap T_{n,\varepsilon}] + \Pr[a_1 \cdots a_n \notin T_{n,\varepsilon}] \\ &\leq |G_n|\, 2^{-n(H(p)-\varepsilon)} + \Pr[a_1 \cdots a_n \notin T_{n,\varepsilon}].\end{aligned}$$

Choose $\varepsilon > 0$ so that $\alpha < H(p) - \varepsilon$. It follows that

$$\lim_{n\to\infty} |G_n|\, 2^{-n(H(p)-\varepsilon)} = 0.$$

As

$$\lim_{n\to\infty} \Pr[a_1 \cdots a_n \notin T_{n,\varepsilon}] = 0$$

by Lemma 9.3, we have (9.2) as required. □

9.3 Von Neumann entropy

Next we will discuss the *von Neumann entropy*, which may be viewed as a quantum information-theoretic analogue of the Shannon entropy. We will spend the next few lectures after this one discussing the properties of the von Neumann entropy as well as some of its uses—but for now let us just focus on the definition.

Let $\mathcal{X}$ be a complex Euclidean space, let $n = \dim(\mathcal{X})$, and let $\rho \in \mathrm{D}(\mathcal{X})$ be a density operator. The von Neumann entropy of ρ is defined as

$$S(\rho) = H(\lambda(\rho)),$$

where $\lambda(\rho) = (\lambda_1(\rho), \ldots, \lambda_n(\rho))$ is the vector of eigenvalues of ρ. An equivalent expression is

$$S(\rho) = -\operatorname{Tr}(\rho \log(\rho)),$$

where $\log(\rho)$ is the Hermitian operator that has exactly the same eigenvectors as ρ, and we take the base 2 logarithm of the corresponding eigenvalues. Technically speaking, $\log(\rho)$ is only defined for ρ positive definite, but $\rho \log(\rho)$ may be defined for all positive semidefinite ρ by interpreting $0 \log(0)$ as 0, just like in the definition of the Shannon entropy.

9.4 Quantum compression

There are some ways in which the von Neumann entropy is similar to the Shannon entropy and some ways in which it is very different. One way in which they are quite similar is in their relationships to notions of compression.

9.4.1 Informal discussion of quantum compression

To explain quantum compression, let us imagine a scenario between Alice and Bob that is similar to the classical scenario we discussed in relation to classical compression. We imagine that Alice has a collection of identical registers $\mathsf{X}_1, \mathsf{X}_2, \ldots, \mathsf{X}_n$, whose associated complex Euclidean spaces are $\mathcal{X}_1 = \mathbb{C}^\Sigma, \ldots, \mathcal{X}_n = \mathbb{C}^\Sigma$ for some finite and nonempty set Σ. She wants to *compress* the contents of these registers into $m = \lfloor \alpha n \rfloor$ qubits, for some choice of $\alpha > 0$, and to send those qubits to Bob. Bob will then *decompress* the qubits to (hopefully) obtain registers $\mathsf{X}_1, \mathsf{X}_2, \ldots, \mathsf{X}_n$ with little disturbance to their initial state.

It will not gnenerally be possible for Alice to do this without some assumption on the state of $(\mathsf{X}_1, \mathsf{X}_2, \ldots, \mathsf{X}_n)$. Our assumption will be analogous to the classical case: we assume that the states of these registers are independent and described by some density operator $\rho \in \mathrm{D}(\mathcal{X})$ (as opposed to a probability vector $p \in \mathbb{R}^\Sigma$). That is, the state of the collection of registers will be assumed to be $\rho^{\otimes n} \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$, where

$$\rho^{\otimes n} = \rho \otimes \cdots \otimes \rho \quad (n \text{ times}).$$

What we will show is that for large n, compression will be possible for $\alpha > S(\rho)$ and impossible for $\alpha < S(\rho)$.

To speak more precisely about what is meant by quantum compression and decompression, let us consider that $\alpha > 0$ has been fixed, let $m = \lfloor \alpha n \rfloor$, and let $\mathsf{Y}_1, \ldots, \mathsf{Y}_m$ be qubit registers, meaning that their associated spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_m$ are each equal to $\mathbb{C}^\Gamma$, for $\Gamma = \{0, 1\}$. Alice's compression mapping will be a channel

$$\Phi \in \mathrm{C}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m)$$

and Bob's decompression mapping will be a channel

$$\Psi \in \mathrm{C}(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m, \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n).$$

Now, we need to be careful about how we measure the accuracy of quantum compression schemes. Our assumption on the state of $(\mathsf{X}_1, \mathsf{X}_2, \ldots, \mathsf{X}_n)$ does not rule out the existence of other registers that these registers may be entangled or otherwise correlated with—so let us imagine that there exists another register Z, and that the initial state of $(\mathsf{X}_1, \mathsf{X}_2, \ldots, \mathsf{X}_n, \mathsf{Z})$ is

$$\xi \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n \otimes \mathcal{Z}).$$

When Alice compresses and Bob decompresses $\mathsf{X}_1, \ldots, \mathsf{X}_n$, the resulting state of $(\mathsf{X}_1, \mathsf{X}_2, \ldots, \mathsf{X}_n, \mathsf{Z})$ is given by

$$\Big(\Psi\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}\Big)(\xi).$$

For the compression to be successful, we require that this density operator is close to ξ. This must in fact hold for all choices of Z and ξ, provided that the assumption $\mathrm{Tr}_{\mathcal{Z}}(\xi) = \rho^{\otimes n}$ is met. There is nothing unreasonable about this assumption—it is the natural quantum analogue to requiring that $g(f(a_1 \cdots a_n)) = a_1 \cdots a_n$ for classical compression.

It might seem complicated that we have to worry about all possible registers Z and all $\xi \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n \otimes \mathcal{Z})$ that satisfy $\mathrm{Tr}_{\mathcal{Z}}(\xi) = \rho^{\otimes n}$, but in fact it will be simple if we make use of the notion of *channel fidelity*.

9.4.2 Quantum channel fidelity

Consider a channel $\Xi \in \mathrm{C}(\mathcal{W})$ for some complex Euclidean space $\mathcal{W}$, and let $\sigma \in \mathrm{D}(\mathcal{W})$ be a density operator on this space. We define the *channel fidelity* between Ξ and σ to be

$$\mathrm{F}_{\text{channel}}(\Xi, \sigma) = \inf\{\mathrm{F}(\xi, (\Xi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(\xi))\},$$

where the infimum is over all complex Euclidean spaces $\mathcal{Z}$ and all $\xi \in \mathrm{D}(\mathcal{W} \otimes \mathcal{Z})$ satisfying $\mathrm{Tr}_{\mathcal{Z}}(\xi) = \sigma$. The channel fidelity $\mathrm{F}_{\text{channel}}(\Xi, \sigma)$ places a lower bound on the fidelity of the input and output of a given channel Ξ provided that it acts on a part of a larger system whose state is σ when restricted to the part on which Ξ acts.

It is not difficult to prove that the infimum in the definition of the channel fidelity may be restricted to pure states $\xi = uu^*$, given that we could always purify a given ξ (possibly replacing $\mathcal{Z}$ with a larger space) and use the fact that the fidelity function is non-decreasing under partial tracing. With this in mind, consider any complex Euclidean space $\mathcal{Z}$, let $u \in \mathcal{W} \otimes \mathcal{Z}$ be any purification of σ, and consider the fidelity

$$\mathrm{F}\left(uu^*, \left(\Xi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}\right)(uu^*)\right) = \sqrt{\left\langle uu^*, \left(\Xi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}\right)(uu^*)\right\rangle}.$$

The purification $u \in \mathcal{W} \otimes \mathcal{Z}$ of σ must take the form

$$u = \mathrm{vec}\left(\sqrt{\sigma} B\right)$$

for some operator $B \in \mathrm{L}(\mathcal{Z}, \mathcal{W})$ satisfying $BB^* = \Pi_{\mathrm{im}(\sigma)}$. Assuming that

$$\Xi(X) = \sum_{j=1}^{k} A_j X A_j^*$$

is a Kraus representation of Ξ, it therefore holds that

$$\mathrm{F}\left(uu^*, \left(\Xi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})}\right)(uu^*)\right) = \sqrt{\sum_{j=1}^{k} \left|\left\langle \sqrt{\sigma} B, A_j \sqrt{\sigma} B \right\rangle\right|^2} = \sqrt{\sum_{j=1}^{k} \left|\left\langle \sigma, A_j \right\rangle\right|^2}.$$

So, it turns out that this quantity is independent of the particular purification of σ that was chosen, and we find that we could alternately have defined the channel fidelity of Ξ with σ as

$$\mathrm{F}_{\text{channel}}(\Xi, \sigma) = \sqrt{\sum_{j=1}^{k} \left|\left\langle \sigma, A_j \right\rangle\right|^2}.$$

9.4.3 Schumacher's quantum source coding theorem

We now have the required tools to establish the relationship between the von Neumann entropy and quantum compression that was discussed earlier in the lecture. Using the same notation that was introduced above, let us say that a pair of channels

$$\Phi \in \mathrm{C}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m),$$
$$\Psi \in \mathrm{C}(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m, \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$$

is an (n, α, δ)-*quantum compression scheme* for $\rho \in \mathrm{D}(\mathcal{X})$ if $m = \lfloor \alpha n \rfloor$ and

$$\mathrm{F}_{\text{channel}}\left(\Psi\Phi, \rho^{\otimes n}\right) > 1 - \delta.$$

The following theorem, which is the quantum analogue to Shannon's source coding theorem, establishes conditions on α for which quantum compression is possible and impossible.

Theorem 9.5 (Schumacher)**.** *Let $\rho \in \mathrm{D}(\mathcal{X})$ be a density operator, let $\alpha > 0$ and let $\delta \in (0, 1)$. The following statements hold.*

1. *If $\alpha > S(\rho)$, then there exists an (n, α, δ)-quantum compression scheme for ρ for all but finitely many choices of $n \in \mathbb{N}$.*
2. *If $\alpha < S(\rho)$, then there exists an (n, α, δ)-quantum compression scheme for ρ for at most finitely many choices of $n \in \mathbb{N}$.*

Proof. Assume first that $\alpha > S(\rho)$. We begin by defining a quantum analogue of the set of typical strings, which is the *typical subspace*. This notion is based on a spectral decomposition

$$\rho = \sum_{a \in \Sigma} p(a) u_a u_a^*.$$

As p is a probability vector, we may consider for each $n \geq 1$ the set of ε-typical strings $T_{n,\varepsilon} \subseteq \Sigma^n$ for this distribution. In particular, we form the projection onto the *typical subspace*:

$$\Pi_{n,\varepsilon} = \sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} u_{a_1} u_{a_1}^* \otimes \cdots \otimes u_{a_n} u_{a_n}^*.$$

Notice that

$$\left\langle \Pi_{n,\varepsilon}, \rho^{\otimes n} \right\rangle = \sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} p(a_1) \cdots p(a_n),$$

and therefore

$$\lim_{n \to \infty} \left\langle \Pi_{n,\varepsilon}, \rho^{\otimes m} \right\rangle = 1,$$

for every choice of $\varepsilon > 0$.

We can now move on to describing a sequence of compression schemes that will suffice to prove the theorem, provided that $\alpha > S(\rho) = H(p)$. By Shannon's source coding theorem (or, to be more precise, our proof of that theorem) we may assume, for sufficiently large n, that we have a classical (n, α, ε)-compression scheme (f, g) for p that satisfies

$$g(f(a_1 \cdots a_n)) = a_1 \cdots a_n$$

for all $a_1 \cdots a_n \in T_{n,\varepsilon}$. Define a linear operator

$$A \in \mathrm{L}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m\right)$$

as

$$A = \sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} e_{f(a_1 \cdots a_n)} (u_{a_1} \otimes \cdots \otimes u_{a_n})^*.$$

for each $a_1 \cdots a_n \in \Sigma^n$. Notice that

$$A^* A = \Pi_{n,\varepsilon}.$$

Now, the mapping defined by $X \mapsto AXA^*$ is completely positive but generally not trace-preserving. However, it is a *sub-channel*, by which it is meant that there must exist a completely positive mapping Ξ for which

$$\Phi(X) = AXA^* + \Xi(X) \tag{9.3}$$

is a channel. For instance, we may take

$$\Xi(X) = \langle \mathbb{1} - \Pi_{n,\varepsilon}, X \rangle \, \sigma$$

for some arbitrary choice of $\sigma \in \mathrm{D}(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m)$. Likewise, the mapping $Y \mapsto A^*YA$ is also a sub-channel, meaning that there must exist a completely positive map Δ for which

$$\Psi(Y) = A^*YA + \Delta(Y) \tag{9.4}$$

is a channel.

It remains to argue that, for sufficiently large n, that the pair (Φ, Ψ) is an (n, α, δ)-quantum compression scheme for any constant $\delta > 0$. From the above expressions (9.3) and (9.4) it is clear that there exists a Kraus representation of $\Psi\Phi$ having the form

$$(\Psi\Phi)(X) = (A^*A)X(A^*A)^* + \sum_{j=1}^{k} B_j X B_j^*$$

for some collection of operators $B_1, \ldots, B_k$ that we do not really care about. It follows that

$$\mathrm{F}_{\text{channel}}(\Psi\Phi, \rho^{\otimes n}) \geq \left| \left\langle \rho^{\otimes n}, A^*A \right\rangle \right| = \left\langle \rho^{\otimes n}, \Pi_{n,\varepsilon} \right\rangle.$$

This quantity approaches 1 in the limit, as we have observed, and therefore for sufficiently large n it must hold that (Φ, Ψ) is an (n, α, δ) quantum compression scheme.

Now consider the case where $\alpha < S(\rho)$. Note that if $\Pi_n \in \mathrm{Pos}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$ is a projection with rank at most $2^{n(S(\rho)-\varepsilon)}$ for each $n \geq 1$, then

$$\lim_{n \to \infty} \left\langle \Pi_n, \rho^{\otimes n} \right\rangle = 0. \tag{9.5}$$

This is because, for any positive semidefinite operator P, the maximum value of $\langle \Pi, P \rangle$ over all choices of orthogonal projections Π with $\mathrm{rank}(\Pi) \leq r$ is precisely the sum of the r largest eigenvalues of P. The eigenvalues of $\rho^{\otimes n}$ are the values $p(a_1) \cdots p(a_n)$ over all choices of $a_1 \cdots a_n \in \Sigma^n$, so for each n we have

$$\left\langle \Pi_n, \rho^{\otimes n} \right\rangle \leq \sum_{a_1 \cdots a_n \in G_n} p(a_1) \cdots p(a_n)$$

for some set G_n of size at most $2^{n(S(\rho)-\varepsilon)}$. At this point the equation (9.5) follows by similar reasoning to the proof of Theorem 9.2.

Now let us suppose, for each $n \geq 1$ and for $m = \lfloor \alpha n \rfloor$, that

$$\Phi_n \in \mathrm{C}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m),$$
$$\Psi_n \in \mathrm{C}(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m, \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$$

are channels. Our goal is to prove that (Φ_n, Ψ_n) fails as a quantum compression scheme for all sufficiently large values of n.

Fix $n \geq 1$, and consider Kraus representations

$$\Phi_n(X) = \sum_{j=1}^{k} A_j X A_j^* \qquad \text{and} \qquad \Psi_n(X) = \sum_{j=1}^{k} B_j X B_j^*,$$

where

$$A_1, \ldots, A_k \in \mathrm{L}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m\right),$$
$$B_1, \ldots, B_k \in \mathrm{L}\left(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m, \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right),$$

and where the assumption that they have the same number of terms is easily made without loss of generality. Let Π_j be the projection onto the range of B_j for each $j = 1, \ldots k$, and note that it obviously holds that

$$\operatorname{rank}(\Pi_j) \leq \dim(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_m) = 2^m.$$

By the Cauchy-Schwarz inequality, we have

$$\begin{aligned}
\mathrm{F}_{\text{channel}}(\Psi_n \Phi_n, \rho^{\otimes n})^2 &= \sum_{i,j} \left| \left\langle \rho^{\otimes n}, B_j A_i \right\rangle \right|^2 \\
&= \sum_{i,j} \left| \left\langle \Pi_j \sqrt{\rho^{\otimes n}}, B_j A_i \sqrt{\rho^{\otimes n}} \right\rangle \right|^2 \\
&\leq \sum_{i,j} \left\langle \Pi_j, \rho^{\otimes n} \right\rangle \left(\operatorname{Tr} B_j A_i \rho^{\otimes n} A_i^* B_j^* \right).
\end{aligned}$$

As

$$\operatorname{Tr}\left(B_j A_i \rho^{\otimes n} A_i^* B_j^* \right) \geq 0$$

for each i, j, and

$$\sum_{i,j} \operatorname{Tr}\left(B_j A_i \rho^{\otimes n} A_i^* B_j^* \right) = \operatorname{Tr}(\Psi \Phi(\rho^{\otimes n})) = 1,$$

it follows that

$$\mathrm{F}_{\text{channel}}(\Psi_n \Phi_n, \rho^{\otimes n})^2 \in \operatorname{conv}\left(\left\{ \left\langle \Pi_j, \rho^{\otimes n} \right\rangle \,:\, j = 1, \ldots, k \right\} \right).$$

As each Π_j has rank at most 2^m, it follows that

$$\lim_{n \to \infty} \mathrm{F}_{\text{channel}}(\Psi_n \Phi_n, \rho^{\otimes n}) = 0.$$

So, for all but finitely many choices of n, the pair (Φ_n, Ψ_n) fails to be an (n, α, δ) quantum compression scheme. □

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

Lecture 10: Continuity of von Neumann entropy; quantum relative entropy

In the previous lecture we defined the Shannon and von Neumann entropy functions, and established the fundamental connection between these functions and the notion of compression. In this lecture and the next we will look more closely at the von Neumann entropy in order to establish some basic properties of this function, as well as an important related function called the *quantum relative entropy*.

10.1 Continuity of von Neumann entropy

The first property we will establish about the von Neumann entropy is that it is continuous everywhere on its domain.

First, let us define a real valued function $\eta : [0, \infty) \to \mathbb{R}$ as follows:

$$\eta(\lambda) = \begin{cases} -\lambda \ln(\lambda) & \lambda > 0 \\ 0 & \lambda = 0. \end{cases}$$

This function is continuous everywhere on its domain, and derivatives of all orders exist for all positive real numbers. In particular we have $\eta'(\lambda) = -(1 + \ln(\lambda))$ and $\eta''(\lambda) = -1/\lambda$. A plot of the function η is shown in Figure 10.1, and its first derivative η' is plotted in Figure 10.2.

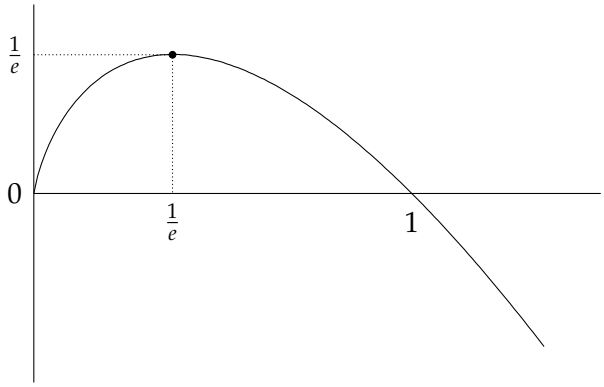

Figure 10.1: A plot of the function $\eta(\lambda) = -\lambda \ln(\lambda)$.

The fact that η is continuous on $[0, \infty)$ implies that for every finite, nonempty set Σ the Shannon entropy is continuous at every point on $[0, \infty)^{\Sigma}$, as

$$H(p) = \frac{1}{\ln(2)} \sum_{a \in \Sigma} \eta(p(a)).$$

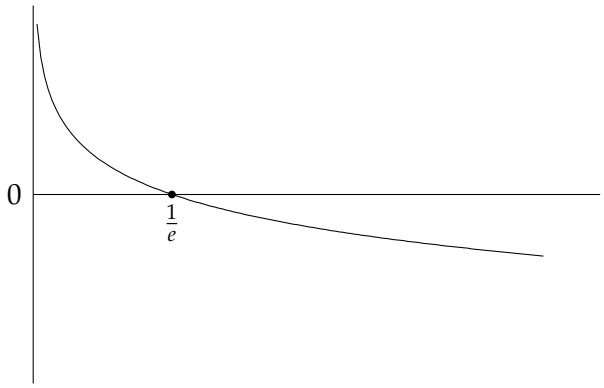

Figure 10.2: A plot of the function $\eta'(\lambda) = -(1 + \ln(\lambda))$.

We are usually only interested in $H(p)$ for probability vectors p, but of course the function is defined on vectors having nonnegative real entries.

Now, to prove that the von Neumann entropy is continuous, we will first prove the following theorem, which establishes one specific sense in which the eigenvalues of a Hermitian operator vary continuously as a function of an operator. We don't really need the precise bound that this theorem establishes—all we really need is that eigenvalues vary continuously as an operator varies, which is somewhat easier to prove and does not require Hermiticity—but we'll take the opportunity to state the theorem because it is interesting in its own right.

Theorem 10.1. *Let $\mathcal{X}$ be a complex Euclidean space and let $A, B \in \mathrm{Herm}(\mathcal{X})$ be Hermitian operators. It holds that*

$$\|\lambda(A) - \lambda(B)\|_1 \leq \|A - B\|_1 .$$

To prove this theorem, we need another fact about eigenvalues of operators, but this one we will take as given. (You can find proofs in several books on matrix analysis.)

Theorem 10.2 (Weyl's monotonicity theorem)**.** *Let $\mathcal{X}$ be a complex Euclidean space and let $A, B \in \mathrm{Herm}(\mathcal{X})$ satisfy $A \leq B$. It holds that $\lambda_j(A) \leq \lambda_j(B)$ for $1 \leq j \leq \dim(\mathcal{X})$.*

Proof of Theorem 10.1. Let $n = \dim(\mathcal{X})$. Using the spectral decomposition of $A - B$, it is possible to define two positive semidefinite operators $P, Q \in \mathrm{Pos}(\mathcal{X})$ such that:

1. $PQ = 0$, and
2. $P - Q = A - B$.

(An expression of a given Hermitian operator as $P - Q$ for such a choice of P and Q is sometimes called a *Jordan–Hahn decomposition* of that operator.) Notice that $\|A - B\|_1 = \mathrm{Tr}(P) + \mathrm{Tr}(Q)$.

Now, define one more Hermitian operator

$$X = P + B = Q + A.$$

We have $X \geq A$, and therefore $\lambda_j(X) \geq \lambda_j(A)$ for $1 \leq j \leq n$ by Weyl's monotonicity theorem. Similarly, it holds that $\lambda_j(X) \geq \lambda_j(B)$ for $1 \leq j \leq n = \dim(\mathcal{X})$. By considering the two possible cases $\lambda_j(A) \geq \lambda_j(B)$ and $\lambda_j(A) \leq \lambda_j(B)$, we therefore find that

$$\big|\lambda_j(A) - \lambda_j(B)\big| \leq 2\lambda_j(X) - (\lambda_j(A) + \lambda_j(B))$$

for $1 \leq j \leq n$. Thus,

$$\|\lambda(A) - \lambda(B)\|_1 = \sum_{j=1}^{n} \big|\lambda_j(A) - \lambda_j(B)\big| \geq \mathrm{Tr}(2X - A - B) = \mathrm{Tr}(P + Q) = \|A - B\|_1$$

as required. □

With the above fact in hand, it is immediate from the expression $S(P) = H(\lambda(P))$ that the von Neumann entropy is continuous (as it is a composition of two continuous functions).

Theorem 10.3. *For every complex Euclidean space $\mathcal{X}$, the von Neumann entropy $S(P)$ is continuous at every point $P \in \mathrm{Pos}(\mathcal{X})$.*

Let us next prove Fannes' inequality, which may be viewed as a quantitative statement concerning the continuity of the von Neumann entropy. To begin, we will use some basic calculus to prove a fact about the function η.

Lemma 10.4. *Suppose α and β are real numbers satisfying $0 \leq \alpha \leq \beta \leq 1$ and $\beta - \alpha \leq 1/2$. It holds that*

$$|\eta(\beta) - \eta(\alpha)| \leq \eta(\beta - \alpha).$$

Proof. Consider the function $\eta'(\lambda) = -(1 + \ln(\lambda))$, which is plotted in Figure 10.2. Given that η' is monotonically decreasing on its domain $(0, \infty)$, it holds that the function

$$f(\lambda) = \int_{\lambda}^{\lambda+\gamma} \eta'(t)dt = \eta(\lambda + \gamma) - \eta(\lambda)$$

is monotonically non-increasing for any choice of $\gamma \geq 0$. This means that the maximum value of $|f(\lambda)|$ over the range $\lambda = [0, 1 - \gamma]$ must occur at either $\lambda = 0$ or $\lambda = 1 - \gamma$, and so for λ in this range we have

$$|\eta(\lambda + \gamma) - \eta(\lambda)| \leq \max\{\eta(\gamma), \eta(1 - \gamma)\}.$$

Here we have used the fact that $\eta(1) = 0$ and $\eta(\lambda) \geq 0$ for $\lambda \in [0, 1]$.

To complete the proof it suffices to prove that $\eta(\gamma) \geq \eta(1 - \gamma)$ for $\gamma \in [0, 1/2]$. This claim is certainly supported by the plot in Figure 10.1, but we can easily prove it analytically. Define a function $g(\lambda) = \eta(\lambda) - \eta(1 - \lambda)$. We see that g happens to have zeroes at $\lambda = 0$ and $\lambda = 1/2$, and were there an additional zero λ of g in the range $(0, 1/2)$, then we would have two distinct values $\delta_1, \delta_2 \in (0, 1/2)$ for which $g'(\delta_1) = g'(\delta_2) = 0$ by the mean value theorem. This, however, is in contradiction with the fact that the second derivative $g''(\lambda) = \frac{1}{1-\lambda} - \frac{1}{\lambda}$ of g is strictly negative in the range $(0, 1/2)$. As $g(1/4) > 0$, for instance, we have that $g(\lambda) \geq 0$ for $\lambda \in [0, 1/2]$ as required. □

Theorem 10.5 (Fannes Inequality)**.** *Let $\mathcal{X}$ be a complex Euclidean space and let $n = \dim(\mathcal{X})$. For all density operators $\rho, \xi \in \mathrm{D}(\mathcal{X})$ such that $\|\rho - \xi\|_1 \leq 1/e$ it holds that*

$$|S(\rho) - S(\xi)| \leq \log(n) \|\rho - \xi\|_1 + \frac{1}{\ln(2)} \eta(\|\rho - \xi\|_1).$$

Proof. Define

$$\varepsilon_i = |\lambda_i(\rho) - \lambda_i(\xi)|$$

and let $\varepsilon = \varepsilon_1 + \cdots + \varepsilon_n$. Note that $\varepsilon_i \leq \|\rho - \xi\|_1 \leq 1/e < 1/2$ for each i, and therefore

$$|S(\rho) - S(\xi)| = \frac{1}{\ln(2)} \left| \sum_{i=1}^{n} \eta(\lambda_i(\rho)) - \eta(\lambda_i(\xi)) \right| \leq \frac{1}{\ln(2)} \sum_{i=1}^{n} \eta(\varepsilon_i)$$

by Lemma 10.4.

For any positive α and β we have $\beta\eta(\alpha/\beta) = \eta(\alpha) + \alpha\ln(\beta)$, so

$$\frac{1}{\ln(2)} \sum_{i=1}^{n} \eta(\varepsilon_i) = \frac{1}{\ln(2)} \sum_{i=1}^{n} (\varepsilon\eta(\varepsilon_i/\varepsilon) - \varepsilon_i \ln(\varepsilon)) = \frac{\varepsilon}{\ln(2)} \sum_{i=1}^{n} \eta(\varepsilon_i/\varepsilon) + \frac{1}{\ln(2)}\eta(\varepsilon).$$

Because $(\varepsilon_1/\varepsilon, \ldots, \varepsilon_n/\varepsilon)$ is a probability vector this gives

$$|S(\rho) - S(\xi)| \leq \varepsilon \log(n) + \frac{1}{\ln(2)}\eta(\varepsilon).$$

We have that $\varepsilon \leq \|\rho - \xi\|_1$, and that η is monotone increasing on the interval $[0, 1/e]$, so

$$|S(\rho) - S(\xi)| \leq \log(n) \|\rho - \xi\|_1 + \frac{1}{\ln(2)}\eta(\|\rho - \xi\|_1),$$

which completes the proof. □

10.2 Quantum relative entropy

Next we will introduce a new function, which is indispensable as a tool for studying the von Neumann entropy: the *quantum relative entropy*. For two positive definite operators $P, Q \in \mathrm{Pd}(\mathcal{X})$ we define the quantum relative entropy of P with Q as follows:

$$S(P\|Q) = \mathrm{Tr}(P\log(P)) - \mathrm{Tr}(P\log(Q)). \tag{10.1}$$

We usually only care about the quantum relative entropy for density operators, but there is nothing that prevents us from allowing the definition to hold for all positive definite operators.

We may also define the quantum relative entropy for positive semidefinite operators that are not positive definite, provided we are willing to have an extended real-valued function. Specifically, if there exists a vector $u \in \mathcal{X}$ such that $u^*Qu = 0$ and $u^*Pu \neq 0$, or (equivalently) when

$$\ker(Q) \not\subseteq \ker(P),$$

we define $S(P\|Q) = \infty$. Otherwise, there is no difficulty in evaluating the above expression (10.1) by following the usual convention of setting $0\log(0) = 0$. Nevertheless, it will typically not be necessary for us to give up the convenience of restricting our attention to positive definite operators. This is because we already know that the von Neumann entropy function is continuous, and we will mostly use the quantum relative entropy in this course to establish facts about the von Neumann entropy.

The quantum relative entropy $S(P\|Q)$ can be negative for some choices of P and Q, but not when they are density operators (or more generally when $\mathrm{Tr}(P) = \mathrm{Tr}(Q)$). The following theorem establishes that this is so, and in fact that the value of the quantum relative entropy of two density operators is zero if and only if they are equal.

Theorem 10.6. *Let $\rho, \xi \in \mathrm{D}(\mathcal{X})$ be positive definite density operators. It holds that*

$$S(\rho\|\xi) \geq \frac{1}{2\ln(2)} \|\rho - \xi\|_2^2.$$

Proof. Let us first note that for every choice of $\alpha, \beta \in (0,1)$ we have

$$\alpha \ln(\alpha) - \alpha \ln(\beta) = (\alpha - \beta)\eta'(\beta) + \eta(\beta) - \eta(\alpha) + \alpha - \beta.$$

Moreover, by Taylor's Theorem, we have that

$$(\alpha - \beta)\eta'(\beta) + \eta(\beta) - \eta(\alpha) = -\frac{1}{2}\eta''(\gamma)(\alpha - \beta)^2$$

for some choice of γ lying between α and β.

Now, let $n = \dim(\mathcal{X})$ and let

$$\rho = \sum_{i=1}^{n} p_i x_i x_i^* \quad \text{and} \quad \xi = \sum_{i=1}^{n} q_i y_i y_i^*$$

be spectral decompositions of ρ and ξ. The assumption that ρ and ξ are positive definite density operators implies that p_i and q_i are positive for $1 \leq i \leq n$. Applying the facts observed above, we have that

$$\begin{aligned} S(\rho\|\xi) &= \frac{1}{\ln(2)} \sum_{1 \leq i,j \leq n} |\langle x_i, y_j \rangle|^2 \left(p_i \ln(p_i) - p_i \ln(q_j)\right) \\ &= \frac{1}{\ln(2)} \sum_{1 \leq i,j \leq n} |\langle x_i, y_j \rangle|^2 \left(q_j - p_i - \frac{1}{2}\eta''(\gamma_{ij})(p_i - q_j)^2\right) \end{aligned}$$

for some choice of real numbers $\{\gamma_{ij}\}$, where each γ_{ij} lies between p_i and q_j. In particular, this means that $0 < \gamma_{ij} \leq 1$, implying that $-\eta''(\gamma_{ij}) \geq 1$, for each choice of i and j. Consequently we have

$$S(\rho\|\xi) \geq \frac{1}{2\ln(2)} \sum_{1 \leq i,j \leq n} |\langle x_i, y_j \rangle|^2 (p_i - q_j)^2 = \frac{1}{2\ln(2)} \|\rho - \xi\|_2^2$$

as required. □

The following corollary represents a simple application of this fact. (We could just as easily prove it using analogous facts about the Shannon entropy, but the proof is essentially the same.)

Corollary 10.7. *Let $\mathcal{X}$ be a complex Euclidean space and let $n = \dim(\mathcal{X})$. It holds that $0 \leq S(\rho) \leq \log(n)$ for all $\rho \in \mathrm{D}(\mathcal{X})$. Furthermore, $\rho = \mathbb{1}/n$ is the unique density operator in $\mathrm{D}(\mathcal{X})$ having von Neumann entropy equal to $\log(n)$.*

Proof. The vector of eigenvalues $\lambda(\rho)$ of any density operator $\rho \in \mathrm{D}(\mathcal{X})$ is a probability vector, so $S(\rho) = H(\lambda(\rho))$ is a sum of nonnegative terms, which implies $S(\rho) \geq 0$. To prove the upper bound, let us assume ρ is a positive definite density operator, and consider the relative entropy $S(\rho\|\mathbb{1}/n)$. We have

$$0 \leq S(\rho\|\mathbb{1}/n) = -S(\rho) - \log(1/n)\,\mathrm{Tr}(\rho) = -S(\rho) + \log(n).$$

Therefore $S(\rho) \leq \log(n)$, and when ρ is not equal to $\mathbb{1}/n$ the inequality becomes strict. For density operators ρ that are not positive definite, the result follows from the continuity of von Neumann entropy. □

Now let us prove two simple properties of the von Neumann entropy: *subadditivity* and *concavity*. These properties also hold for the Shannon entropy—and while it is not difficult to prove them directly for the Shannon entropy, we get the properties for free once they are established for the von Neumann entropy.

When we refer to the von Neumann entropy of some collection of registers, we mean the von Neumann entropy of the state of those registers at some instant. For example, if X and Y are registers and $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ is the state of the pair (X, Y) at some instant, then

$$S(\mathsf{X}, \mathsf{Y}) = S(\rho), \quad S(\mathsf{X}) = S(\rho^{\mathsf{X}}), \quad \text{and} \quad S(\mathsf{Y}) = S(\rho^{\mathsf{Y}}),$$

where, in accordance with standard conventions, we have written $\rho^{\mathsf{X}} = \mathrm{Tr}_{\mathcal{Y}}(\rho)$ and $\rho^{\mathsf{Y}} = \mathrm{Tr}_{\mathcal{X}}(\rho)$. We often state properties of the von Neumann entropy in terms of registers, with the understanding that whatever statement is being discussed holds for all or some specified subset of the possible states of these registers. A similar convention is used for the Shannon entropy (for classical registers).

Theorem 10.8 (Subadditivity of von Neumann entropy)**.** *Let* X *and* Y *be quantum registers. For every state of the pair* (X, Y) *we have*

$$S(\mathsf{X}, \mathsf{Y}) \leq S(\mathsf{X}) + S(\mathsf{Y}).$$

Proof. Assume that the state of the pair (X, Y) is $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$. We will prove the theorem for ρ positive definite, from which the general case follows by continuity.

Consider the quantum relative entropy $S(\rho^{\mathsf{XY}} \| \rho^{\mathsf{X}} \otimes \rho^{\mathsf{Y}})$. Using the formula

$$\log(P \otimes Q) = \log(P) \otimes \mathbb{1} + \mathbb{1} \otimes \log(Q)$$

we find that

$$S(\rho^{\mathsf{XY}} \| \rho^{\mathsf{X}} \otimes \rho^{\mathsf{Y}}) = -S(\rho^{\mathsf{XY}}) + S(\rho^{\mathsf{X}}) + S(\rho^{\mathsf{Y}}).$$

By Theorem 10.6 we have $S(\rho^{\mathsf{XY}} \| \rho^{\mathsf{X}} \otimes \rho^{\mathsf{Y}}) \geq 0$, which completes the proof. □

In the next lecture we will prove a much stronger version of subadditivity, which is aptly named: *strong subadditivity*. It will imply the truth of the previous theorem, but it is instructive to compare the very easy proof above with the much more difficult proof of strong subadditivity.

Subadditivity also holds for the Shannon entropy:

$$H(\mathsf{X}, \mathsf{Y}) \leq H(\mathsf{X}) + H(\mathsf{Y})$$

for any choice of classical registers X and Y. This is simply a special case of the above theorem, where the density operator ρ is diagonal with respect to the standard basis of $\mathcal{X} \otimes \mathcal{Y}$.

Subadditivity implies that the von Neumann entropy is concave, as is established by the proof of the following theorem.

Theorem 10.9 (Concavity of von Neumann entropy)**.** *Let* $\rho, \xi \in \mathrm{D}(\mathcal{X})$ *and* $\lambda \in [0, 1]$*. It holds that*

$$S(\lambda\rho + (1-\lambda)\xi) \geq \lambda S(\rho) + (1-\lambda) S(\xi).$$

Proof. Let Y be a register corresponding to a single qubit, so that its associated space is $\mathcal{Y} = \mathbb{C}^{\{0,1\}}$. Consider the density operator

$$\sigma = \lambda\rho \otimes E_{0,0} + (1-\lambda)\xi \otimes E_{1,1},$$

and suppose that the state of the registers (X, Y) is described by σ. We have

$$S(\mathsf{X}, \mathsf{Y}) = \lambda S(\rho) + (1 - \lambda) S(\xi) + H(\lambda),$$

which is easily established by considering spectral decompositions of ρ and ξ. (Here we have referred to the *binary entropy function* $H(\lambda) = -\lambda \log(\lambda) - (1 - \lambda) \log(1 - \lambda)$.) Furthermore, we have

$$S(\mathsf{X}) = S(\lambda \rho + (1 - \lambda) \xi)$$

and

$$S(\mathsf{Y}) = H(\lambda).$$

It follows by subadditivity that

$$\lambda S(\rho) + (1 - \lambda) S(\xi) + H(\lambda) \leq S(\lambda \rho + (1 - \lambda) \xi) + H(\lambda)$$

which proves the theorem. □

Concavity also holds for the Shannon entropy as a simple consequence of this theorem, as we may take ρ and ξ to be diagonal with respect to the standard basis.

10.3 Conditional entropy and mutual information

Let us finish off the lecture by defining a few more quantities associated with the von Neumann entropy. We will not be able to say very much about these quantities until after we prove strong subadditivity in the next lecture.

Classically we define the *conditional Shannon entropy* as follows for two classical registers X and Y:

$$H(\mathsf{X}|\mathsf{Y}) = \sum_a \Pr[\mathsf{Y} = a] H(\mathsf{X}|\mathsf{Y} = a).$$

This quantity represents the expected value of the entropy of X given that you know the value of Y. It is not hard to prove that

$$H(\mathsf{X}|\mathsf{Y}) = H(\mathsf{X}, \mathsf{Y}) - H(\mathsf{Y}).$$

It follows from subadditivity that

$$H(\mathsf{X}|\mathsf{Y}) \leq H(\mathsf{X}).$$

The intuition is that your uncertainty can only increase when you know less.

In the quantum setting the first definition does not really make sense, so we use the second fact as our definition—the *conditional von Neumann entropy* of X given Y is

$$S(\mathsf{X}|\mathsf{Y}) = S(\mathsf{X}, \mathsf{Y}) - S(\mathsf{Y}).$$

Now we start to see some strangeness: we can have $S(\mathsf{Y}) > S(\mathsf{X}, \mathsf{Y})$, as we will if (X, Y) is in a pure, non-product state. This means that $S(\mathsf{X}|\mathsf{Y})$ can be negative, but such is life.

Next, the (classical) *mutual information* between two classical registers X and Y is defined as

$$I(\mathsf{X} : \mathsf{Y}) = H(\mathsf{X}) + H(\mathsf{Y}) - H(\mathsf{X}, \mathsf{Y}).$$

This can alternately be expressed as

$$I(\mathsf{X} : \mathsf{Y}) = H(\mathsf{Y}) - H(\mathsf{Y}|\mathsf{X}) = H(\mathsf{X}) - H(\mathsf{X}|\mathsf{Y}).$$

We view this quantity as representing the amount of information in X about Y and vice versa. The *quantum mutual information* is defined similarly:

$$S(\mathsf{X} : \mathsf{Y}) = S(\mathsf{X}) + S(\mathsf{Y}) - S(\mathsf{X}, \mathsf{Y}).$$

At least we know from subadditivity that this quantity is always nonnegative. We will, however, need to further develop our understanding before we can safely associate any intuition with this quantity.

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

Lecture 11: Strong subadditivity of von Neumann entropy

In this lecture we will prove a fundamental fact about the von Neumann entropy, known as *strong subadditivity*. Let us begin with a precise statement of this fact.

Theorem 11.1 (Strong subadditivity of von Neumann entropy)**.** *Let* X*,* Y*, and* Z *be registers. For every state* $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z})$ *of these registers it holds that*

$$S(\mathsf{X},\mathsf{Y},\mathsf{Z}) + S(\mathsf{Z}) \leq S(\mathsf{X},\mathsf{Z}) + S(\mathsf{Y},\mathsf{Z}).$$

There are multiple known ways to prove this theorem. The approach we will take is to first establish a property of the quantum relative entropy, known as *joint convexity*. Once we establish this property, it will be straightforward to prove strong subadditivity.

11.1 Joint convexity of the quantum relative entropy

We will now prove that the quantum relative entropy is jointly convex, as is stated by the following theorem.

Theorem 11.2 (Joint convexity of the quantum relative entropy)**.** *Let* $\mathcal{X}$ *be a complex Euclidean space, let* $\rho_0, \rho_1, \sigma_0, \sigma_1 \in \mathrm{D}(\mathcal{X})$ *be positive definite density operators, and let* $\lambda \in [0,1]$*. It holds that*

$$S(\lambda\rho_0 + (1-\lambda)\rho_1 \| \lambda\sigma_0 + (1-\lambda)\sigma_1) \leq \lambda\, S(\rho_0\|\sigma_0) + (1-\lambda)\, S(\rho_1\|\sigma_1).$$

The proof of Theorem 11.2 that we will study is fairly standard and has the nice property of being elementary. It is, however, relatively complicated, so we will need to break it up into a few pieces.

Before considering the proof, let us note that the theorem remains true if we allow ρ_0, ρ_1, σ_0, and σ_1 to be arbitrary density operators, provided we allow the quantum relative entropy to take infinite values as we discussed in the previous lecture. Supposing that we do this, we see that if either $S(\rho_0\|\sigma_0)$ or $S(\rho_1\|\sigma_1)$ is infinite, there is nothing to prove. If it is the case that $S(\lambda\rho_0 + (1-\lambda)\rho_1\|\lambda\sigma_0 + (1-\lambda)\sigma_1)$ is infinite, then either $S(\rho_0\|\sigma_0)$ or $S(\rho_1\|\sigma_1)$ is infinite as well: if $\lambda \in (0,1)$, then $\ker(\lambda\rho_0 + (1-\lambda)\rho_1) = \ker(\rho_0) \cap \ker(\rho_1)$ and $\ker(\lambda\sigma_0 + (1-\lambda)\sigma_1) = \ker(\sigma_0) \cap \ker(\sigma_1)$, owing to the fact that ρ_0, ρ_1, σ_0, and σ_1 are all positive semidefinite; and so

$$\ker(\lambda\sigma_0 + (1-\lambda)\sigma_1) \not\subseteq \ker(\lambda\rho_0 + (1-\lambda)\rho_1)$$

implies $\ker(\sigma_0) \not\subseteq \ker(\rho_0)$ or $\ker(\sigma_1) \not\subseteq \ker(\rho_1)$ (or both). In the remaining case, which is that $S(\lambda\rho_0 + (1-\lambda)\rho_1\|\lambda\sigma_0 + (1-\lambda)\sigma_1)$, $S(\rho_0\|\sigma_0)$, and $S(\rho_1\|\sigma_1)$ are all finite, a fairly straightforward continuity argument will establish the inequality from the one stated in the theorem.

Now, to prove the theorem, the first step is to consider a real-valued function $f_{\rho,\sigma} : \mathbb{R} \to \mathbb{R}$ defined as

$$f_{\rho,\sigma}(\alpha) = \mathrm{Tr}\left(\sigma^{\alpha}\rho^{1-\alpha}\right)$$

for all $\alpha \in \mathbb{R}$, for any fixed choice of positive definite density operators $\rho, \sigma \in \mathrm{D}(\mathcal{X})$. Under the assumption that ρ and σ are both positive definite, we have that the function $f_{\rho,\sigma}$ is well defined, and is in fact differentiable (and therefore continuous) everywhere on its domain. In particular, we have

$$f'_{\rho,\sigma}(\alpha) = \mathrm{Tr}\left[\sigma^{\alpha}\rho^{1-\alpha}\left(\ln(\sigma) - \ln(\rho)\right)\right]. \tag{11.1}$$

To verify that this expression is correct, we may consider spectral decompositions

$$\rho = \sum_{i=1}^{n} p_i x_i x_i^* \quad \text{and} \quad \sigma = \sum_{i=1}^{n} q_i y_i y_i^*.$$

We have

$$\mathrm{Tr}\left(\sigma^{\alpha}\rho^{1-\alpha}\right) = \sum_{1 \leq i,j \leq n} q_j^{\alpha} p_i^{1-\alpha} \left|\langle x_i, y_j \rangle\right|^2$$

and so

$$f'_{\rho,\sigma}(\alpha) = \sum_{1 \leq i,j \leq n} (\ln(q_j) - \ln(p_i)) q_j^{\alpha} p_i^{1-\alpha} \left|\langle x_i, y_j \rangle\right|^2 = \mathrm{Tr}\left[\sigma^{\alpha}\rho^{1-\alpha}\left(\ln(\sigma) - \ln(\rho)\right)\right]$$

as claimed.

The main reason we are interested in the function $f_{\rho,\sigma}$ is that its derivative has an interesting value at 0:

$$f'_{\rho,\sigma}(0) = -\ln(2) S(\rho\|\sigma).$$

We may therefore write

$$S(\rho\|\sigma) = -\frac{1}{\ln(2)} f'_{\rho,\sigma}(0) = -\frac{1}{\ln(2)} \lim_{\alpha \to 0^+} \frac{\mathrm{Tr}\left(\sigma^{\alpha}\rho^{1-\alpha}\right) - 1}{\alpha},$$

where the second equality follows by substituting $f_{\rho,\sigma}(0) = 1$ into the definition of the derivative.

Now consider the following theorem that concerns the relationship among the functions $f_{\rho,\sigma}$ for various choices of ρ and σ.

Theorem 11.3. *Let $\sigma_0, \sigma_1, \rho_0, \rho_1 \in \mathrm{Pd}(\mathcal{X})$ be positive definite operators. For every choice of $\alpha, \lambda \in [0,1]$ we have*

$$\mathrm{Tr}\left((\lambda\sigma_0 + (1-\lambda)\sigma_1)^{\alpha}(\lambda\rho_0 + (1-\lambda)\rho_1)^{1-\alpha}\right) \geq \lambda \,\mathrm{Tr}\left(\sigma_0^{\alpha}\rho_0^{1-\alpha}\right) + (1-\lambda)\,\mathrm{Tr}\left(\sigma_1^{\alpha}\rho_1^{1-\alpha}\right).$$

(The theorem happens to be true for all positive definite operators ρ_0, ρ_1, σ_0, and σ_1, but we will really only need it for density operators.)

Before proving this theorem, let us note that it implies Theorem 11.2.

Proof of Theorem 11.2 (assuming Theorem 11.3). We have

$$\begin{aligned}
&S(\lambda\rho_0 + (1-\lambda)\rho_1\|\lambda\sigma_0 + (1-\lambda)\sigma_1) \\
&\qquad = -\frac{1}{\ln(2)} \lim_{\alpha \to 0^+} \frac{\mathrm{Tr}\left((\lambda\sigma_0 + (1-\lambda)\sigma_1)^{\alpha}(\lambda\rho_0 + (1-\lambda)\rho_1)^{1-\alpha}\right) - 1}{\alpha} \\
&\qquad \leq -\frac{1}{\ln(2)} \lim_{\alpha \to 0^+} \frac{\lambda\,\mathrm{Tr}\left(\sigma_0^{\alpha}\rho_0^{1-\alpha}\right) + (1-\lambda)\,\mathrm{Tr}\left(\sigma_1^{\alpha}\rho_1^{1-\alpha}\right) - 1}{\alpha} \\
&\qquad = -\frac{1}{\ln(2)} \lim_{\alpha \to 0^+} \left[\lambda\left(\frac{\mathrm{Tr}\left(\sigma_0^{\alpha}\rho_0^{1-\alpha}\right) - 1}{\alpha}\right) + (1-\lambda)\left(\frac{\mathrm{Tr}\left(\sigma_1^{\alpha}\rho_1^{1-\alpha}\right) - 1}{\alpha}\right)\right] \\
&\qquad = \lambda\, S(\rho_0\|\sigma_0) + (1-\lambda)\, S(\rho_1\|\sigma_1)
\end{aligned}$$

as required. □

Our goal has therefore shifted to proving Theorem 11.3. To prove Theorem 11.3 we require another fact that is stated in the theorem that follows. It is equivalent to a theorem known as *Lieb's concavity theorem*, and Theorem 11.3 is a special case of that theorem, but Lieb's concavity theorem itself is usually stated in a somewhat different form than the one that follows.

Theorem 11.4. *Let $A_0, A_1 \in \mathrm{Pd}(\mathcal{X})$ and $B_0, B_1 \in \mathrm{Pd}(\mathcal{Y})$ be positive definite operators. For every choice of $\alpha \in [0,1]$ we have*

$$(A_0 + A_1)^{\alpha} \otimes (B_0 + B_1)^{1-\alpha} \geq A_0^{\alpha} \otimes B_0^{1-\alpha} + A_1^{\alpha} \otimes B_1^{1-\alpha}.$$

Once again, before proving this theorem, let us note that it implies the main result we are working toward.

Proof of Theorem 11.3 (assuming Theorem 11.4). The substitutions

$$A_0 = \lambda\sigma_0, \quad B_0 = \lambda\rho_0^{\mathsf{T}}, \quad A_1 = (1-\lambda)\sigma_1, \quad B_1 = (1-\lambda)\rho_1^{\mathsf{T}},$$

taken in Theorem 11.4 imply the operator inequality

$$\begin{aligned}(\lambda\sigma_0 + (1-\lambda)\sigma_1)^{\alpha} \otimes (\lambda\rho_0^{\mathsf{T}} + (1-\lambda)\rho_1^{\mathsf{T}})^{1-\alpha} & \\ \geq \lambda\, \sigma^{\alpha} \otimes (\rho_0^{\mathsf{T}})^{1-\alpha} + (1-\lambda)\, \sigma_1^{\alpha} \otimes (\rho_1^{\mathsf{T}})^{1-\alpha} & \\ = \lambda\, \sigma^{\alpha} \otimes (\rho_0^{1-\alpha})^{\mathsf{T}} + (1-\lambda)\, \sigma_1^{\alpha} \otimes (\rho_1^{1-\alpha})^{\mathsf{T}}. &\end{aligned}$$

Applying the identity $\mathrm{vec}(\mathbb{1})^*(X \otimes Y^{\mathsf{T}})\,\mathrm{vec}(\mathbb{1}) = \mathrm{Tr}(XY)$ to both sides of the inequality then gives the desired result. □

Now, toward the proof of Theorem 11.4, we require the following lemma.

Lemma 11.5. *Let $P_0, P_1, Q_0, Q_1, R_0, R_1 \in \mathrm{Pd}(\mathcal{X})$ be positive definite operators that satisfy these conditions:*

1. $[P_0, P_1] = [Q_0, Q_1] = [R_0, R_1] = 0$,
2. $P_0^2 \geq Q_0^2 + R_0^2$, *and*
3. $P_1^2 \geq Q_1^2 + R_1^2$.

It holds that $P_0 P_1 \geq Q_0 Q_1 + R_0 R_1$.

Remark. Notice that in the conclusion of the lemma, $P_0 P_1$ is positive definite given the assumption that $[P_0, P_1] = 0$, and likewise for $Q_0 Q_1$ and $R_0 R_1$.

Proof. The conclusion of the lemma is equivalent to $X \leq \mathbb{1}$ for

$$X = P_0^{-1/2} P_1^{-1/2} (Q_0 Q_1 + R_0 R_1) P_1^{-1/2} P_0^{-1/2}.$$

As X is positive definite, and therefore Hermitian, this in turn is equivalent to the condition that every eigenvalue of X is at most 1.

To establish that every eigenvalue of X is at most 1, let us suppose that u is any eigenvector of X whose corresponding eigenvalue is λ. As P_0 and P_1 are invertible and u is nonzero, we have that $P_0^{-1/2}P_1^{1/2}u$ is nonzero as well, and therefore we may define a unit vector v as follows:

$$v = \frac{P_0^{-1/2}P_1^{1/2}u}{\left\| P_0^{-1/2}P_1^{1/2}u \right\|}.$$

It holds that v is an eigenvector of $P_0^{-1}(Q_0Q_1 + R_0R_1)P_1^{-1}$ with eigenvalue λ, and because v is a unit vector it follows that

$$v^*P_0^{-1}(Q_0Q_1 + R_0R_1)P_1^{-1}v = \lambda.$$

Finally, using the fact that v is a unit vector, we can establish the required bound on λ as follows:

$$\begin{aligned}
\lambda &= v^*P_0^{-1}(Q_0Q_1 + R_0R_1)P_1^{-1}v \\
&\leq \left| v^*P_0^{-1}Q_0Q_1P_1^{-1}v \right| + \left| v^*P_0^{-1}R_0R_1P_1^{-1}v \right| \\
&\leq \sqrt{v^*P_0^{-1}Q_0^2P_0^{-1}v}\sqrt{v^*P_1^{-1}Q_1^2P_1^{-1}v} + \sqrt{v^*P_0^{-1}R_0^2P_0^{-1}v}\sqrt{v^*P_1^{-1}R_1^2P_1^{-1}v} \\
&\leq \sqrt{v^*P_0^{-1}(Q_0^2 + R_0^2)P_0^{-1}v}\sqrt{v^*P_1^{-1}(Q_1^2 + R_1^2)P_1^{-1}v} \\
&\leq 1.
\end{aligned}$$

Here we have used the triangle inequality once and the Cauchy-Schwarz inequality twice, along with the given assumptions on the operators. □

Finally, we can finish of the proof of Theorem 11.2 by proving Theorem 11.4.

Proof of Theorem 11.4. Let us define a function $f : [0,1] \to \mathrm{Herm}\,(\mathcal{X} \otimes \mathcal{Y})$ as

$$f(\alpha) = (A_0 + A_1)^\alpha \otimes (B_0 + B_1)^{1-\alpha} - \left(A_0^\alpha \otimes B_0^{1-\alpha} + A_1^\alpha \otimes B_1^{1-\alpha} \right),$$

and let $K = \{\alpha \in [0,1] : f(\alpha) \in \mathrm{Pos}\,(\mathcal{X} \otimes \mathcal{Y})\}$ be the pre-image under f of the set $\mathrm{Pos}\,(\mathcal{X} \otimes \mathcal{Y})$. Notice that K is a closed set, given that f is continuous and $\mathrm{Pos}\,(\mathcal{X} \otimes \mathcal{Y})$ is closed. Our goal is to prove that $K = [0,1]$.

It is obvious that 0 and 1 are elements of K. For an arbitrary choice of $\alpha, \beta \in K$, consider the following operators:

$$\begin{aligned}
P_0 &= (A_0 + A_1)^{\alpha/2} \otimes (B_0 + B_1)^{(1-\alpha)/2}, \\
P_1 &= (A_0 + A_1)^{\beta/2} \otimes (B_0 + B_1)^{(1-\beta)/2}, \\
Q_0 &= A_0^{\alpha/2} \otimes B_0^{(1-\alpha)/2}, \\
Q_1 &= A_0^{\beta/2} \otimes B_0^{(1-\beta)/2}, \\
R_0 &= A_1^{\alpha/2} \otimes B_1^{(1-\alpha)/2}, \\
R_1 &= A_1^{\beta/2} \otimes B_1^{(1-\beta)/2}.
\end{aligned}$$

The conditions $[P_0, P_1] = [Q_0, Q_1] = [R_0, R_1] = 0$ are immediate, while the assumptions that $\alpha \in K$ and $\beta \in K$ correspond to the conditions $P_0^2 \geq Q_0^2 + R_0^2$ and $P_1^2 \geq Q_1^2 + R_1^2$, respectively. We may therefore apply Lemma 11.5 to obtain

$$(A_0 + A_1)^\gamma \otimes (B_0 + B_1)^{1-\gamma} \geq A_0^\gamma \otimes B_0^{1-\gamma} + A_1^\gamma \otimes B_1^{1-\gamma}$$

for $\gamma = (\alpha + \beta)/2$, which implies that $(\alpha + \beta)/2 \in K$.

Now, given that $0 \in K$, $1 \in K$, and $(\alpha + \beta)/2 \in K$ for any choice of $\alpha, \beta \in K$, we have that K is dense in $[0, 1]$. In particular, K contains every number of the form $m/2^n$ for n and m nonnegative integers with $m \leq 2^n$. As K is closed, this implies that $K = [0, 1]$ as required. □

11.2 Strong subadditivity

We have worked hard to prove that the quantum relative entropy is jointly convex, and now it is time to reap the rewards. Let us begin by proving the following simple theorem, which states that mixed unitary channels cannot increase the relative entropy of two density operators.

Theorem 11.6. *Let $\mathcal{X}$ be a complex Euclidean space and let $\Phi \in \mathrm{C}(\mathcal{X})$ be a mixed unitary channel. For any choice of positive definite density operators $\rho, \sigma \in \mathrm{D}(\mathcal{X})$ we have*

$$S(\Phi(\rho) \| \Phi(\sigma)) \leq S(\rho \| \sigma).$$

Proof. As Φ is mixed unitary, we may write

$$\Phi(X) = \sum_{j=1}^{m} p_j U_j X U_j^*$$

for a probability vector $(p_1, \ldots, p_m)$ and unitary operators $U_1, \ldots, U_m \in \mathrm{U}(\mathcal{X})$. By Theorem 11.2 we have

$$S(\Phi(\rho) \| \Phi(\sigma)) = S\left(\sum_{j=1}^{m} p_j U_j \rho U_j^* \,\middle\|\, \sum_{j=1}^{m} p_j U_j \sigma U_j^*\right) \leq \sum_{j=1}^{m} p_j S\left(U_j \rho U_j^* \,\middle\|\, U_j \sigma U_j^*\right).$$

The quantum relative entropy is clearly unitarily invariant, meaning

$$S(\rho \| \sigma) = S(U \rho U^* \| U \sigma U^*)$$

for all $U \in \mathrm{U}(\mathcal{X})$. This implies that

$$\sum_{j=1}^{m} p_j S\left(U_j \rho U_j^* \,\middle\|\, U_j \sigma U_j^*\right) = S(\rho \| \sigma),$$

and therefore completes the proof. □

Notice that for any choice of positive definite density operators $\rho_0, \rho_1, \sigma_0, \sigma_1 \in \mathrm{D}(\mathcal{X})$ we have

$$S(\rho_0 \otimes \rho_1 \| \sigma_0 \otimes \sigma_1) = S(\rho_0 \| \sigma_0) + S(\rho_1 \| \sigma_1).$$

This fact follows easily from the identity $\log(P \otimes Q) = \log(P) \otimes \mathbb{1} + \mathbb{1} \otimes \log(Q)$, which is valid for all $P, Q \in \mathrm{Pd}(\mathcal{X})$. Combining this observation with the previous theorem yields the following corollary.

Corollary 11.7. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces. For any choice of positive definite density operators $\rho, \sigma \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ it holds that*

$$S(\mathrm{Tr}_{\mathcal{Y}}(\rho) \| \mathrm{Tr}_{\mathcal{Y}}(\sigma)) \leq S(\rho \| \sigma).$$

Proof. The completely depolarizing operation $\Omega \in \mathrm{C}(\mathcal{Y})$ is mixed unitary, as we proved in Lecture 6, which implies that $\mathbb{1}_{\mathrm{L}(\mathcal{X})} \otimes \Omega$ is mixed unitary as well. For every $\xi \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ we have

$$(\mathbb{1}_{\mathrm{L}(\mathcal{X})} \otimes \Omega)(\xi) = \mathrm{Tr}_{\mathcal{Y}}(\xi) \otimes \frac{\mathbb{1}_{\mathcal{Y}}}{m}$$

where $m = \dim(\mathcal{Y})$, and therefore

$$\begin{aligned} S\left(\mathrm{Tr}_{\mathcal{Y}}(\rho) \| \mathrm{Tr}_{\mathcal{Y}}(\sigma)\right) &= S\left(\mathrm{Tr}_{\mathcal{Y}}(\rho) \otimes \frac{\mathbb{1}_{\mathcal{Y}}}{m} \,\middle\|\, \mathrm{Tr}_{\mathcal{Y}}(\sigma) \otimes \frac{\mathbb{1}_{\mathcal{Y}}}{m}\right) \\ &= S\left((\mathbb{1}_{\mathrm{L}(\mathcal{X})} \otimes \Omega)(\rho) \,\|\, (\mathbb{1}_{\mathrm{L}(\mathcal{X})} \otimes \Omega)(\sigma)\right) \\ &\leq S(\rho \| \sigma) \end{aligned}$$

as required. □

Note that the above theorem and corollary extend to arbitrary density operators given that the same is true of Theorem 11.2. Making use of the Stinespring representation of quantum channels, we obtain the following fact.

Corollary 11.8. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $\rho, \sigma \in \mathrm{D}(\mathcal{X})$ be density operators, and let $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ be a channel. It holds that*

$$S(\Phi(\rho) \| \Phi(\sigma)) \leq S(\rho \| \sigma).$$

Finally we are prepared to prove strong subadditivity, which turns out to be very easy now that we have established Corollary 11.7.

Proof of Theorem 11.1. We need to prove that the inequality

$$S(\rho^{\mathsf{XYZ}}) + S(\rho^{\mathsf{Z}}) \leq S(\rho^{\mathsf{XZ}}) + S(\rho^{\mathsf{YZ}})$$

holds for all choices of $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z})$. It suffices to prove this inequality for all positive definite ρ, as it then follows for arbitrary density operators ρ by the continuity of the von Neumann entropy.

Let $n = \dim(\mathcal{X})$, and observe that the following two identities hold: the first is

$$S\left(\rho^{\mathsf{XYZ}} \,\middle\|\, \frac{\mathbb{1}_{\mathcal{X}}}{n} \otimes \rho^{\mathsf{YZ}}\right) = -S(\rho^{\mathsf{XYZ}}) + S(\rho^{\mathsf{YZ}}) + \log(n),$$

and the second is

$$S\left(\rho^{\mathsf{XZ}} \,\middle\|\, \frac{\mathbb{1}_{\mathcal{X}}}{n} \otimes \rho^{\mathsf{Z}}\right) = -S(\rho^{\mathsf{XZ}}) + S(\rho^{\mathsf{Z}}) + \log(n).$$

By Corollary 11.7 we have

$$S\left(\rho^{\mathsf{XZ}} \,\middle\|\, \frac{\mathbb{1}_{\mathcal{X}}}{n} \otimes \rho^{\mathsf{Z}}\right) \leq S\left(\rho^{\mathsf{XYZ}} \,\middle\|\, \frac{\mathbb{1}_{\mathcal{X}}}{n} \otimes \rho^{\mathsf{YZ}}\right),$$

and therefore

$$S(\rho^{\mathsf{XYZ}}) + S(\rho^{\mathsf{Z}}) \leq S(\rho^{\mathsf{XZ}}) + S(\rho^{\mathsf{YZ}})$$

as required. □

To conclude the lecture, let us prove a statement about quantum mutual information that is equivalent to strong subadditivity.

Corollary 11.9. *Let* X*,* Y*, and* Z *be registers. For every state* $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z})$ *of these registers we have*

$$S(\mathsf{X} : \mathsf{Y}) \leq S(\mathsf{X} : \mathsf{Y}, \mathsf{Z}).$$

Proof. By strong subadditivity we have

$$S(\mathsf{X}, \mathsf{Y}, \mathsf{Z}) + S(\mathsf{Y}) \leq S(\mathsf{X}, \mathsf{Y}) + S(\mathsf{Y}, \mathsf{Z}),$$

which is equivalent to

$$S(\mathsf{Y}) - S(\mathsf{X}, \mathsf{Y}) \leq S(\mathsf{Y}, \mathsf{Z}) - S(\mathsf{X}, \mathsf{Y}, \mathsf{Z}).$$

Adding $S(\mathsf{X})$ to both sides gives

$$S(\mathsf{X}) + S(\mathsf{Y}) - S(\mathsf{X}, \mathsf{Y}) \leq S(\mathsf{X}) + S(\mathsf{Y}, \mathsf{Z}) - S(\mathsf{X}, \mathsf{Y}, \mathsf{Z}).$$

This inequality is equivalent to

$$S(\mathsf{X} : \mathsf{Y}) \leq S(\mathsf{X} : \mathsf{Y}, \mathsf{Z}),$$

which establishes the claim. □

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

Lecture 12: Holevo's theorem and Nayak's bound

In this lecture we will prove Holevo's theorem. This is a famous theorem in quantum information theory, which is often informally summarized by a statement along the lines of this:

> *It is not possible to communicate more than n classical bits of information by the transmission of n qubits alone.*

Although this is an implication of Holevo's theorem, the theorem itself says more, and is stated in more precise terms that has no resemblance to the above statement. After stating and proving Holevo's theorem, we will discuss an interesting application of this theorem to the notion of a *quantum random access code*. In particular, we will prove Nayak's bound, which demonstrates that quantum random access codes are surprisingly limited in power.

12.1 Holevo's theorem

We will first discuss some of the concepts that Holevo's theorem concerns, and then state and prove the theorem itself. Although the theorem is difficult to prove from first principles, it turns out that there is a very simple proof that makes use of the strong subadditivity of the von Neumann entropy. Having proved strong subadditivity in the previous lecture, we will naturally opt for this simple proof.

12.1.1 Mutual information

Recall that if A and B are classical registers, whose values are distributed in some particular way, then the *mutual information* between A and B for this distribution is defined as

$$\begin{aligned} I(\mathsf{A}:\mathsf{B}) &\triangleq H(\mathsf{A}) + H(\mathsf{B}) - H(\mathsf{A},\mathsf{B}) \\ &= H(\mathsf{A}) - H(\mathsf{A}|\mathsf{B}) \\ &= H(\mathsf{B}) - H(\mathsf{B}|\mathsf{A}). \end{aligned}$$

The usual interpretation of this quantity is that it describes how many bits of information about B are, on average, revealed by the value of A; or equivalently, given that the quantity is symmetric in A and B, how many bits of information about A are revealed by the value of B. Like all quantities involving the Shannon entropy, this interpretation should be understood to really only be meaningful in an asymptotic sense.

To illustrate the intuition behind this interpretation, let us suppose that A and B are distributed in some particular way, and Alice looks at the value of A. As Bob does not know what value Alice sees, he has $H(\mathsf{A})$ bits of uncertainty about her value. After sampling B, Bob's average uncertainty about Alice's value becomes $H(\mathsf{A}|\mathsf{B})$, which is always at most $H(\mathsf{A})$ and is less assuming that A and B are correlated. Therefore, by sampling B, Bob has decreased his uncertainty of Alice's value by $I(\mathsf{A}:\mathsf{B})$ bits.

In analogy to the above formula we have defined the *quantum mutual information* between two registers X and Y as

$$S(\mathsf{X} : \mathsf{Y}) \triangleq S(\mathsf{X}) + S(\mathsf{Y}) - S(\mathsf{X}, \mathsf{Y}).$$

Although Holevo's theorem does not directly concern the quantum mutual information, it is nevertheless related and indirectly appears in the proof.

12.1.2 Accessible information

Imagine that Alice wants to communicate classical information to Bob. In particular, suppose Alice wishes to communicate to Bob information about the value of a classical register A, whose possible values are drawn from some set Σ and where $p \in \mathbb{R}^{\Sigma}$ is the probability vector that describes the distribution of these values:

$$p(a) = \Pr[\mathsf{A} = a]$$

for each $a \in \Sigma$.

The way that Alice chooses to do this is by preparing a quantum register X in some way, depending on A, after which X is sent to Bob. Specifically, let us suppose that $\{\rho_a : a \in \Sigma\}$ is a collection of density operators in $\mathrm{D}(\mathcal{X})$, and that Alice prepares X in the state ρ_a for whichever $a \in \Sigma$ is the value of A. The register X is sent to Bob, and Bob measures it to gain information about the value of Alice's register A.

One possible approach that Bob could take would be to measure X with respect to some measurement $\mu : \Sigma \to \mathrm{Pos}(\mathcal{X})$, chosen so as to maximize the probability that his measurement result b agrees with Alice's sample a (as was discussed in Lecture 8). We will not, however, make the assumption that this is Bob's approach, and in fact we will not even assume that Bob chooses a measurement whose outcomes agree with Σ. Instead, we will consider a completely general situation in which Bob chooses a measurement

$$\mu : \Gamma \to \mathrm{Pos}(\mathcal{X}) : b \mapsto P_b$$

with which to measure the register X sent by Alice. Let us denote by B a classical register that stores the result of this measurement, so that the pair of registers (A, B) is then distributed as follows:

$$\Pr[(\mathsf{A}, \mathsf{B}) = (a, b)] = p(a) \langle P_b, \rho_a \rangle$$

for each $(a, b) \in \Sigma \times \Gamma$. The amount of information that Bob gains about A by means of this process is given by the mutual information $I(\mathsf{A} : \mathsf{B})$.

The *accessible information* is the maximum value of $I(\mathsf{A} : \mathsf{B})$ that can be achieved by Bob, over all possible measurements. More precisely, the accessible information of the *ensemble*

$$\mathcal{E} = \{(p(a), \rho_a) : a \in \Sigma\}$$

is defined as the maximum of $I(\mathsf{A} : \mathsf{B})$ over all possible choices of the set Γ and the measurement $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$, assuming that the pair (A, B) is distributed as described above for this choice of a measurement. (Given that there is no upper bound on the size of Bob's outcome set Γ, it is not obvious that the accessible information of a given ensemble $\mathcal{E}$ is always achievable for some fixed choice of a measurement $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$. It turns out, however, that there is always an achievable maximum value for $I(\mathsf{A} : \mathsf{B})$ that Bob reaches when his set of outcomes Γ has size at most $\dim(\mathcal{X})^2$.) We will write $I_{\mathrm{acc}}(\mathcal{E})$ to denote the accessible information of the ensemble $\mathcal{E}$.

12.1.3 The Holevo quantity

The last quantity that we need to discuss before stating and proving Holevo's theorem is the *Holevo χ-quantity*. Let us consider again an ensemble $\mathcal{E} = \{(p(a), \rho_a) : a \in \Sigma\}$, where each ρ_a is a density operator on $\mathcal{X}$ and $p \in \mathbb{R}^{\Sigma}$ is a probability vector. For such an ensemble we define the Holevo χ-quantity of $\mathcal{E}$ as

$$\chi(\mathcal{E}) \triangleq S\left(\sum_{a\in\Sigma} p(a)\rho_a\right) - \sum_{a\in\Sigma} p(a)S(\rho_a).$$

Notice that the quantity $\chi(\mathcal{E})$ is always nonnegative, which follows from the concavity of the von Neumann entropy.

One way to think about this quantity is as follows. Consider the situation above where Alice has prepared the register X depending on the value of A, and Bob has received (but not yet measured) the register X. From Bob's point of view, the state of X is therefore

$$\rho = \sum_{a\in\Sigma} p(a)\rho_a.$$

If, however, Bob were to learn that the value of A is $a \in \Sigma$, he would then describe the state of X as ρ_a. The quantity $\chi(\mathcal{E})$ therefore represents the average decrease in the von Neumann entropy of X that Bob would expect from learning the value of A.

Another way to view the quantity $\chi(\mathcal{E})$ is to consider the state of the pair (A, X) in the situation just considered, which is

$$\xi = \sum_{a\in\Sigma} p(a)E_{a,a} \otimes \rho_a.$$

We have

$$\begin{aligned} S(\mathsf{A}, \mathsf{X}) &= H(p) + \sum_{a\in\Sigma} p(a)S(\rho_a), \\ S(\mathsf{A}) &= H(p), \\ S(\mathsf{X}) &= S\left(\sum_{a\in\Sigma} p(a)\rho_a\right), \end{aligned}$$

and therefore $\chi(\mathcal{E}) = S(\mathsf{A}) + S(\mathsf{X}) - S(\mathsf{A}, \mathsf{X}) = S(\mathsf{A} : \mathsf{X})$.

12.1.4 Statement and proof of Holevo's theorem

Now we are prepared to state and prove Holevo's theorem. The formal statement of the theorem follows.

Theorem 12.1 (Holevo's theorem)**.** *Let $\mathcal{E} = \{(p(a), \rho_a) : a \in \Sigma\}$ be an ensemble of density operators over some complex Euclidean space $\mathcal{X}$. It holds that $I_{acc}(\mathcal{E}) \leq \chi(\mathcal{E})$.*

Proof. Suppose Γ is a finite, nonempty set and $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X}) : b \mapsto P_b$ is a measurement on $\mathcal{X}$. Let $\mathcal{A} = \mathbb{C}^{\Sigma}$, $\mathcal{B} = \mathbb{C}^{\Gamma}$, and let us regard μ as a channel of the form $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{B})$ defined as

$$\Phi(X) = \sum_{b\in\Gamma} \langle P_b, X\rangle E_{b,b}$$

for each $X \in \mathrm{L}(\mathcal{X})$. Like every channel, there exists a Stinespring representation for Φ:

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(VXV^*)$$

for some choice of a complex Euclidean space $\mathcal{Z}$ and a linear isometry $V \in \mathrm{U}(\mathcal{X}, \mathcal{B} \otimes \mathcal{Z})$.

Now define two density operators, $\sigma \in \mathrm{D}(\mathcal{A} \otimes \mathcal{X})$ and $\xi \in \mathrm{D}(\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{Z})$, as follows:

$$\sigma = \sum_{a \in \Sigma} p(a) E_{a,a} \otimes \rho_a \qquad \text{and} \qquad \xi = (\mathbb{1}_{\mathcal{A}} \otimes V)\sigma(\mathbb{1}_{\mathcal{A}} \otimes V)^*.$$

Given that V is an isometry, the following equalities hold:

$$\begin{aligned} S(\xi^{\mathsf{A}}) &= S(\sigma^{\mathsf{A}}) = H(p) \\ S(\xi^{\mathsf{ABZ}}) &= S(\sigma^{\mathsf{AX}}) = H(p) + \sum_{a \in \Sigma} p(a) S(\rho_a) \\ S(\xi^{\mathsf{BZ}}) &= S(\sigma^{\mathsf{X}}) = S\left(\sum_{a \in \Sigma} p(a) \rho_a \right), \end{aligned}$$

and therefore, for the state $\xi \in \mathrm{D}(\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{Z})$, we have

$$S(\mathsf{A} : \mathsf{B}, \mathsf{Z}) = S(\mathsf{A}) + S(\mathsf{B}, \mathsf{Z}) - S(\mathsf{A}, \mathsf{B}, \mathsf{Z}) = S\left(\sum_{a \in \Sigma} p(a) \rho_a \right) - \sum_{a \in \Sigma} p(a) S(\rho_a) = \chi(\mathcal{E}).$$

By the strong subadditivity of the von Neumann entropy, we have

$$S(\mathsf{A} : \mathsf{B}) \leq S(\mathsf{A} : \mathsf{B}, \mathsf{Z}) = \chi(\mathcal{E}).$$

Noting that the state $\xi^{\mathsf{AB}} \in \mathrm{D}(\mathcal{A} \otimes \mathcal{B})$ takes the form

$$\xi = \sum_{a \in \Sigma} \sum_{b \in \Gamma} p(a) \langle P_b, \rho_a \rangle E_{a,a} \otimes E_{b,b},$$

we see that the quantity $S(\mathsf{A} : \mathsf{B})$ is equal to the accessible information $I_{\mathrm{acc}}(\mathcal{E})$ for an optimally chosen measurement $\mu : \Gamma \to \mathrm{Pos}(\mathcal{X})$. It follows that $I_{\mathrm{acc}}(\mathcal{E}) \leq \chi(\mathcal{E})$ as required.

□

As discussed at the beginning of the lecture, this theorem implies that Alice can communicate no more than n classical bits of information to Bob by sending n qubits alone. If the register X comprises n qubits, and therefore $\mathcal{X}$ has dimension 2^n, then for any ensemble

$$\mathcal{E} = \{(p(a), \rho_a) \,:\, a \in \Sigma\}$$

of density operators on $\mathcal{X}$ we have

$$\chi(\mathcal{E}) \leq S\left(\sum_{a \in \Sigma} p(a) \rho_a \right) \leq n.$$

This means that for any choice of the register A, the ensemble $\mathcal{E}$, and the measurement that determines the value of a classical register B, we must have $I(\mathsf{A} : \mathsf{B}) \leq n$. In other words, Bob can learn no more than n bits of information by means of the process he and Alice have performed.

12.2 Nayak's bound

We will now consider a related, but nevertheless different setting from the one that Holevo's theorem concerns. Suppose now that Alice has m bits, and she wants to encode them into fewer than n qubits in such a way that Bob can recover not the entire string of bits, but rather any *single* bit (or small number of bits) of his choice. Given that Bob will only learn a very small amount of information by means of this process, the possibility that Alice could do this does not violate Holevo's theorem in any obvious way.

This idea has been described as a "quantum phone book." Imagine a very compact phone book implemented using quantum information. The user measures the qubits forming the phone book using a measurement that is unique to the individual whose number is being sought. The user's measurement destroys the phone book, so only a small number of digits of information are effectively transmitted by sending the phone book. Perhaps it is not unreasonable to hope that such a phone book containing 100,000 numbers could be constructed using, say, 1,000 qubits?

Here is an example showing that something nontrivial along these lines can be realized. Suppose Alice wants to encode 2 bits $a, b \in \{0,1\}$ into one qubit so that when she sends this qubit to Bob, he can pick a two-outcome measurement giving him either a or b with reasonable probability. Define

$$|\psi(\theta)\rangle = \cos(\theta)\,|0\rangle + \sin(\theta)\,|1\rangle$$

for $\theta \in [0, 2\pi]$. Alice encodes ab as follows:

$$\begin{aligned} 00 &\rightarrow |\psi(\pi/8)\rangle \\ 10 &\rightarrow |\psi(3\pi/8)\rangle \\ 11 &\rightarrow |\psi(5\pi/8)\rangle \\ 01 &\rightarrow |\psi(7\pi/8)\rangle \end{aligned}$$

Alice sends the qubit to Bob. If Bob wants to decode a, be measures in the $\{|0\rangle, |1\rangle\}$ basis, and if he wants to decode b he measures in the $\{|+\rangle, |-\rangle\}$ basis (where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$). A simple calculation shows that Bob will correctly decode the bit he has chosen with probability $\cos^2(\pi/8) \approx .85$. There does not exist an analogous classical scheme that allow Bob to do better than randomly guessing for at least one of his two possible choices.

12.2.1 Definition of quantum random access encodings

In more generality, we define a *quantum random access encoding* according to the definition that follows. Here, and for the remainder of the lecture, we let $\Sigma = \{0,1\}$.

Definition 12.2. Let m and n be positive integers, and let $p \in [0,1]$. An $m \overset{p}{\mapsto} n$ quantum random access encoding is a function

$$R : \Sigma^m \rightarrow \mathrm{D}\left(\mathbb{C}^{\Sigma^n}\right) : a_1 \cdots a_m \mapsto \rho_{a_1 \cdots a_m}$$

such that the following holds. For each $j \in \{1, \ldots, m\}$ there exists a measurement

$$\left\{P_0^j, P_1^j\right\} \subset \mathrm{Pos}\left(\mathbb{C}^{\Sigma^n}\right)$$

such that

$$\left\langle P_{a_j}^j, \rho_{a_1 \cdots a_m} \right\rangle \geq p$$

for every $j \in \{1, \ldots, m\}$ and every choice of $a_1 \cdots a_m \in \Sigma^m$.

For example, the above example is a $2 \overset{.85}{\mapsto} 1$ quantum random access encoding.

12.2.2 Fano's inequality

In order to determine whether $m \overset{p}{\mapsto} n$ quantum random access codes exist for various choices of the parameters n, m, and p, we will need a result from classical information theory known as *Fano's inequality*. When considering this result, recall that the binary entropy function is defined as

$$H(\lambda) = -\lambda \log(\lambda) - (1-\lambda)\log(1-\lambda)$$

for $\lambda \in [0,1]$.

Theorem 12.3 (Fano's inequality)**.** *Let* A *and* B *be classical registers taking values in some finite set* Γ *and let* $q = \Pr[\mathsf{A} \neq \mathsf{B}]$*. It holds that*

$$H(\mathsf{A}|\mathsf{B}) \leq H(q) + q\log(|\Gamma| - 1).$$

Proof. Define a new register C whose value is determined by A and B as follows:

$$\mathsf{C} = \begin{cases} 1 & \text{if } \mathsf{A} \neq \mathsf{B} \\ 0 & \text{if } \mathsf{A} = \mathsf{B}. \end{cases}$$

Let us first note that

$$H(\mathsf{A}|\mathsf{B}) = H(\mathsf{C}|\mathsf{B}) + H(\mathsf{A}|\mathsf{B},\mathsf{C}) - H(\mathsf{C}|\mathsf{A},\mathsf{B}).$$

This holds for any choice of registers as a result of the following equations:

$$\begin{aligned} H(\mathsf{A}|\mathsf{B}) &= H(\mathsf{A},\mathsf{B}) - H(\mathsf{B}), \\ H(\mathsf{C}|\mathsf{B}) &= H(\mathsf{B},\mathsf{C}) - H(\mathsf{B}), \\ H(\mathsf{A}|\mathsf{B},\mathsf{C}) &= H(\mathsf{A},\mathsf{B},\mathsf{C}) - H(\mathsf{B},\mathsf{C}), \\ H(\mathsf{C}|\mathsf{A},\mathsf{B}) &= H(\mathsf{A},\mathsf{B},\mathsf{C}) - H(\mathsf{A},\mathsf{B}). \end{aligned}$$

Next, note that

$$H(\mathsf{C}|\mathsf{B}) \leq H(\mathsf{C}) = H(q).$$

Finally, we have $H(\mathsf{C}|\mathsf{A},\mathsf{B}) = 0$ because C is determined by A and B. So, at this point we conclude

$$H(\mathsf{A}|\mathsf{B}) \leq H(q) + H(\mathsf{A}|\mathsf{B},\mathsf{C}).$$

It remains to put an upper bound on $H(\mathsf{A}|\mathsf{B},\mathsf{C})$. We have

$$H(\mathsf{A}|\mathsf{B},\mathsf{C}) = \Pr[\mathsf{C}=0]H(\mathsf{A}|\mathsf{B},\mathsf{C}=0) + \Pr[\mathsf{C}=1]H(\mathsf{A}|\mathsf{B},\mathsf{C}=1).$$

We also have

$$H(\mathsf{A}|\mathsf{B},\mathsf{C}=0) = 0,$$

because $\mathsf{C} = 0$ implies $\mathsf{A} = \mathsf{B}$, and

$$H(\mathsf{A}|\mathsf{B},\mathsf{C}=1) \leq \log(|\Gamma| - 1)$$

because $\mathsf{C} = 1$ implies that $\mathsf{A} \neq \mathsf{B}$, so the largest the uncertainty of A given $\mathsf{B} = b$ can be is $\log(|\Gamma| - 1)$, which is the case when A is uniform over all elements of Γ besides b. Thus

$$H(\mathsf{A}|\mathsf{B}) \leq H(q) + q\log(|\Gamma| - 1)$$

as required. □

The following special case of Fano's inequality, where $\Gamma = \{0,1\}$ and A is uniformly distributed, will be useful.

Corollary 12.4. *Let A be a uniformly distributed Boolean register and let B be any Boolean register. For $q = \Pr(\mathsf{A} = \mathsf{B})$ we have $I(\mathsf{A} : \mathsf{B}) \geq 1 - H(q)$.*

12.2.3 Statement and proof of Nayak's bound

We are now ready to state Nayak's bound, which implies that the quest for a compact quantum phone book was doomed to fail: any $m \overset{p}{\mapsto} n$ quantum random access code requires that n and m are linearly related, with the constant of proportionality tending to 1 as p approaches 1.

Theorem 12.5 (Nayak's bound)**.** *Let n and m be positive integers and let $p \in [1/2, 1]$. If there exists a $m \overset{p}{\mapsto} n$ quantum random access encoding, then $n \geq (1 - H(p))m$.*

To prove this theorem, we will first require the following lemma, which is a consequence of Holevo's theorem and Fano's inequality.

Lemma 12.6. *Suppose $\rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})$ are density operators, $\{Q_0, Q_1\} \subseteq \mathrm{Pos}(\mathcal{X})$ is a measurement, and $q \in [1/2, 1]$. If it is the case that*

$$\langle Q_b, \rho_b \rangle \geq q$$

for $b \in \Sigma$, then

$$S\left(\frac{\rho_0 + \rho_1}{2}\right) - \frac{S(\rho_0) + S(\rho_1)}{2} \geq 1 - H(q)$$

Proof. Let A and B be classical Boolean registers, let $p \in \mathbb{R}^{\Sigma}$ be the uniform probability vector (meaning $p(0) = p(1) = 1/2$), and assume that

$$\Pr[(\mathsf{A}, \mathsf{B}) = (a, b)] = p(a) \langle Q_b, \rho_a \rangle$$

for $a, b \in \Sigma$. By Holevo's theorem we have

$$I(\mathsf{A} : \mathsf{B}) \leq S\left(\frac{\rho_0 + \rho_1}{2}\right) - \frac{S(\rho_0) + S(\rho_1)}{2},$$

and by Fano's inequality we have

$$I(\mathsf{A} : \mathsf{B}) \geq 1 - H(\Pr[\mathsf{A} = \mathsf{B}])) \geq 1 - H(q),$$

from which the lemma follows. □

Proof of Theorem 12.5. Suppose we have some $m \overset{p}{\mapsto} n$ quantum random access encoding

$$R : a_1 \cdots a_m \mapsto \rho_{a_1 \cdots a_m}.$$

For $0 \leq k \leq m - 1$ let

$$\rho_{a_1 \cdots a_k} = \frac{1}{2^{m-k}} \sum_{a_{k+1} \cdots a_m \in \Sigma^{m-k}} \rho_{a_1 \cdots a_m},$$

and note that

$$\rho_{a_1 \cdots a_k} = \frac{1}{2}(\rho_{a_1 \cdots a_k 0} + \rho_{a_1 \cdots a_k 1}).$$

By the assumption that R is a random access encoding, we have that there exists a measurement $\{P_0^k, P_1^k\}$, for $1 \leq k \leq m$, that satisfies

$$\left\langle P_b^k, \rho_{a_1 \cdots a_{k-1} b} \right\rangle \geq p$$

for each $b \in \Sigma$. Thus, by Lemma 12.6,

$$S(\rho_{a_1 \cdots a_{k-1}}) \geq \frac{1}{2}(S(\rho_{a_1 \cdots a_{k-1} 0}) + S(\rho_{a_1 \cdots a_{k-1} 1})) + (1 - H(p))$$

for $1 \leq k \leq m$ and all choices of $a_1 \cdots a_{k-1}$. By applying this inequality repeatedly, we conclude that

$$m(1 - H(p)) \leq S(\rho) \leq n,$$

which completes the proof. □

It can be shown that there exists a classical random access encoding $m \overset{p}{\mapsto} n$ for any $p > 1/2$ provided that $n \in (1 - H(p))m + O(\log m)$. Thus, asymptotically speaking, there is no significant advantage to be gained from quantum random access codes over classical random access codes.

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

Lecture 13: Majorization for real vectors and Hermitian operators

This lecture discusses the notion of *majorization* and some of its connections to quantum information. The main application of majorization that we will see in this course will come in a later lecture when we study *Nielsen's theorem*, which precisely characterizes when it is possible for two parties to transform one pure state into another by means of local operations and classical communication. There are other interesting applications of the notion, however, and a few of them will be discussed in this lecture.

13.1 Doubly stochastic operators

Let Σ be a finite, nonempty set, and for the sake of this discussion let us focus on the real vector space $\mathbb{R}^{\Sigma}$. An operator $A \in \mathrm{L}\left(\mathbb{R}^{\Sigma}\right)$ acting on this vector space is said to be *stochastic* if

1. $A(a,b) \geq 0$ for each $(a,b) \in \Sigma \times \Sigma$, and
2. $\sum_{a \in \Sigma} A(a,b) = 1$ for each $b \in \Sigma$.

This condition is equivalent to requiring that Ae_b is a probability vector for each $b \in \Sigma$, or equivalently that A maps probability vectors to probability vectors.

An operator $A \in \mathrm{L}\left(\mathbb{R}^{\Sigma}\right)$ is *doubly stochastic* if it is the case that both A and A^{T} (or, equivalently, A and A^{*}) are stochastic. In other words, when viewed as a matrix, every row and every column of A forms a probability vector:

1. $A(a,b) \geq 0$ for each $(a,b) \in \Sigma \times \Sigma$,
2. $\sum_{a \in \Sigma} A(a,b) = 1$ for each $b \in \Sigma$, and
3. $\sum_{b \in \Sigma} A(a,b) = 1$ for each $a \in \Sigma$.

Next, let us write $\mathrm{Sym}(\Sigma)$ to denote the set of one-to-one and onto functions of the form $\pi : \Sigma \to \Sigma$ (or, in other words, the *permutations* of Σ). For each $\pi \in \mathrm{Sym}(\Sigma)$ we define an operator $V_{\pi} \in \mathrm{L}\left(\mathbb{R}^{\Sigma}\right)$ as

$$V_{\pi}(a,b) = \begin{cases} 1 & \text{if } a = \pi(b) \\ 0 & \text{otherwise} \end{cases}$$

for every $(a,b) \in \Sigma \times \Sigma$. Equivalently, V_{π} is the operator defined by $V_{\pi} e_b = e_{\pi(b)}$ for each $b \in \Sigma$. Such an operator is called a *permutation operator*.

It is clear that every permutation operator is doubly stochastic, and that the set of doubly stochastic operators is a convex set. The following famous theorem establishes that the doubly stochastic operators are, in fact, given by the convex hull of the permutation operators.

Theorem 13.1 (The Birkhoff–von Neumann theorem)**.** *Let Σ be a finite, nonempty set and let $A \in \mathrm{L}\left(\mathbb{R}^{\Sigma}\right)$ be a linear operator on $\mathbb{R}^{\Sigma}$. It holds that A is a doubly stochastic operator if and only if there exists a probability vector $p \in \mathbb{R}^{\mathrm{Sym}(\Sigma)}$ such that*

$$A = \sum_{\pi \in \mathrm{Sym}(\Sigma)} p(\pi) V_{\pi}.$$

Proof. The Krein-Milman theorem states that every compact, convex set is equal to the convex hull of its extreme points. As the set of doubly stochastic operators is compact and convex, the theorem will therefore follow if we prove that every extreme point in this set is a permutation operator.

To this end, let us consider any doubly stochastic operator A that is not a permutation operator. Our goal is to prove that A is not an extreme point in the set of doubly stochastic operators. Given that A is doubly stochastic but not a permutation operator, there must exist at least one pair $(a_1, b_1) \in \Sigma \times \Sigma$ such that $A(a_1, b_1) \in (0, 1)$. As $\sum_b A(a_1, b) = 1$ and $A(a_1, b_1) \in (0, 1)$, we conclude that there must exist $b_2 \neq b_1$ such that $A(a_1, b_2) \in (0, 1)$. Applying similar reasoning, but to the first index rather than the second, there must exist $a_2 \neq a_1$ such that $A(a_2, b_2) \in (0, 1)$. This argument may repeated, alternating between the first and second indices (i.e., between rows and columns), until eventually a closed loop of even length is formed that alternates between horizontal and vertical moves among the entries of A. (Of course a loop must eventually be formed, given that there are only finitely many entries in the matrix A, and an odd length loop can be avoided by an appropriate choice for the entry that closes the loop.) This process is illustrated in Figure 13.1, where the loop is indicated by the dotted lines.

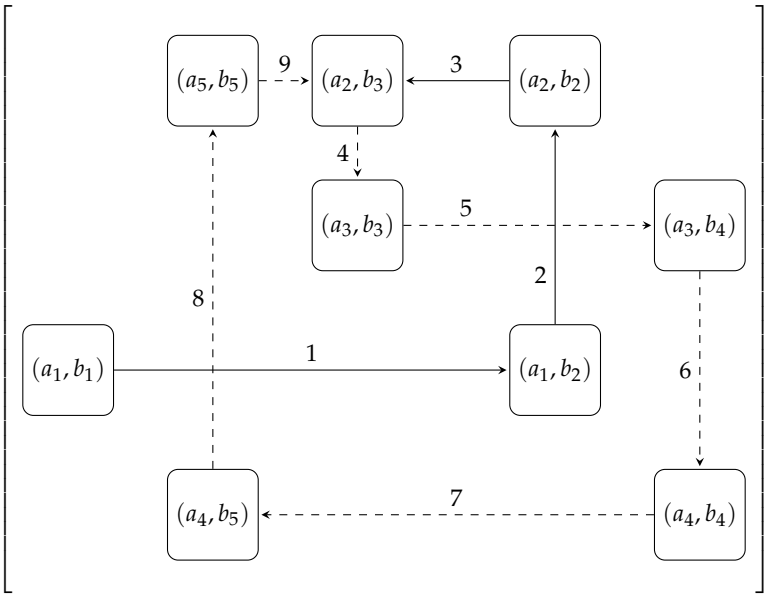

Figure 13.1: An example of a closed loop consisting of entries of A that are contained in the interval $(0, 1)$.

Now, let $\varepsilon \in (0, 1)$ be equal to the minimum value over the entries in the closed loop, and define B to be the operator obtained by setting each entry in the closed loop to be $\pm\varepsilon$, alternating sign along the entries as suggested in Figure 13.2. All of the other entries in B are set to 0.

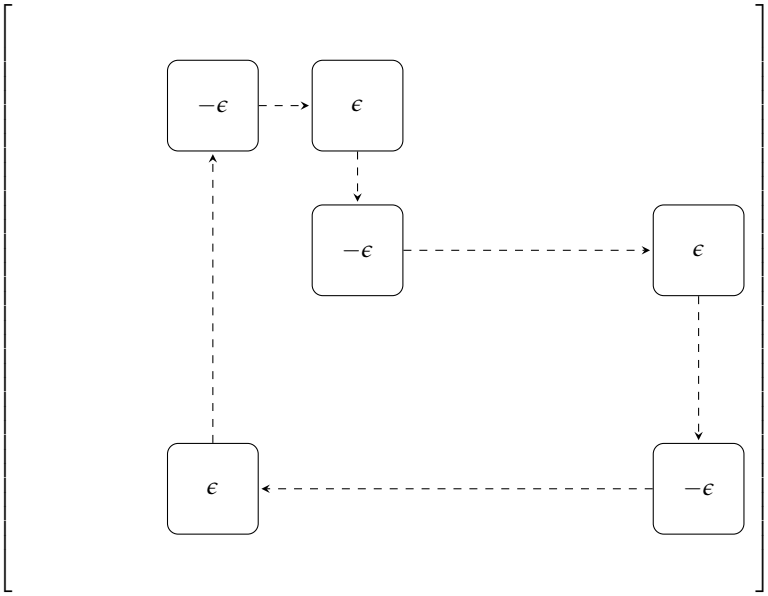

Figure 13.2: The operator B. All entries besides those indicated are 0.

Finally, consider the operators $A + B$ and $A - B$. As A is doubly stochastic and the row and column sums of B are all 0, we have that both $A + B$ and $A - B$ also have row and column sums equal to 1. As ε was chosen to be no larger than the smallest entry within the chosen closed loop, none of the entries of $A + B$ or $A - B$ are negative, and therefore $A - B$ and $A + B$ are doubly stochastic. As B is non-zero, we have that $A + B$ and $A - B$ are distinct. Thus, we have that

$$A = \frac{1}{2}(A + B) + \frac{1}{2}(A - B)$$

is a proper convex combination of doubly stochastic operators, and is therefore not an extreme point in the set of doubly stochastic operators. This is what we needed to prove, and so we are done. □

13.2 Majorization for real vectors

We will now define what it means for one real vector to *majorize* another, and we will discuss two alternate characterizations of this notion. As usual we take Σ to be a finite, nonempty set, and as in the previous section we will focus on the real vector space $\mathbb{R}^\Sigma$. The definition is as follows: for $u, v \in \mathbb{R}^\Sigma$, we say that u *majorizes* v if there exists a doubly stochastic operator A such that $v = Au$. We denote this relation as $v \prec u$ (or $u \succ v$ if it is convenient to switch the ordering).

By the Birkhoff–von Neumann theorem, this definition can intuitively be interpreted as saying that $v \prec u$ if and only if there is a way to "randomly shuffle" the entries of u to obtain v, where by "randomly shuffle" it is meant that one averages in some way a collection of vectors that is obtained by permuting the entries of u to obtain v. Informally speaking, the relation $v \prec u$ means that u is "more ordered" than v, because we can get from u to v by randomizing the order of the vector indices.

An alternate characterization of majorization (which is in fact more frequently taken as the definition) is based on a condition on various sums of the entries of the vectors involved. To state

the condition more precisely, let us introduce the following notation. For every vector $u \in \mathbb{R}^{\Sigma}$ and for $n = |\Sigma|$, we write

$$s(u) = (s_1(u), \ldots, s_n(u))$$

to denote the vector obtained by *sorting* the entries of u from largest to smallest. In other words, we have

$$\{u(a) \,:\, a \in \Sigma\} = \{s_1(u), \ldots, s_n(u)\},$$

where the equality considers the two sides of the equation to be multisets, and moreover

$$s_1(u) \geq \cdots \geq s_n(u).$$

The characterization is given by the equivalence of the first and second items in the following theorem. (The equivalence of the third item in the theorem gives a third characterization that is closely related to the definition, and will turn out to be useful later in the lecture.)

Theorem 13.2. *Let Σ be a finite, non-empty set, and let $u, v \in \mathbb{R}^{\Sigma}$. The following are equivalent.*

1. $v \prec u$.
2. *For $n = |\Sigma|$ and for $1 \leq k < n$ we have*

$$\sum_{j=1}^{k} s_j(v) \leq \sum_{j=1}^{k} s_j(u), \tag{13.1}$$

   and moreover

$$\sum_{j=1}^{n} s_j(v) = \sum_{j=1}^{n} s_j(u). \tag{13.2}$$

3. *There exists a unitary operator $U \in \mathrm{L}\left(\mathbb{C}^{\Sigma}\right)$ such that $v = Au$, where $A \in \mathrm{L}\left(\mathbb{R}^{\Sigma}\right)$ is the operator defined by $A(a,b) = |U(a,b)|^2$ for all $(a,b) \in \Sigma \times \Sigma$.*

Proof. First let us prove that item 1 implies item 2. Assume that A is a doubly stochastic operator satisfying $v = Au$. It is clear that the condition (13.2) holds, as doubly stochastic operators preserve the sum of the entries in any vector, and so it remains to prove the condition (13.1) for $1 \leq k < n$.

To do this, let us first consider the effect of an arbitrary doubly stochastic operator $B \in \mathrm{L}\left(\mathbb{R}^{\Sigma}\right)$ on a vector of the form

$$e_{\Gamma} = \sum_{a \in \Gamma} e_a$$

where $\Gamma \subseteq \Sigma$. The vector e_{Γ} is the *characteristic vector* of the subset $\Gamma \subseteq \Sigma$. The resulting vector Be_{Γ} is a convex combination of permutations of e_{Γ}, or in other words is a convex combination of characteristic vectors of sets having size $|\Gamma|$. The sum of the entries of Be_{Γ} is therefore $|\Gamma|$, and each entry must lie in the interval $[0,1]$. For any set $\Delta \subseteq \Sigma$ with $|\Delta| = |\Gamma|$, the vector $e_{\Delta} - Be_{\Gamma}$ therefore has entries summing to 0, and satisfies $\left(e_{\Delta} - Be_{\Gamma}\right)(a) \geq 0$ for every $a \in \Delta$ and $\left(e_{\Delta} - Be_{\Gamma}\right)(a) \leq 0$ for every $a \notin \Delta$.

Now, for each value $1 \leq k < n$, define $\Delta_k, \Gamma_k \subseteq \Sigma$ to be the subsets indexing the k largest entries of u and v, respectively. In other words,

$$\sum_{j=1}^{k} s_j(u) = \sum_{a \in \Delta_k} u(a) = \langle e_{\Delta_k}, u \rangle \qquad \text{and} \qquad \sum_{j=1}^{k} s_j(v) = \sum_{a \in \Gamma_k} v(a) = \langle e_{\Gamma_k}, v \rangle .$$

We now see that

$$\sum_{i=1}^{k} s_i(u) - \sum_{i=1}^{k} s_i(v) = \langle e_{\Delta_k}, u\rangle - \langle e_{\Gamma_k}, v\rangle = \langle e_{\Delta_k}, u\rangle - \langle e_{\Gamma_k}, Au\rangle = \langle e_{\Delta_k} - A^* e_{\Gamma_k}, u\rangle .$$

This quantity in turn may be expressed as

$$\langle e_{\Delta_k} - A^* e_{\Gamma_k}, u\rangle = \sum_{a\in\Delta_k} \alpha_a\, u(a) - \sum_{a\notin\Delta_k} \alpha_a\, u(a),$$

where

$$\alpha_a = \begin{cases} (e_{\Delta_k} - A^* e_{\Gamma_k})(a) & \text{if } a \in \Delta_k \\ -(e_{\Delta_k} - A^* e_{\Gamma_k})(a) & \text{if } a \notin \Delta_k. \end{cases}$$

As argued above, we have $\alpha_a \geq 0$ for each $a \in \Sigma$ and $\sum_{a\in\Delta_k} \alpha_a = \sum_{a\notin\Delta_k} \alpha_a$. By the choice of Δ_k we have $u(a) \geq u(b)$ for all choices of $a \in \Delta_k$ and $b \notin \Delta_k$, and therefore

$$\sum_{a\in\Delta_k} \alpha_a\, u(a) \geq \sum_{a\notin\Delta_k} \alpha_a\, u(a).$$

This is equivalent to (13.1) as required.

Next we will prove item 2 implies item 3, by induction on $|\Sigma|$. The case $|\Sigma| = 1$ is trivial, so let us consider the case that $|\Sigma| \geq 2$. Assume for simplicity that $\Sigma = \{1, \ldots, n\}$, that $u = (u_1, \ldots, u_n)$ for $u_1 \geq \cdots \geq u_n$, and that $v = (v_1, \ldots, v_n)$ for $v_1 \geq \cdots \geq v_n$. This causes no loss of generality because the majorization relationship is invariant under renaming and independently reordering the indices of the vectors under consideration. Let us also identify the operators U and A we wish to construct with $n \times n$ matrices having entries denoted $U_{i,j}$ and $A_{i,j}$.

Now, assuming item 2 holds, we must have that $u_1 \geq v_1 \geq u_k$ for some choice of $k \in \{1, \ldots, n\}$. Take k to be minimal among all such indices. If it is the case that $k = 1$ then $u_1 = v_1$; and by setting $x = (u_2, \ldots, x_n)$ and $y = (v_2, \ldots, v_n)$ we conclude from the induction hypothesis that there exists an $(n-1) \times (n-1)$ unitary matrix X so that the doubly stochastic matrix B defined by $B_{i,j} = \left|X_{i,j}\right|^2$ satisfies $y = Bx$. By taking U to be the $n \times n$ unitary matrix

$$U = \begin{pmatrix} 1 & 0 \\ 0 & X \end{pmatrix}$$

and letting A be defined by $A_{i,j} = \left|U_{i,j}\right|^2$, we have that $v = Au$ as is required.

The more difficult case is where $k \geq 2$. Let $\lambda \in [0, 1]$ satisfy $v_1 = \lambda u_1 + (1-\lambda) u_k$, and define W to be the $n \times n$ unitary matrix determined by the following equations:

$$\begin{aligned} We_1 &= \sqrt{\lambda} e_1 - \sqrt{1-\lambda} e_k \\ We_k &= \sqrt{1-\lambda} e_1 + \sqrt{\lambda} e_k \\ We_j &= e_j \qquad (\text{for } j \notin \{1, k\}). \end{aligned}$$

The action of W on the span of $\{e_1, e_k\}$ is described by this matrix:

$$\begin{pmatrix} \sqrt{\lambda} & \sqrt{1-\lambda} \\ -\sqrt{1-\lambda} & \sqrt{\lambda} \end{pmatrix}.$$

Notice that the $n \times n$ doubly stochastic matrix D given by $D_{i,j} = \left|W_{i,j}\right|^2$ may be written

$$D = \lambda \mathbb{1} + (1-\lambda) V_{(1\,k)},$$

where $(1\ k) \in S_n$ denotes the permutation that swaps 1 and k, leaving every other element of $\{1, \ldots, n\}$ fixed.

Next, define $(n-1)$-dimensional vectors

$$\begin{aligned} x &= (u_2, \ldots, u_{k-1}, \lambda u_k + (1-\lambda) u_1, u_{k+1}, \ldots, u_n) \\ y &= (v_2, \ldots, v_n). \end{aligned}$$

We will index these vectors as $x = (x_2, \ldots, x_n)$ and $y = (y_2, \ldots, y_n)$ for clarity. For $1 \leq l \leq k-1$ we clearly have

$$\sum_{j=2}^{l} y_j = \sum_{j=2}^{l} v_j \leq \sum_{j=2}^{l} u_j = \sum_{j=2}^{l} x_j$$

given that $v_n \leq \cdots \leq v_1 \leq u_{k-1} \leq \cdots \leq u_1$. For $k \leq l \leq n$, we have

$$\sum_{j=2}^{l} x_j = \sum_{j=1}^{l} u_i - (\lambda u_1 + (1-\lambda) u_k) \geq \sum_{j=2}^{l} v_j.$$

Thus, we may again apply the induction hypothesis to obtain an $(n-1) \times (n-1)$ unitary matrix X such that, for B the doubly stochastic matrix defined by $B_{i,j} = \left|X_{i,j}\right|^2$, we have $y = Bx$.

Now define

$$U = \begin{pmatrix} 1 & 0 \\ 0 & X \end{pmatrix} W.$$

This is a unitary matrix, and to complete the proof it suffices to prove that the doubly stochastic matrix A defined by $A_{i,j} = \left|U_{i,j}\right|^2$ satisfies $v = Au$. We have the following entries of A:

$$\begin{aligned} A_{1,1} &= |U_{1,1}|^2 = \lambda, & A_{i,1} &= (1-\lambda) \left|X_{i-1,k-1}\right|^2 = (1-\lambda) B_{i-1,k-1}, \\ A_{1,k} &= |U_{1,k}|^2 = 1-\lambda, & A_{i,k} &= \lambda \left|X_{i-1,k-1}\right|^2 = \lambda B_{i-1,k-1}, \\ A_{1,j} &= 0, & A_{i,j} &= \left|X_{i-1,j-1}\right|^2 = B_{i-1,j-1}, \end{aligned}$$

Where i and j range over all choices of indices with $i, j \notin \{1, k\}$. From these equations we see that

$$A = \begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix} D,$$

which satisfies $v = Au$ as required.

The final step in the proof is to observe that item 3 implies item 1, which is trivial given that the operator A determined by item 3 must be doubly stochastic. □

13.3 Majorization for Hermitian operators

We will now define an analogous notion of majorization for Hermitian operators. For Hermitian operators $A, B \in \mathrm{Herm}(\mathcal{X})$ we say that A majorizes B, which we express as $B \prec A$ or $A \succ B$, if there exists a mixed unitary channel $\Phi \in \mathrm{C}(\mathcal{X})$ such that

$$B = \Phi(A).$$

Inspiration for this definition partly comes from the Birkhoff–von Neumann theorem, along with the intuitive idea that randomizing the entries of a real vector is analogous to randomizing the choice of an orthonormal basis for a Hermitian operator.

The following theorem gives an alternate characterization of this relationship that also connects it with majorization for real vectors.

Theorem 13.3. *Let $\mathcal{X}$ be a complex Euclidean space and let $A, B \in \mathrm{Herm}(\mathcal{X})$. It holds that $B \prec A$ if and only if $\lambda(B) \prec \lambda(A)$.*

Proof. Let $n = \dim(\mathcal{X})$. By the Spectral theorem, we may write

$$B = \sum_{j=1}^{n} \lambda_j(B) u_j u_j^* \quad \text{and} \quad A = \sum_{j=1}^{n} \lambda_j(A) v_j v_j^*$$

for orthonormal bases $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ of $\mathcal{X}$.

Let us first assume that $\lambda(B) \prec \lambda(A)$. This implies there exist a probability vector $p \in \mathbb{R}^{S_n}$ such that

$$\lambda_j(B) = \sum_{\pi \in S_n} p(\pi) \lambda_{\pi(j)}(A)$$

for $1 \leq j \leq n$. For each permutation $\pi \in S_n$, define a unitary operator

$$U_\pi = \sum_{j=1}^{n} u_j v_{\pi(j)}^*.$$

It holds that

$$\sum_{\pi \in S_n} p(\pi) U_\pi A U_\pi^* = \sum_{j=1}^{n} \sum_{\pi \in S_n} p(\pi) \lambda_{\pi(j)}(A)\, u_j u_j^* = B.$$

Suppose on the other hand that there exists a probability vector $(p_1, \ldots, p_m)$ and unitary operators $U_1, \ldots, U_m$ so that

$$B = \sum_{i=1}^{m} p_i U_i A U_i^*.$$

By considering the spectral decompositions above, we have

$$\lambda_j(B) = \sum_{i=1}^{m} p_i u_j^* U_i A U_i^* u_j = \sum_{i=1}^{m} \sum_{k=1}^{n} p_i \left| u_j^* U_i v_k \right|^2 \lambda_k(A).$$

Define an $n \times n$ matrix D as

$$D_{j,k} = \sum_{i=1}^{m} p_i \left| u_j^* U_i v_k \right|^2.$$

It holds that D is doubly stochastic and satisfies $D\lambda(A) = \lambda(B)$. Therefore $\lambda(B) \prec \lambda(A)$ as required. □

13.4 Applications

Finally, we will note a few applications of the facts we have proved about majorization.

13.4.1 Entropy, norms, and majorization

We begin with two simple facts, one relating entropy with majorization, and the other relating Schatten p-norms to majorization.

Proposition 13.4. *Suppose that $\rho, \xi \in \mathrm{D}(\mathcal{X})$ satisfy $\rho \succ \xi$. It holds that $S(\rho) \leq S(\xi)$.*

Proof. The proposition follows from fact that for every density operator ρ and every mixed unitary operation Φ, we have $S(\rho) \leq S(\Phi(\rho))$ by the concavity of the von Neumann entropy. □

Note that we could equally well have first observed that $H(p) \leq H(q)$ for probability vectors p and q for which $p \succ q$, and then applied Theorem 13.3.

Proposition 13.5. *Suppose that $A, B \in \mathrm{Herm}(\mathcal{X})$ satisfy $A \succ B$. For every $p \in [1, \infty]$, it holds that $\|A\|_p \geq \|B\|_p$.*

Proof. As $A \succ B$, there exists a mixed unitary operator

$$\Phi(X) = \sum_{a \in \Gamma} q(a) U_a X U_a^*$$

such that $B = \Phi(A)$. It holds that

$$\|B\|_p = \|\Phi(A)\|_p = \left\| \sum_{a \in \Gamma} q(a) U_a A U_a^* \right\|_p \leq \sum_{a \in \Gamma} q(a) \|U_a A U_a^*\|_p = \sum_{a \in \Gamma} q(a) \|A\|_p = \|A\|_p,$$

where the inequality is by the triangle inequality, and the third equality holds by the unitary invariance of Schatten p-norms. □

13.4.2 A theorem of Schur relating diagonal entries to eigenvalues

The second application of majorization concerns a relationship between the diagonal entries of an operator and its eigenvalues, which is attributed to Issai Schur. First, a simple lemma relating to dephasing channels (discussed in Lecture 6) is required.

Lemma 13.6. *Let $\mathcal{X}$ be a complex Euclidean space and let $\{x_a : a \in \Sigma\}$ be any orthonormal basis of $\mathcal{X}$. The channel*

$$\Phi(A) = \sum_{a \in \Sigma} (x_a^* A x_a) \, x_a x_a^*$$

is mixed unitary.

Proof. We will assume that $\Sigma = \mathbb{Z}_n$ for some $n \geq 1$. This assumption causes no loss of generality, because neither the ordering of elements in Σ nor their specific names have any bearing on the statement of the lemma.

First consider the standard basis $\{e_a : a \in \mathbb{Z}_n\}$, and define a mixed unitary channel

$$\Delta(A) = \frac{1}{n} \sum_{a \in \mathbb{Z}_n} Z^a A (Z^a)^*,$$

as was done in Lecture 6. We have

$$\Delta(E_{b,c}) = \frac{1}{n} \sum_{a \in \mathbb{Z}_n} \omega^{a(b-c)} E_{b,c} = \begin{cases} E_{b,b} & \text{if } b = c \\ 0 & \text{if } b \neq c, \end{cases}$$

and therefore

$$\Delta(A) = \sum_{a \in \mathbb{Z}_n} (e_a^* A e_a) E_{a,a}.$$

For $U \in \mathrm{U}(\mathcal{X})$ defined as

$$U = \sum_{a \in \mathbb{Z}_n} x_a e_a^*$$

it follows that

$$\frac{1}{n} \sum_{a \in \mathbb{Z}_n} (U Z^a U^*) A (U Z^a U^*)^* = U \Delta(U^* A U) U^* = \Phi(A).$$

The mapping Φ is therefore mixed unitary as required. □

Theorem 13.7 (Schur)**.** *Let $\mathcal{X}$ be a complex Euclidean space, let $A \in \mathrm{Herm}(\mathcal{X})$ be a Hermitian operator, and let $\{x_a : a \in \Sigma\}$ be an orthonormal basis of $\mathcal{X}$. For $v \in \mathbb{R}^\Sigma$ defined as $v(a) = x_a^* A x_a$ for each $a \in \Sigma$, it holds that $v \prec \lambda(A)$.*

Proof. Immediate from Lemma 13.6 and Theorem 13.3. □

Notice that this theorem implies that the probability distribution arising from any *complete* projective measurement of a density operator ρ must have Shannon entropy at least $S(\rho)$.

It is natural to ask if the converse of Theorem 13.7 holds. That is, given a Hermitian operator $A \in \mathrm{Herm}(\mathcal{X})$, for $\mathcal{X} = \mathbb{C}^\Sigma$, and a vector $v \in \mathbb{R}^\Sigma$ such that $\lambda(A) \succ v$, does there necessarily exist an orthonormal basis $\{x_a : a \in \Sigma\}$ of $\mathcal{X}$ such that $v(a) = \langle x_a x_a^*, A \rangle$ for each $a \in \Sigma$? The answer is "yes," as the following theorem states.

Theorem 13.8. *Suppose Σ is a finite, nonempty set, let $\mathcal{X} = \mathbb{C}^\Sigma$, and suppose that $A \in \mathrm{Herm}(\mathcal{X})$ and $v \in \mathbb{R}^\Sigma$ satisfy $v \prec \lambda(A)$. There exists an orthonormal basis $\{x_a : a \in \Sigma\}$ of $\mathcal{X}$ such that $v(a) = x_a^* A x_a$ for each $a \in \Sigma$.*

Proof. Let

$$A = \sum_{a \in \Sigma} w(a) u_a u_a^*$$

be a spectral decomposition of A. The assumptions of the theorem imply, by Theorem 13.2, that there exists a unitary operator U such that, for D defined by

$$D(a,b) = |U(a,b)|^2$$

for $(a,b) \in \Sigma \times \Sigma$, we have $v = Dw$.

Define

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

and let $x_a = V^* U^* V u_a$ for each $a \in \Sigma$. It holds that

$$x_a^* A x_a = \sum_b |U(a,b)|^2 w(b) = (Dw)(a) = v(a),$$

which proves the theorem. □

Theorems 13.7 and 13.8 are sometimes together referred to as the *Schur-Horn theorem*.

13.4.3 Density operators consistent with a given probability vector

Finally, we will prove a characterization of precisely which probability vectors are consistent with a given density operator, meaning that the density operator could have arisen from a random choice of pure states according to the distribution described by the probability vector.

Theorem 13.9. *Let $X = \mathbb{C}^{\Sigma}$ for Σ a finite, nonempty set, and suppose that a density operator $\rho \in \mathrm{D}(\mathcal{X})$ and a probability vector $p \in \mathbb{R}^{\Sigma}$ are given. There exist (not necessarily orthogonal) unit vectors $\{u_a : a \in \Sigma\}$ in $\mathcal{X}$ such that*

$$\rho = \sum_{a \in \Sigma} p(a) u_a u_a^*$$

if and only if $p \prec \lambda(\rho)$.

Proof. Assume first that $p \prec \lambda(\rho)$. By Theorem 13.8 we have that there exists an orthonormal basis $\{x_a : a \in \Sigma\}$ of $\mathcal{X}$ with the property that $\langle x_a x_a^*, \rho \rangle = p(a)$ for each $a \in \Sigma$. Let $y_a = \sqrt{\rho} x_a$ for each $a \in \Sigma$. It holds that

$$\|y_a\|^2 = \langle \sqrt{\rho} x_a, \sqrt{\rho} x_a \rangle = x_a^* \rho x_a = p(a).$$

Define

$$u_a = \begin{cases} \frac{y_a}{\|y_a\|} & \text{if } y_a \neq 0 \\ z & \text{if } y_a = 0, \end{cases}$$

where $z \in \mathcal{X}$ is an arbitrary unit vector. We have

$$\sum_{a \in \Sigma} p(a) u_a u_a^* = \sum_{a \in \Sigma} y_a y_a^* = \sum_{a \in \Sigma} \sqrt{\rho} x_a x_a^* \sqrt{\rho} = \rho$$

as required.

Suppose, on the other hand, that

$$\rho = \sum_{a \in \Sigma} p(a) u_a u_a^*$$

for some collection $\{u_a : a \in \Sigma\}$ of unit vectors. Define $A \in \mathrm{L}(\mathcal{X})$ as

$$A = \sum_{a \in \Sigma} \sqrt{p(a)} u_a e_a^*,$$

and note that $AA^* = \rho$. It holds that

$$A^* A = \sum_{a,b \in \Sigma} \sqrt{p(a)p(b)} \, \langle u_a, u_b \rangle \, E_{a,b},$$

so $e_a^* A^* A e_a = p(a)$. By Theorem 13.7 this implies $\lambda(A^*A) \succ p$. As $\lambda(A^*A) = \lambda(AA^*)$, the theorem is proved. □

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 $P \in \text{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is *separable* if and only if there exists a positive integer m and positive semidefinite operators

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

such that

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

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

Let us also define

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

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:

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

Thus, every element $\rho \in \text{SepD}(\mathcal{X} : \mathcal{Y})$ 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 $\text{SepD}(\mathcal{X} : \mathcal{Y})$ follow. Suppose X and Y are registers in a separable state $\rho \in \text{SepD}(\mathcal{X} : \mathcal{Y})$. 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) $\text{Sep}(\mathcal{X}_1 : \mathcal{X}_2 : \cdots : \mathcal{X}_n)$ 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 $\mathcal{S}(\mathcal{X})$ and $\mathcal{S}(\mathcal{Y})$ are compact, and therefore so too is the Cartesian product $\mathcal{S}(\mathcal{X}) \times \mathcal{S}(\mathcal{Y})$. 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

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

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 $P \in \operatorname{Pos}(\mathcal{X} \otimes \mathcal{Y})$. It holds that $P \in \operatorname{Sep}(\mathcal{X} : \mathcal{Y})$ if and only if*

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

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

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

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

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

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

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

1. $\langle H, Q \otimes R \rangle \geq 0$ for all $Q \in \operatorname{Pos}(\mathcal{X})$ and $R \in \operatorname{Pos}(\mathcal{Y})$, 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 $Q \in \operatorname{Pos}(\mathcal{X})$ and $R \in \operatorname{Pos}(\mathcal{Y})$ we therefore have

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

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

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

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

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

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

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

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. □

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. □

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

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 nonnegative integer k let us consider the collection of operators

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

In other words, a given positive semidefinite operator $P \in \mathrm{Pos}(\mathcal{X}\otimes\mathcal{Y})$ is contained in $\mathrm{R}_k(\mathcal{X}:\mathcal{Y})$ 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 $A_1,\ldots,A_m \in \mathrm{L}(\mathcal{Y},\mathcal{X})$, 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 $\mathrm{R}_k(\mathcal{X}:\mathcal{Y})$ is a closed convex cone. It is easy to see that

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

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

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

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

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

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

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

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

for all $X \in \mathrm{L}(\mathcal{X}_A \otimes \mathcal{X}_B)$. 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

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

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

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

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

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

if and only if

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

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

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

then it holds that

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

The set $\mathrm{Sep}(\mathcal{Y}_A \otimes \mathcal{X}_A : \mathcal{Y}_B \otimes \mathcal{X}_B)$, on the other hand, is a subset of $\mathrm{L}(\mathcal{Y}_A \otimes \mathcal{X}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_B)$, not $\mathrm{L}(\mathcal{Y}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_A \otimes \mathcal{X}_B)$; 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 $W \in \mathrm{L}(\mathcal{Y}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{X}_A \otimes \mathcal{Y}_B \otimes \mathcal{X}_B)$ 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

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

in the proposition, we should write

$$W J(\Phi) W^* \in \operatorname{Sep}\left(\mathcal{Y}_A \otimes \mathcal{X}_A : \mathcal{Y}_B \otimes \mathcal{X}_B\right).$$

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

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

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

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

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

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 $\Phi \in \operatorname{SepT}\left(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B\right)$ be a separable mapping and let $P \in \mathrm{R}_k\left(\mathcal{X}_A : \mathcal{X}_B\right)$. It holds that*

$$\Phi(P) \in \mathrm{R}_k\left(\mathcal{Y}_A : \mathcal{Y}_B\right).$$

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

Proof. Assume $A_1, \ldots, A_m \in \mathrm{L}\left(\mathcal{X}_A, \mathcal{Y}_A\right)$ and $B_1, \ldots, B_m \in \mathrm{L}\left(\mathcal{X}_B, \mathcal{Y}_B\right)$ satisfy

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

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

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

As

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

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

$$\Phi(\operatorname{vec}(Y) \operatorname{vec}(Y)^*) \in \mathrm{R}_r\left(\mathcal{Y}_A : \mathcal{Y}_B\right)$$

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

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. □

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 $\Delta \in \mathrm{C}(\mathcal{Z})$ 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

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

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

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

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

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

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

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

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

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

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

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

as required. A similar argument proves that every Bob-to-Alice classical communication channel is a separable channel. □

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

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

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

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

Lecture 16: Nielsen's theorem on pure state entanglement transformation

In this lecture we will consider *pure-state entanglement transformation*. The setting is as follows: Alice and Bob share a pure state $x \in \mathcal{X}_A \otimes \mathcal{X}_B$, and they would like to transform this state to another pure state $y \in \mathcal{Y}_A \otimes \mathcal{Y}_B$ by means of local operations and classical communication. This is possible for some choices of x and y and impossible for others, and what we would like is to have a condition on x and y that tells us precisely when it is possible. Nielsen's theorem, which we will prove in this lecture, provides such a condition.

Theorem 16.1 (Nielsen's theorem)**.** *Let $x \in \mathcal{X}_A \otimes \mathcal{X}_B$ and $y \in \mathcal{Y}_A \otimes \mathcal{Y}_B$ be unit vectors, for any choice of complex Euclidean spaces $\mathcal{X}_A$, $\mathcal{X}_B$, $\mathcal{Y}_A$, and $\mathcal{Y}_B$. There exists a channel $\Phi \in \mathrm{LOCC}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$ such that $\Phi(xx^*) = yy^*$ if and only if $\mathrm{Tr}_{\mathcal{X}_B}(xx^*) \prec \mathrm{Tr}_{\mathcal{Y}_B}(yy^*)$.*

It may be that $\mathcal{X}_A$ and $\mathcal{Y}_A$ do not have the same dimension, so the relationship

$$\mathrm{Tr}_{\mathcal{X}_B}(xx^*) \prec \mathrm{Tr}_{\mathcal{Y}_B}(yy^*)$$

requires an explanation. In general, given positive semidefinite operators $P \in \mathrm{Pos}(\mathcal{X})$ and $Q \in \mathrm{Pos}(\mathcal{Y})$, we define that $P \prec Q$ if and only if

$$VPV^* \prec WQW^* \tag{16.1}$$

for some choice of a complex Euclidean space $\mathcal{Z}$ and isometries $V \in \mathrm{U}(\mathcal{X}, \mathcal{Z})$ and $W \in \mathrm{U}(\mathcal{Y}, \mathcal{Z})$. If the above condition (16.1) holds for one such choice of $\mathcal{Z}$ and isometries V and W, it holds for all other possible choices of these objects. In particular, one may always take $\mathcal{Z}$ to have dimension equal to the larger of $\dim(\mathcal{X})$ and $\dim(\mathcal{Y})$.

In essence, this interpretation is analogous to padding vectors with zeroes, as is done when we wish to consider the majorization relation between vectors of nonnegative real numbers having possibly different dimensions. In the operator case, the isometries V and W embed the operators P and Q into a single space so that they may be related by our definition of majorization.

It will be helpful to note that if $P \in \mathrm{Pos}(\mathcal{X})$ and $Q \in \mathrm{Pos}(\mathcal{Y})$ are positive semidefinite operators, and $P \prec Q$, then it must hold that $\mathrm{rank}(P) \geq \mathrm{rank}(Q)$. One way to verify this claim is to examine the vectors of eigenvalues $\lambda(P)$ and $\lambda(Q)$, whose nonzero entries agree with $\lambda(VPV^*)$ and $\lambda(WQW^*)$ for any choice of isometries V and W, and to note that Theorem 13.2 implies that $\lambda(WQW^*)$ cannot possibly majorize $\lambda(VPV^*)$ if $\lambda(Q)$ has strictly more nonzero entries than $\lambda(P)$. An alternate way to verify the claim is to note that mixed unitary channels can never decrease the rank of any positive semidefinite operator. It follows from this observation that if $P \in \mathrm{Pd}(\mathcal{X})$ and $Q \in \mathrm{Pd}(\mathcal{Y})$ are positive definite operators, and $P \prec Q$, then $\dim(\mathcal{X}) \geq \dim(\mathcal{Y})$. The condition $P \prec Q$ is therefore equivalent to the existence of an isometry $W \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$ such that $P \prec WQW^*$ in this case.

The remainder of this lecture will be devoted to proving Nielsen's theorem. For the sake of the proof, it will be helpful to make a simplifying assumption, which causes no loss of generality. The assumption is that these equalities hold:

$$\dim(\mathcal{X}_A) = \operatorname{rank}\left(\operatorname{Tr}_{\mathcal{X}_B}(xx^*)\right) = \dim(\mathcal{X}_B),$$
$$\dim(\mathcal{Y}_A) = \operatorname{rank}\left(\operatorname{Tr}_{\mathcal{Y}_B}(yy^*)\right) = \dim(\mathcal{Y}_B).$$

That we can make this assumption follow from a consideration of Schmidt decompositions of x and y:

$$x = \sum_{j=1}^{m} \sqrt{p_j}\, x_{A,j} \otimes x_{B,j} \quad \text{and} \quad y = \sum_{k=1}^{n} \sqrt{q_k}\, y_{A,k} \otimes y_{B,k},$$

where $p_1, \ldots, p_m > 0$ and $q_1, \ldots, q_n > 0$, so that $m = \operatorname{rank}\left(\operatorname{Tr}_{\mathcal{X}_B}(xx^*)\right)$ and $n = \operatorname{rank}\left(\operatorname{Tr}_{\mathcal{Y}_B}(yy^*)\right)$. By restricting $\mathcal{X}_A$ to $\operatorname{span}\{x_{A,1}, \ldots, x_{A,m}\}$, $\mathcal{X}_B$ to $\operatorname{span}\{x_{B,1}, \ldots, x_{B,m}\}$, $\mathcal{Y}_A$ to $\operatorname{span}\{y_{A,1}, \ldots, y_{A,n}\}$, and $\mathcal{Y}_B$ to $\operatorname{span}\{y_{B,1}, \ldots, y_{B,n}\}$, we have that the spaces $\mathcal{X}_A$, $\mathcal{X}_B$, $\mathcal{Y}_A$, and $\mathcal{Y}_B$ are only as large in dimension as they need to be to support the vectors x and y. The reason why this assumption causes no loss of generality is that neither the notion of an LOCC channel transforming xx^* to yy^*, nor the majorization relationship $\operatorname{Tr}_{\mathcal{X}_B}(xx^*) \prec \operatorname{Tr}_{\mathcal{Y}_B}(yy^*)$, is sensitive to the possibility that the ambient spaces in which xx^* and yy^* exist are larger than necessary to support x and y.

16.1 The easier implication: from mixed unitary channels to LOCC channels

We will begin with the easier implication of Nielsen's theorem, which states that the majorization relationship

$$\operatorname{Tr}_{\mathcal{X}_B}(xx^*) \prec \operatorname{Tr}_{\mathcal{Y}_B}(yy^*) \tag{16.2}$$

implies the existence of an LOCC channel mapping xx^* to yy^*. To prove the implication, let us begin by letting $X \in \mathrm{L}(\mathcal{X}_B, \mathcal{X}_A)$ and $Y \in \mathrm{L}(\mathcal{Y}_B, \mathcal{Y}_A)$ satisfy

$$x = \operatorname{vec}(X) \qquad \text{and} \qquad y = \operatorname{vec}(Y),$$

so that (16.2) is equivalent to $XX^* \prec YY^*$. The assumption $\dim(\mathcal{X}_A) = \operatorname{rank}\left(\operatorname{Tr}_{\mathcal{X}_B}(xx^*)\right) = \dim(\mathcal{X}_B)$ implies that XX^* is positive definite (and therefore X is invertible). Likewise, the assumption $\dim(\mathcal{Y}_A) = \operatorname{rank}\left(\operatorname{Tr}_{\mathcal{Y}_B}(yy^*)\right) = \dim(\mathcal{Y}_B)$ implies that YY^* is positive definite. It follows that

$$XX^* = \Psi(WYY^*W^*)$$

for some choice of an isometry $W \in \mathrm{U}(\mathcal{Y}_A, \mathcal{X}_A)$ and a mixed unitary channel $\Psi \in \mathrm{C}(\mathcal{X}_A)$. Let us write this channel as

$$\Psi(\rho) = \sum_{a \in \Sigma} p(a) U_a \rho U_a^*$$

for Σ being a finite and nonempty set, $p \in \mathbb{R}^{\Sigma}$ being a probability vector, and $\{U_a : a \in \Sigma\} \subset \mathrm{U}(\mathcal{X}_A)$ being a collection of unitary operators.

Next, define a channel $\Xi \in \mathrm{C}(\mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{X}_A \otimes \mathcal{Y}_B)$ as

$$\Xi(\rho) = \sum_{a \in \Sigma} \left(U_a^* \otimes \overline{B_a}\right) \rho \left(U_a^* \otimes \overline{B_a}\right)^*$$

for each $\rho \in \mathrm{L}(\mathcal{X}_A \otimes \mathcal{X}_B)$, where $B_a \in \mathrm{L}(\mathcal{X}_B, \mathcal{Y}_B)$ is defined as

$$B_a = \sqrt{p(a)}\left(X^{-1} U_a W Y\right)^*$$

for each $a \in \Sigma$. It holds that

$$\sum_{a\in\Sigma} B_a^* B_a = \sum_{a\in\Sigma} p(a) X^{-1} U_a W Y Y^* W^* U_a^* (X^{-1})^* = X^{-1} \Psi\left(W Y Y^* W^*\right) (X^{-1})^* = \mathbb{1}_{\mathcal{X}_A},$$

and therefore

$$\sum_{a\in\Sigma} B_a^{\mathsf{T}} \overline{B_a} = \overline{\sum_{a\in\Sigma} B_a^* B_a} = \mathbb{1}_{\mathcal{X}_A}.$$

It follows that Ξ is trace-preserving, because

$$\sum_{a\in\Sigma} \left(U_a^* \otimes \overline{B_a}\right)^* \left(U_a^* \otimes \overline{B_a}\right) = \sum_{a\in\Sigma} \left(\mathbb{1}_{\mathcal{X}_A} \otimes B_a^{\mathsf{T}} \overline{B_a}\right) = \mathbb{1}_{\mathcal{X}_A} \otimes \mathbb{1}_{\mathcal{X}_A}.$$

The channel Ξ is, in fact, an LOCC channel. To implement it as an LOCC channel, Bob may first apply the local channel

$$\xi \mapsto \sum_{a\in\Sigma} E_{a,a} \otimes \overline{B_a} \xi B_a^{\mathsf{T}},$$

which has the form of a mapping from $\mathrm{L}(\mathcal{X}_B)$ to $\mathrm{L}(\mathcal{Z} \otimes \mathcal{Y}_B)$ for $\mathcal{Z} = \mathbb{C}^\Sigma$. He then sends the register Z corresponding to the space $\mathcal{Z}$ through a classical channel to Alice. Alice then performs the local channel given by

$$\sigma \mapsto \sum_{b\in\Sigma} \left(U_b^* \otimes e_b^*\right) \sigma \left(U_b^* \otimes e_b^*\right)^*,$$

which has the form of a mapping from $\mathrm{L}(\mathcal{X}_A \otimes \mathcal{Z})$ to $\mathrm{L}(\mathcal{X}_A)$. The composition of these three channels is given by Ξ, which shows that $\Xi \in \mathrm{LOCC}(\mathcal{X}_A, \mathcal{X}_A : \mathcal{X}_B, \mathcal{Y}_B)$ as claimed.

The channel Ξ almost satisfies the requirements of the theorem, for we have

$$\begin{aligned}
\Xi(xx^*) &= \sum_{a\in\Sigma} \left(U_a^* \otimes \overline{B_a}\right) \mathrm{vec}(X)\, \mathrm{vec}(X)^* \left(U_a^* \otimes \overline{B_a}\right)^* \\
&= \sum_{a\in\Sigma} \mathrm{vec}\left(U_a^* X B_a^*\right) \mathrm{vec}\left(U_a^* X B_a^*\right)^* \\
&= \sum_{a\in\Sigma} p(a)\, \mathrm{vec}\left(U_a^* X X^{-1} U_a W Y\right) \mathrm{vec}\left(U_a^* X X^{-1} U_a W Y\right)^* \\
&= \mathrm{vec}(WY)\, \mathrm{vec}(WY)^* \\
&= (W \otimes \mathbb{1}_{\mathcal{Y}_B}) yy^* (W \otimes \mathbb{1}_{\mathcal{Y}_B})^*.
\end{aligned}$$

That is, Ξ transforms xx^* to yy^*, followed by the isometry W being applied to Alice's space $\mathcal{Y}_A$, embedding it in $\mathcal{X}_A$. To "undo" this embedding, Alice may apply the channel

$$\xi \mapsto W^* \xi W + \langle \mathbb{1}_{\mathcal{Y}_A} - WW^*, \xi \rangle\, \sigma \tag{16.3}$$

to her portion of the state $(W \otimes \mathbb{1}_{\mathcal{Y}_B}) yy^* (W \otimes \mathbb{1}_{\mathcal{Y}_B})^*$, where $\sigma \in \mathrm{D}(\mathcal{Y}_A)$ is an arbitrary density matrix that has no influence on the proof. Letting $\Phi \in \mathrm{C}(\mathcal{X}_A \otimes \mathcal{X}_B, \mathcal{Y}_A \otimes \mathcal{Y}_B)$ be the channel that results from composing (16.3) with Ξ, we have that Φ is an LOCC channel and satisfies $\Phi(xx^*) = yy^*$ as required.

16.2 The harder implication: from LOCC channels to mixed unitary channels

The reverse implication, from the one proved in the previous section, states that if $\Phi(xx^*) = yy^*$ for an LOCC channel $\Phi \in \mathrm{C}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$, then $\mathrm{Tr}_{\mathcal{X}_B}(xx^*) \prec \mathrm{Tr}_{\mathcal{Y}_B}(yy^*)$. The main difficulty in proving this fact is that our proof must account for all possible LOCC channels, which do not admit a simple mathematical characterization (so far as anyone knows). For instance, a given LOCC channel could potentially require a composition of 1,000,000 channels that alternate between product channels and classical communication channels, possibly without any shorter composition yielding the same channel.

However, in the situation that we only care about the action of a given LOCC channel on a single pure state—such as the state xx^* being considered in the context of the implication we are trying to prove—LOCC channels can always be reduced to a very simple form. To describe this form, let us begin by defining a restricted class of LOCC channels, acting on the space of operators $\mathrm{L}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ for any fixed choice of complex Euclidean spaces $\mathcal{Z}_A$ and $\mathcal{Z}_B$, as follows.

1. A channel $\Phi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ will be said to be an *A→B channel* if there exists a finite and nonempty set Σ, a collection of operators $\{A_a : a \in \Sigma\} \subset \mathrm{L}(\mathcal{Z}_A)$ satisfying the constraint

   $$\sum_{a \in \Sigma} A_a^* A_a = \mathbb{1}_{\mathcal{Z}_A},$$

   and a collection of unitary operators $\{U_a : a \in \Sigma\} \subset \mathrm{U}(\mathcal{Z}_B)$ such that

   $$\Phi(\rho) = \sum_{a \in \Sigma} (A_a \otimes U_a) \rho (A_a \otimes U_a)^*.$$

   One imagines that such an operation represents the situation where Alice performs a non-destructive measurement represented by the collection $\{A_a : a \in \Sigma\}$, transmits the result to Bob, and Bob applies a unitary channel to his system that depends on Alice's measurement result.

2. A channel $\Phi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ will be said to be a *B→A channel* if there exists a finite and nonempty set Σ, a collection of operators $\{B_a : a \in \Sigma\} \subset \mathrm{L}(\mathcal{Z}_B)$ satisfying the constraint

   $$\sum_{a \in \Sigma} B_a^* B_a = \mathbb{1}_{\mathcal{Z}_B},$$

   and a collection of unitary operators $\{V_a : a \in \Sigma\} \subset \mathrm{U}(\mathcal{Z}_A)$ such that

   $$\Phi(\rho) = \sum_{a \in \Sigma} (V_a \otimes B_a) \rho (V_a \otimes B_a)^*.$$

   Such a channel is analogous to an A→B channel, but where the roles of Alice and Bob are reversed. (The channel constructed in the previous section had this basic form, although the operators $\{B_a\}$ were not necessarily square in that case.)

3. Finally, a channel $\Phi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ will be said to be a *restricted LOCC channel* if it is a composition of A→B and *B* →A channels.

It should be noted that the terms *A→B channel*, *B→A channel*, and *restricted LOCC channel* are being used for the sake of this proof only: they are not standard terms, and will not be used elsewhere in the course.

It is not difficult to see that every restricted LOCC channel is an LOCC channel, using a similar argument to the one showing that the channel Ξ from the previous section was indeed an LOCC channel. As the following theorem shows, restricted LOCC channels turn out to be as powerful as general LOCC channels, provided they are free to act on sufficiently large spaces.

Theorem 16.2. *Suppose $\Phi \in \mathrm{LOCC}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$ is an LOCC channel. There exist complex Euclidean spaces $\mathcal{Z}_A$ and $\mathcal{Z}_B$, linear isometries*

$$V_A \in \mathrm{U}(\mathcal{X}_A, \mathcal{Z}_A), \quad W_A \in \mathrm{U}(\mathcal{Y}_A, \mathcal{Z}_A), \quad V_B \in \mathrm{U}(\mathcal{X}_B, \mathcal{Z}_B), \quad W_B \in \mathrm{U}(\mathcal{Y}_B, \mathcal{Z}_B),$$

and a restricted LOCC channel $\Psi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ such that

$$(W_A \otimes W_B)\Phi(\rho)(W_A \otimes W_B)^* = \Psi\left((V_A \otimes V_B)\rho(V_A \otimes V_B)^*\right) \tag{16.4}$$

for all $\rho \in \mathrm{L}(\mathcal{X}_A \otimes \mathcal{X}_B)$.

Remark 16.3. Before we prove this theorem, let us consider what it is saying. Alice's input space $\mathcal{X}_A$ and output space $\mathcal{Y}_A$ may have different dimensions, but we want to view these two spaces as being embedded in a single space $\mathcal{Z}_A$. The isometries V_A and W_A describe these embeddings. Likewise, V_B and W_B describe the embeddings of Bob's input and output spaces $\mathcal{X}_B$ and $\mathcal{Y}_B$ in a single space $\mathcal{Z}_B$. The above equation (16.4) simply means that Ψ correctly represents Φ in terms of these embeddings: Alice and Bob could either embed the input $\rho \in \mathrm{L}(\mathcal{X}_A \otimes \mathcal{X}_B)$ in $\mathrm{L}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ as $(V_A \otimes V_B)\rho(V_A \otimes V_B)^*$, and then apply Ψ; or they could first perform Φ and then embed the output $\Phi(\rho)$ into $\mathrm{L}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ as $(W_A \otimes W_B)\Phi(\rho)(W_A \otimes W_B)^*$. The equation (16.4) means that they obtain the same thing either way.

Proof. Let us suppose that Φ is a composition of mappings

$$\Phi = \Phi_{n-1} \cdots \Phi_1,$$

where each mapping Φ_k takes the form

$$\Phi_k \in \mathrm{LOCC}\left(\mathcal{X}_A^k, \mathcal{X}_A^{k+1} : \mathcal{X}_B^k, \mathcal{X}_B^{k+1}\right),$$

and is either a local operation for Alice, a local operation for Bob, a classical communication from Alice to Bob, or a classical communication from Bob to Alice. Here we assume

$$\mathcal{X}_A^1 = \mathcal{X}_A, \quad \mathcal{X}_B^1 = \mathcal{X}_B, \quad \mathcal{X}_A^n = \mathcal{Y}_A, \quad \text{and} \quad \mathcal{X}_B^n = \mathcal{Y}_B;$$

the remaining spaces are arbitrary, so long as they have forms that are appropriate to the choices $\Phi_1, \ldots, \Phi_{n-1}$. For instance, if Φ_k is a local operation for Alice, then $\mathcal{X}_B^k = \mathcal{X}_B^{k+1}$, while if Φ_k is a classical communication from Alice to Bob, then $\mathcal{X}_A^k = \mathcal{X}_A^{k+1} \otimes \mathcal{W}_k$ and $\mathcal{X}_B^{k+1} = \mathcal{X}_B^k \otimes \mathcal{W}_k$ for $\mathcal{W}_k$ representing the system that stores the classical information communicated from Alice to Bob. There is no loss of generality in assuming that every such $\mathcal{W}_k$ takes the form $\mathcal{W}_k = \mathbb{C}^\Gamma$ for some fixed finite and non-empty set Γ, chosen to be large enough to account for any one of the message transmissions among the mappings $\Phi_1, \ldots, \Phi_{n-1}$.

We will take

$$\mathcal{Z}_A = \mathcal{X}_A^1 \oplus \cdots \oplus \mathcal{X}_A^n \qquad \text{and} \qquad \mathcal{Z}_B = \mathcal{X}_B^1 \oplus \cdots \oplus \mathcal{X}_B^n.$$

These spaces will generally not have minimal dimension among the possible choices that would work for the proof, but they are convenient choices that allow for a simple presentation of the

proof. Let us also define isometries $V_{A,k} \in \mathrm{U}\left(\mathcal{X}_A^k, \mathcal{Z}_A\right)$ and $V_{B,k} \in \mathrm{U}\left(\mathcal{X}_B^k, \mathcal{Z}_B\right)$ to be the most straightforward ways of embedding $\mathcal{X}_A^k$ into $\mathcal{Z}_A$ and $\mathcal{X}_B^k$ into $\mathcal{Z}_B$, i.e.,

$$V_{A,k}x_k = \underbrace{0 \oplus \cdots \oplus 0}_{k-1 \text{ times}} \oplus x_k \oplus \underbrace{0 \oplus \cdots \oplus 0}_{n-k \text{ times}}$$

for every choice of $k = 1, \ldots, n$ and $x_1 \in \mathcal{X}_A^1, \ldots, x_n \in \mathcal{X}_A^n$, and likewise for $V_{B,1}, \ldots, V_{B,n}$.

Suppose Φ_k is a local operation for Alice. This means that there exist a collection of operators

$$\{A_{k,a} \,:\, a \in \Sigma\} \subset \mathrm{L}\left(\mathcal{X}_A^k, \mathcal{X}_A^{k+1}\right)$$

such that

$$\sum_{a \in \Sigma} A_{k,a}^* A_{k,a} = \mathbb{1}_{\mathcal{X}_A^k}$$

and

$$\Phi_k(\rho) = \sum_{a \in \Sigma} \left(A_{k,a} \otimes \mathbb{1}_{\mathcal{X}_B^k, \mathcal{X}_B^{k+1}}\right) \rho \left(A_{k,a} \otimes \mathbb{1}_{\mathcal{X}_B^k, \mathcal{X}_B^{k+1}}\right)^*.$$

This expression refers to the identity mapping from $\mathcal{X}_B^k$ to $\mathcal{X}_B^{k+1}$, which makes sense if we keep in mind that these spaces are equal (given that Φ_k is a local operation for Alice). We wish to extend this mapping to an A→B channel on $\mathrm{L}\left(\mathcal{Z}_A \otimes \mathcal{Z}_B\right)$. Let

$$\{B_{k,b} \,:\, b \in \Delta\} \subset \mathrm{L}\left(\mathcal{X}_A^{k+1}, \mathcal{X}_A^k\right)$$

be an arbitrary collection of operators for which

$$\sum_{b \in \Delta} B_{k,b}^* B_{k,b} = \mathbb{1}_{\mathcal{X}_A^{k+1}},$$

and define $C_{k,a,b} \in \mathrm{L}\left(\mathcal{Z}_A\right)$ as

$$C_{k,a,b} = \begin{pmatrix} \mathbb{1}_{\mathcal{X}_A^1} & & & & & & & & \\ & \mathbb{1}_{\mathcal{X}_A^2} & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & B_{k,b} & & & & \\ & & & A_{k,a} & 0 & & & & \\ & & & & & \mathbb{1}_{\mathcal{X}_A^{k+2}} & & & \\ & & & & & & \ddots & & \\ & & & & & & & \mathbb{1}_{\mathcal{X}_A^n} \end{pmatrix}$$

for each $a \in \Sigma$ and $b \in \Delta$, define $U_k \in \mathrm{U}\left(\mathcal{Z}_B\right)$ as

$$U_k = \begin{pmatrix} \mathbb{1}_{\mathcal{X}_A^1} & & & & & & & & \\ & \mathbb{1}_{\mathcal{X}_A^2} & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & \mathbb{1}_{\mathcal{X}_B^{k+1}, \mathcal{X}_B^k} & & & & \\ & & & \mathbb{1}_{\mathcal{X}_B^k, \mathcal{X}_B^{k+1}} & 0 & & & & \\ & & & & & \mathbb{1}_{\mathcal{X}_A^{k+2}} & & & \\ & & & & & & \ddots & & \\ & & & & & & & \mathbb{1}_{\mathcal{X}_A^n} \end{pmatrix},$$

and define

$$\Xi_k(\sigma) = \sum_{\substack{a\in\Sigma\\ b\in\Delta}} \left(C_{k,a,b}\otimes U_k\right)\rho\left(C_{k,a,b}\otimes U_k\right)^*.$$

(In both of the matrices above, empty entries are to be understood as containing zero operators of the appropriate dimensions.) It holds that Ξ_k is an A→B channel, and it may be verified that

$$\Xi_k\left((V_{A,k}\otimes V_{B,k})\rho(V_{A,k}\otimes V_{B,k})^*\right) = (V_{A,k+1}\otimes V_{B,k+1})\Phi_k(\rho)(V_{A,k+1}\otimes V_{B,k+1})^* \tag{16.5}$$

for every $\rho\in \mathrm{L}\left(\mathcal{X}_A^k\otimes\mathcal{X}_B^k\right)$.

In case Φ_k is a local operation for Bob rather than Alice, we define Ξ_k to be a $B\to A$ channel through a similar process, where the roles of Alice and Bob are reversed. The equality (16.5) holds in this case through similar reasoning.

Now suppose that Φ_k is a classical message transmission from Alice to Bob. As stated above, we assume that $\mathcal{X}_A^k = \mathcal{X}_A^{k+1}\otimes\mathbb{C}^\Gamma$ and $\mathcal{X}_B^{k+1} = \mathcal{X}_B^k\otimes\mathbb{C}^\Gamma$. Define

$$C_{k,a} = \begin{pmatrix}
\mathbb{1}_{\mathcal{X}_A^1} & & & & & & & & \\
& \mathbb{1}_{\mathcal{X}_A^2} & & & & & & & \\
& & \ddots & & & & & & \\
& & & 0 & \mathbb{1}_{\mathcal{X}_A^{k+1}}\otimes e_a & & & & \\
& & & \mathbb{1}_{\mathcal{X}_A^{k+1}}\otimes e_a^* & 0 & & & & \\
& & & & & \mathbb{1}_{\mathcal{X}_A^{k+2}} & & & \\
& & & & & & \ddots & & \\
& & & & & & & \mathbb{1}_{\mathcal{X}_A^n}
\end{pmatrix}$$

for each $a\in\Gamma$, define $U_{k,a}\in \mathrm{U}\left(\mathcal{Z}_B\right)$ as

$$U_{k,a} = \begin{pmatrix}
\mathbb{1}_{\mathcal{X}_A^1} & & & & & & & & \\
& \mathbb{1}_{\mathcal{X}_A^2} & & & & & & & \\
& & \ddots & & & & & & \\
& & & 0 & \mathbb{1}_{\mathcal{X}_B^{k+1}}\otimes e_a^* & & & & \\
& & & \mathbb{1}_{\mathcal{X}_B^k}\otimes e_a & \mathbb{1}_{\mathcal{X}_B^{k+1}}\otimes \Pi_a & & & & \\
& & & & & \mathbb{1}_{\mathcal{X}_A^{k+2}} & & & \\
& & & & & & \ddots & & \\
& & & & & & & \mathbb{1}_{\mathcal{X}_A^n}
\end{pmatrix},$$

where

$$\Pi_a = \sum_{\substack{b\in\Gamma\\ b\neq a}} E_{b,b},$$

and define

$$\Xi_k(\sigma) = \sum_{a\in\Gamma}\left(C_{k,a}\otimes U_{k,a}\right)\rho\left(C_{k,a}\otimes U_{k,a}\right)^*.$$

It may be checked that each $U_{k,a}$ is unitary and that $\sum_{a\in\Gamma} C_{k,a}^* C_{k,a} = \mathbb{1}_{\mathcal{Z}_A}$. Thus, Ξ_k is an A→B channel, and once again it may be verified that (16.5) holds for every $\rho\in \mathrm{L}\left(\mathcal{X}_A^k\otimes\mathcal{X}_B^k\right)$. A similar

process is used to define a $B \to A$ channel Ξ_k obeying the equation (16.5) in case Φ_k is a message transmission from Bob to Alice.

By making use of (16.5) iteratively, we find that

$$(\Xi_{n-1} \cdots \Xi_1)\left((V_{A,1} \otimes V_{B,1})\rho(V_{A,1} \otimes V_{B,1})^*\right) = (V_{A,n} \otimes V_{B,n})(\Phi_{n-1} \cdots \Phi_1)(\rho)(V_{A,n} \otimes V_{B,n})^*.$$

Setting $V_A = V_{A,1}$, $V_B = V_{B,1}$, $W_A = V_{A,n}$, $W_B = V_{A,n}$, and recalling that $\mathcal{Y}_A = \mathcal{X}_A^n$ and $\mathcal{Y}_B = \mathcal{X}_B^n$, we have that $\Psi = \Xi_n \cdots \Xi_1$ is a restricted LOCC channel satisfying the requirements of the theorem. □

Next, we observe that restricted LOCC channels can be "collapsed" to a single A→B or B→A channel, assuming their action on a single know pure state is the only concern.

Lemma 16.4. *For any choice of complex Euclidean spaces $\mathcal{Z}_A$ and $\mathcal{Z}_B$ having equal dimension, every restricted LOCC channel $\Phi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$, and every vector $x \in \mathcal{Z}_A \otimes \mathcal{Z}_B$, the following statements hold.*

1. *There exists an $A \to B$ channel $\Psi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ such that $\Psi(xx^*) = \Phi(xx^*)$.*
2. *There exists a $B \to A$ channel $\Psi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ such that $\Psi(xx^*) = \Phi(xx^*)$.*

Proof. The idea of the proof is to show that A→B and B→A channels can be interchanged for fixed pure-state inputs, which allows any restricted LOCC channel to be collapsed to a single A→B or B→A channel by applying the interchanges recursively, and noting that A→B channels and $B \to A$ channels are (separately) both closed under composition.

Suppose that $\{A_a : a \in \Sigma\} \subset \mathrm{L}(\mathcal{Z}_A)$ is a collection of operators for which $\sum_{a\in\Sigma} A_a^* A = \mathbb{1}_{\mathcal{Z}_A}$, $\{U_a : a \in \Sigma\} \subset \mathrm{U}(\mathcal{Z}_B)$ is a collection of unitary operators, and

$$\Xi(\rho) = \sum_{a\in\Sigma} (A_a \otimes U_a)\rho(A_a \otimes U_a)^*$$

is the A→B channel that is described by these operators. Let $X \in \mathrm{L}(\mathcal{Z}_B, \mathcal{Z}_A)$ satisfy $\mathrm{vec}(X) = x$. It holds that

$$\Xi(xx^*) = \Xi(\mathrm{vec}(X)\,\mathrm{vec}(X)^*) = \sum_{a\in\Sigma} \mathrm{vec}\left(A_a X U_a^{\mathsf{T}}\right)\mathrm{vec}\left(A_a X U_a^{\mathsf{T}}\right)^*.$$

Our goal is to find a collection of operators $\{B_a : a \in \Sigma\} \subset \mathrm{L}(\mathcal{Z}_B)$ satisfying $\sum_{a\in\Sigma} B_a^* B_a = \mathbb{1}_{\mathcal{Z}_B}$ and a collection of unitary operators $\{V_a : a \in \Sigma\} \subset \mathrm{U}(\mathcal{Z}_A)$ such that

$$V_a X B_a^{\mathsf{T}} = A_a X U_a^{\mathsf{T}}$$

for all $a \in \Sigma$. If such a collection of operators is found, then we will have that

$$\begin{aligned}\sum_{a\in\Sigma} (V_a \otimes B_a)\,\mathrm{vec}(X)\,\mathrm{vec}(X)^*(V_a \otimes B_a)^* &= \sum_{a\in\Sigma} \mathrm{vec}(V_a X B_a^{\mathsf{T}})\,\mathrm{vec}(V_a X B_a^{\mathsf{T}})^* \\ &= \sum_{a\in\Sigma} \mathrm{vec}(A_a X U_a^{\mathsf{T}})\,\mathrm{vec}(A_a X U_a^{\mathsf{T}})^* = \sum_{a\in\Sigma} (A_a \otimes U_a)\,\mathrm{vec}(X)\,\mathrm{vec}(X)^*(A_a \otimes U_a)^*,\end{aligned}$$

so that $\Xi(uu^*) = \Lambda(uu^*)$ for Λ being the B→A channel defined by

$$\Lambda(\rho) = \sum_{a\in\Sigma} (V_a \otimes B_a)\rho(V_a \otimes B_a)^*.$$

Choose a unitary operator $U \in \mathrm{U}(\mathcal{Z}_A, \mathcal{Z}_B)$ such that $XU \in \mathrm{Pos}(\mathcal{Z}_A)$. Such a U can be found by considering a singular value decomposition of X. Also, for each $a \in \Sigma$, choose a unitary operator $W_a \in \mathrm{U}(\mathcal{Z}_A, \mathcal{Z}_B)$ such that

$$A_a X U_a^{\mathsf{T}} W_a \in \mathrm{Pos}(\mathcal{Z}_A).$$

We have that

$$A_a X U_a^{\mathsf{T}} W_a = (A_a X U_a^{\mathsf{T}} W_a)^* = (A_a (XU) U^* U_a^{\mathsf{T}} W_a)^* = W_a^* \overline{U_a} U (XU) A_a^*,$$

so that

$$A_a X U_a^{\mathsf{T}} = W_a^* \overline{U_a} U X U A_a^* W_a^*.$$

Define

$$V_a = W_a^* \overline{U_a} U \qquad \text{and} \qquad B_a = (U A_a^* W_a^*)^{\mathsf{T}}$$

for each $a \in \Sigma$. Each V_a is unitary and it can be checked that

$$\sum_{a \in \Sigma} B_a^* B_a = \mathbb{1}_{\mathcal{Z}_B}.$$

We have $V_a X B_a^{\mathsf{T}} = A_a X U_a^{\mathsf{T}}$ as required.

We have therefore proved that for every A→B channel $\Xi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$, there exists a B→A channel $\Lambda \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ such that $\Xi(xx^*) = \Lambda(xx^*)$. A symmetric argument shows that for every B→A channel Ξ, there exists an A→B channel Λ such that $\Lambda(xx^*) = \Xi(xx^*)$.

Finally, notice that the composition of any two A→B channels is also an A→B channel, and likewise for B→A channels. Therefore, by applying the above arguments repeatedly for the A→B and B→A channels from which Φ is composed, we find that there exists an A→B channel Ψ such that $\Psi(uu^*) = \Phi(uu^*)$, and likewise for Ψ being a B→A channel. □

We are now prepared to finish the proof of Nielsen's theorem. We assume that there exists an LOCC channel Φ mapping xx^* to yy^*. By Theorem 16.2 and Lemma 16.4, we have that there is no loss of generality in assuming $x, y \in \mathcal{Z}_A \otimes \mathcal{Z}_B$ for $\mathcal{Z}_A$ and $\mathcal{Z}_B$ having equal dimension, and moreover that $\Phi \in \mathrm{C}(\mathcal{Z}_A \otimes \mathcal{Z}_B)$ is a B→A channel. Write

$$\Phi(\rho) = \sum_{a \in \Sigma} (V_a \otimes B_a) \rho (V_a \otimes B_a)^*,$$

for $\{B_a : a \in \Sigma\}$ satisfying $\sum_{a \in \Sigma} B_a^* B_a = \mathbb{1}_{\mathcal{Z}_B}$ and $\{V_a : a \in \Sigma\}$ being a collection of unitary operators on $\mathcal{Z}_A$.

Let $X, Y \in \mathrm{L}(\mathcal{Z}_B, \mathcal{Z}_A)$ satisfy $x = \mathrm{vec}(X)$ and $y = \mathrm{vec}(Y)$, so that

$$\Phi(\mathrm{vec}(X)\,\mathrm{vec}(X)^*) = \sum_{a \in \Sigma} \mathrm{vec}(V_a X B_a^{\mathsf{T}})\,\mathrm{vec}(V_a X B_a^{\mathsf{T}})^* = \mathrm{vec}(Y)\,\mathrm{vec}(Y)^*.$$

This implies that

$$V_a X B_a^{\mathsf{T}} = \alpha_a Y$$

and therefore

$$X B_a^{\mathsf{T}} = \alpha_a V_a^* Y$$

for each $a \in \Sigma$, where $\{\alpha_a : a \in \Sigma\}$ is a collection of complex numbers. We now have

$$\sum_{a \in \Sigma} |\alpha_a|^2 V_a^* Y Y^* V_a = \sum_{a \in \Sigma} X B_a^{\mathsf{T}} \overline{B_a} X^* = X X^*.$$

Taking the trace of both sides of this equation reveals that $\sum_{a \in \Sigma} |\alpha_a|^2 = 1$. It has therefore been shown that there exists a mixed unitary channel mapping YY^* to XX^*. It therefore holds that $XX^* \prec YY^*$ (or, equivalently, $\mathrm{Tr}_{\mathcal{Z}_B}(xx^*) \prec \mathrm{Tr}_{\mathcal{Z}_B}(yy^*)$) as required.

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

Lecture 17: Measures of entanglement

The topic of this lecture is *measures of entanglement*. The underlying idea throughout this discussion is that entanglement may be viewed as a resource that is useful for various communication-related tasks, such as teleportation, and we would like to quantify the amount of entanglement that is contained in different states.

17.1 Maximum inner product with a maximally entangled state

We will begin with a simple quantity that relates to the amount of entanglement in a given state: the maximum inner product with a maximally entangled state. It is not necessarily an interesting concept in its own right, but it will be useful as a mathematical tool in the sections of this lecture that follow.

Suppose $\mathcal{X}$ and $\mathcal{Y}$ are complex Euclidean spaces, and assume for the moment that $\dim(\mathcal{X}) \geq \dim(\mathcal{Y}) = n$. A *maximally entangled state* of a pair of registers (X, Y) to which these spaces are associated is any pure state uu^* for which

$$\mathrm{Tr}_{\mathcal{X}}(uu^*) = \frac{1}{n}\mathbb{1}_{\mathcal{Y}};$$

or, in other words, tracing out the larger space leaves the completely mixed state on the other register. Equivalently, the maximally entangled states are those that may be expressed as

$$\frac{1}{n}\,\mathrm{vec}(U)\,\mathrm{vec}(U)^*$$

for some choice of a linear isometry $U \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$. If it is the case that $n = \dim(\mathcal{X}) \leq \dim(\mathcal{Y})$ then the maximally entangled states are those states uu^* such that

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = \frac{1}{n}\mathbb{1}_{\mathcal{X}},$$

or equivalently those that can be written

$$\frac{1}{n}\,\mathrm{vec}(U^*)\,\mathrm{vec}(U^*)^*$$

where $U \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$ is a linear isometry. Quite frequently, the term *maximally entangled* refers to the situation in which $\dim(\mathcal{X}) = \dim(\mathcal{Y})$, where the two notions coincide. As is to be expected when discussing pure states, we sometimes refer to a unit vector u as being a maximally entangled state, which means that uu^* is maximally entangled.

Now, for an arbitrary density operator $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$, let us define

$$M(\rho) = \max\{\langle uu^*, \rho\rangle \,:\, u \in \mathcal{X} \otimes \mathcal{Y} \text{ is maximally entangled}\}.$$

Clearly it holds that $0 < M(\rho) \leq 1$ for every density operator $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$. The following lemma establishes an upper bound on $M(\rho)$ based on the min-rank of ρ.

Lemma 17.1. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, and let $n = \min\{\dim(\mathcal{X}), \dim(\mathcal{Y})\}$. It holds that*

$$M(\rho) \leq \frac{\text{min-rank}(\rho)}{n}$$

for all $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$.

Proof. Let us assume $\dim(\mathcal{X}) \geq \dim(\mathcal{Y}) = n$, and note that the argument is equivalent in case the inequality is reversed.

First let us note that M is a convex function on $\mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$. To see this, consider any choice of $\sigma, \xi \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ and $p \in [0,1]$. For $U \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$ we have

$$\begin{aligned}
&\frac{1}{n} \operatorname{vec}(U)^* \left(p\sigma + (1-p)\xi\right) \operatorname{vec}(U) \\
&\qquad = p \, \frac{1}{n} \operatorname{vec}(U)^* \sigma \operatorname{vec}(U) + (1-p) \, \frac{1}{n} \operatorname{vec}(U)^* \xi \operatorname{vec}(U) \\
&\qquad \leq pM(\sigma) + (1-p)M(\xi).
\end{aligned}$$

Maximizing over all $U \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$ establishes that M is convex as claimed.

Now, given that M is convex, we see that it suffices to prove the lemma by considering only pure states. Every pure density operator on $\mathcal{X} \otimes \mathcal{Y}$ may be written as $\operatorname{vec}(A) \operatorname{vec}(A)^*$ for $A \in \mathrm{L}(\mathcal{Y}, \mathcal{X})$ satisfying $\|A\|_2 = 1$. We have

$$M\left(\operatorname{vec}(A) \operatorname{vec}(A)^*\right) = \frac{1}{n} \max_{U \in \mathrm{U}(\mathcal{Y}, \mathcal{X})} |\langle U, A \rangle|^2 = \frac{1}{n} \|A\|_1^2 .$$

Given that

$$\|A\|_1 \leq \sqrt{\operatorname{rank}(A)} \, \|A\|_2$$

for every operator A, the lemma follows. □

17.2 Entanglement cost and distillable entanglement

We will now discuss two fundamental measures of entanglement: the *entanglement cost* and the *distillable entanglement*. For the remainder of the lecture, let us take

$$\mathcal{Y}_A = \mathbb{C}^{\{0,1\}} \quad \text{and} \quad \mathcal{Y}_B = \mathbb{C}^{\{0,1\}}$$

to be complex Euclidean spaces corresponding to single qubits, and let $\tau \in \mathrm{D}(\mathcal{Y}_A \otimes \mathcal{Y}_B)$ denote the density operator

$$\tau = \frac{1}{2}(e_0 \otimes e_0 + e_1 \otimes e_1)(e_0 \otimes e_0 + e_1 \otimes e_1)^*,$$

which may be more recognizable to some when expressed in the Dirac notation as

$$\tau = \left|\phi^+\right\rangle \left\langle\phi^+\right| \qquad \text{for} \qquad \left|\phi^+\right\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle .$$

We view that the state τ represents one unit of entanglement, typically called an *e-bit* of entanglement.

17.2.1 Definition of entanglement cost

The first measure of entanglement we will consider is called the *entanglement cost*. Informally speaking, the entanglement cost of a density operator $\rho \in \mathrm{D}(\mathcal{X}_A \otimes \mathcal{X}_B)$ represents the number of e-bits Alice and Bob need to share in order to create a copy of ρ by means of an LOCC operation with high fidelity. It is an information-theoretic quantity, so it must be understood to be asymptotic in nature—where one amortizes over many parallel repetitions of such a conversion. The following definition states this more precisely.

Definition 17.2. The *entanglement cost* of a density operator $\rho \in \mathrm{D}(\mathcal{X}_A \otimes \mathcal{X}_B)$, denoted $E_c(\rho)$, is the infimum over all real numbers $\alpha \geq 0$ for which there exists a sequence of LOCC channels $\{\Phi_n : n \in \mathbb{N}\}$, where

$$\Phi_n \in \mathrm{LOCC}\left(\mathcal{Y}_A^{\otimes \lfloor \alpha n \rfloor}, \mathcal{X}_A^{\otimes n} : \mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}, \mathcal{X}_B^{\otimes n}\right),$$

such that

$$\lim_{n\to\infty} \mathrm{F}\left(\Phi_n\left(\tau^{\otimes \lfloor \alpha n \rfloor}\right), \rho^{\otimes n}\right) = 1.$$

The interpretation of the definition is that, in the limit of large n, Alice and Bob are able to convert $\lfloor \alpha n \rfloor$ e-bits into n copies of ρ with high fidelity for any $\alpha > E_c(\rho)$. It is not entirely obvious that there should exist any value of α for which there exists a sequence of LOCC channels $\{\Phi_n : n \in \mathbb{N}\}$ as in the statement of the definition, but indeed there always does exist a suitable choice of α.

17.2.2 Definition of distillable entanglement

The second measure of entanglement we will consider is the *distillable entanglement*, which is essentially the reverse of the entanglement cost. It quantifies the number of e-bits that Alice and Bob can extract from the state in question, again amortized over many copies.

Definition 17.3. The *distillable entanglement* of a density operator $\rho \in \mathrm{D}(\mathcal{X}_A \otimes \mathcal{X}_B)$, denoted $E_d(\rho)$, is the supremum over all real numbers $\alpha \geq 0$ for which there exists a sequence of LOCC channels $\{\Phi_n : n \in \mathbb{N}\}$, where

$$\Phi_n \in \mathrm{LOCC}\left(\mathcal{X}_A^{\otimes n}, \mathcal{Y}_A^{\otimes \lfloor \alpha n \rfloor} : \mathcal{X}_B^{\otimes n}, \mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}\right),$$

such that

$$\lim_{n\to\infty} \mathrm{F}\left(\Phi_n\left(\rho^{\otimes n}\right), \tau^{\otimes \lfloor \alpha n \rfloor}\right) = 1.$$

The interpretation of the definition is that, in the limit of large n, Alice and Bob are able to convert n copies of ρ into $\lfloor \alpha n \rfloor$ e-bits with high fidelity for any $\alpha < E_d(\rho)$. In order to clarify the definition, let us state explicitly that the operator $\tau^{\otimes 0}$ is interpreted to be the scalar 1, implying that condition in the lemma is trivially satisfied for $\alpha = 0$.

17.2.3 The distillable entanglement is at most the entanglement cost

At an intuitive level it is clear that the entanglement cost must be at least as large as the distillable entanglement, for otherwise Alice and Bob would be able to open an "entanglement factory" that would violate the principle that LOCC channels cannot create entanglement out of thin air. Let us now prove this formally.

Theorem 17.4. *For every state $\rho \in \mathrm{D}(\mathcal{X}_A \otimes \mathcal{X}_B)$ we have $E_d(\rho) \leq E_c(\rho)$.*

Proof. Let us assume that α and β are nonnegative real numbers such that the following two properties are satisfied:

1. There exists a sequence of LOCC channels $\{\Phi_n : n \in \mathbb{N}\}$, where
$$\Phi_n \in \mathrm{LOCC}\left(\mathcal{Y}_A^{\otimes \lfloor \alpha n \rfloor}, \mathcal{X}_A^{\otimes n} : \mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}, \mathcal{X}_B^{\otimes n}\right),$$
such that
$$\lim_{n\to\infty} \mathrm{F}\left(\Phi_n\left(\tau^{\otimes \lfloor \alpha n \rfloor}\right), \rho^{\otimes n}\right) = 1.$$
2. There exists a sequence of LOCC channels $\{\Psi_n : n \in \mathbb{N}\}$, where
$$\Psi_n \in \mathrm{LOCC}\left(\mathcal{X}_A^{\otimes n}, \mathcal{Y}_A^{\otimes \lfloor \beta n \rfloor} : \mathcal{X}_B^{\otimes n}, \mathcal{Y}_B^{\otimes \lfloor \beta n \rfloor}\right),$$
such that
$$\lim_{n\to\infty} \mathrm{F}\left(\Psi_n\left(\rho^{\otimes n}\right), \tau^{\otimes \lfloor \beta n \rfloor}\right) = 1.$$

Using the Fuchs–van de Graaf inequalities, along with triangle inequality for the trace norm, we conclude that
$$\lim_{n\to\infty} \mathrm{F}\left((\Psi_n \Phi_n)\left(\tau^{\otimes \lfloor \alpha n \rfloor}\right), \tau^{\otimes \lfloor \beta n \rfloor}\right) = 1. \tag{17.1}$$
Because $\text{min-rank}(\tau^{\otimes k}) = 2^k$ for every choice of $k \geq 1$, and LOCC channels cannot increase min-rank, we have that
$$\mathrm{F}\left((\Psi_n \Phi_n)\left(\tau^{\otimes \lfloor \alpha n \rfloor}\right), \tau^{\otimes \lfloor \beta n \rfloor}\right)^2 \leq 2^{\lfloor \alpha n \rfloor - \lfloor \beta n \rfloor} \tag{17.2}$$
by Lemma 17.1. By equations (17.1) and (17.2), we therefore have that $\alpha \geq \beta$.

Given that $E_c(\rho)$ is the infimum over all α, and $E_d(\rho)$ is the supremum over all β, with the above properties, we have that $E_c(\rho) \geq E_d(\rho)$ as required. □

17.3 Pure state entanglement

The remainder of the lecture will focus on the entanglement cost and distillable entanglement for bipartite pure states. In this case, these measures turn out to be identical, and coincide precisely with the von Neumann entropy of the reduced state of either subsystem.

Theorem 17.5. *Let $\mathcal{X}_A$ and $\mathcal{X}_B$ be complex Euclidean spaces and let $u \in \mathcal{X}_A \otimes \mathcal{X}_B$ be a unit vector. It holds that $E_c(uu^*) = E_d(uu^*) = S(\mathrm{Tr}_{\mathcal{X}_A}(uu^*)) = S(\mathrm{Tr}_{\mathcal{X}_B}(uu^*))$.*

Proof. The proof will start with some basic observations about the vector u that will be used to calculate both the entanglement cost and the distillable entanglement. First, let
$$u = \sum_{a\in\Sigma} \sqrt{p(a)}\, v_a \otimes w_a$$
be a Schmidt decomposition of u, so that
$$\mathrm{Tr}_{\mathcal{X}_B}(uu^*) = \sum_{a\in\Sigma} p(a)\, v_a v_a^* \qquad \text{and} \qquad \mathrm{Tr}_{\mathcal{X}_A}(uu^*) = \sum_{a\in\Sigma} p(a)\, w_a w_a^*.$$

We have that $p \in \mathbb{R}^{\Sigma}$ is a probability vector, and $S(\mathrm{Tr}_{\mathcal{X}_A}(uu^*)) = H(p) = S(\mathrm{Tr}_{\mathcal{X}_B}(uu^*))$. Let us assume hereafter that $H(p) > 0$, for the case $H(p) = 0$ corresponds to the situation where u is separable (in which case the entanglement cost and distillable entanglement are both easily seen to be 0).

We will make use of concepts regarding compression that were discussed in Lecture 9. Recall that for each choice of n and $\varepsilon > 0$, we denote by $T_{n,\varepsilon} \subseteq \Sigma^n$ the set of ε-typical sequences of length n with respect to the probability vector p:

$$T_{n,\varepsilon} = \left\{ a_1 \cdots a_n \in \Sigma^n \,:\, 2^{-n(H(p)+\varepsilon)} < p(a_1) \cdots p(a_n) < 2^{-n(H(p)-\varepsilon)} \right\}.$$

For each $n \in \mathbb{N}$ and $\varepsilon > 0$, let us define a vector

$$x_{n,\varepsilon} = \sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} \sqrt{p(a_1) \cdots p(a_n)}\, (v_{a_1} \otimes w_{a_1}) \otimes \cdots \otimes (v_{a_n} \otimes w_{a_n}) \in (\mathcal{X}_A \otimes \mathcal{X}_B)^{\otimes n}.$$

We have

$$\| x_{n,\varepsilon} \|^2 = \sum_{a_1 \cdots a_n \in T_{n,\varepsilon}} p(a_1) \cdots p(a_n),$$

which is the probability that a random choice of $a_1 \cdots a_n$ is ε-typical with respect to the probability vector p. It follows that $\lim_{n\to\infty} \| x_{n,\varepsilon} \| = 1$ for any choice of $\varepsilon > 0$. Let

$$y_{n,\varepsilon} = \frac{x_{n,\varepsilon}}{\| x_{n,\varepsilon} \|}$$

denote the normalized versions of these vectors.

Next, consider the vector of eigenvalues

$$\lambda\left(\mathrm{Tr}_{\mathcal{X}_B^{\otimes n}} \left(x_{n,\varepsilon} x_{n,\varepsilon}^* \right) \right).$$

The nonzero eigenvalues are given by the probabilities for the various ε-typical sequences, and so

$$2^{-n(H(p)+\varepsilon)} \;<\; \lambda_j\left(\mathrm{Tr}_{\mathcal{X}_B^{\otimes n}} \left(x_{n,\varepsilon} x_{n,\varepsilon}^* \right) \right) \;<\; 2^{-n(H(p)-\varepsilon)}$$

for $j = 1, \ldots, |T_{n,\varepsilon}|$. (The remaining eigenvalues are 0.) It follows that

$$\frac{2^{-n(H(p)+\varepsilon)}}{\| x_{n,\varepsilon} \|^2} \;<\; \lambda_j\left(\mathrm{Tr}_{\mathcal{X}_B^{\otimes n}} \left(y_{n,\varepsilon} y_{n,\varepsilon}^* \right) \right) \;<\; \frac{2^{-n(H(p)-\varepsilon)}}{\| x_{n,\varepsilon} \|^2}$$

for $j = 1, \ldots, |T_{n,\varepsilon}|$, and again the remaining eigenvalues are 0.

Let us now consider the entanglement cost of uu^*. We wish to show that for every real number $\alpha > H(p)$ there exists a sequence $\{\Phi_n : n \in \mathbb{N}\}$ of LOCC channels such that

$$\lim_{n\to\infty} \mathrm{F}\left(\Phi_n\left(\tau^{\otimes \lfloor \alpha n \rfloor} \right), (uu^*)^{\otimes n} \right) = 1. \tag{17.3}$$

We will do this by means of Nielsen's theorem. Specifically, let us choose $\varepsilon > 0$ so that $\alpha > H(p) + 2\varepsilon$, from which it follows that $\lfloor \alpha n \rfloor \geq n(H(p) + \varepsilon)$ for sufficiently large n. We have

$$\lambda_j\left(\mathrm{Tr}_{\mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}} \left(\tau^{\otimes \lfloor \alpha n \rfloor} \right) \right) = 2^{-\lfloor \alpha n \rfloor}$$

for $j = 1, \ldots, 2^{\lfloor \alpha n \rfloor}$. Given that

$$\frac{2^{-n(H(p)+\varepsilon)}}{\|x_{n,\varepsilon}\|^2} \geq 2^{-n(H(p)+\varepsilon)} \geq 2^{-\lfloor \alpha n \rfloor},$$

for sufficiently large n, it follows that

$$\mathrm{Tr}_{\mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}} \left(\tau^{\otimes \lfloor \alpha n \rfloor} \right) \prec \mathrm{Tr}_{\mathcal{X}_B^{\otimes n}} \left(y_{n,\varepsilon} y_{n,\varepsilon}^* \right). \tag{17.4}$$

This means that $\tau^{\otimes \lfloor \alpha n \rfloor}$ can be converted to $y_{n,\varepsilon} y_{n,\varepsilon}^*$ by means of an LOCC channel Φ_n by Nielsen's theorem. Given that

$$\lim_{n \to \infty} \mathrm{F} \left(y_{n,\varepsilon} y_{n,\varepsilon}^*, (uu^*)^{\otimes n} \right) = 1$$

this implies that the required equation (17.3) holds. Consequently $E_c(uu^*) \leq H(p)$.

Next let us consider the distillable entanglement, for which a similar argument is used. Our goal is to prove that for every $\alpha < H(p)$, there exists a sequence $\{\Psi_n : n \in \mathbb{N}\}$ of LOCC channels such that

$$\lim_{n \to \infty} \mathrm{F} \left(\Psi_n \left((uu^*)^{\otimes n} \right), \tau^{\otimes \lfloor \alpha n \rfloor} \right) = 1. \tag{17.5}$$

In this case, let us choose $\varepsilon > 0$ small enough so that $\alpha < H(p) - 2\varepsilon$. For sufficiently large n we have

$$2^{\lfloor \alpha n \rfloor} \leq \|x_{n,\varepsilon}\|^2 2^{n(H(p)-\varepsilon)}.$$

Similar to above, we therefore have

$$\mathrm{Tr}_{\mathcal{X}_B^{\otimes n}} \left(y_{n,\varepsilon} y_{n,\varepsilon}^* \right) \prec \mathrm{Tr}_{\mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}} \left(\tau^{\otimes \lfloor \alpha n \rfloor} \right),$$

which implies that the state $y_{n,\varepsilon} y_{n,\varepsilon}^*$ can be converted to the state $\tau^{\otimes \lfloor \alpha n \rfloor}$ by means of an LOCC channel Ψ_n for sufficiently large n. Given that

$$\lim_{n \to \infty} \left\| (uu^*)^{\otimes n} - y_{n,\varepsilon} y_{n,\varepsilon}^* \right\|_1 = 0$$

it follows that

$$\begin{aligned} &\lim_{n \to \infty} \left\| \Psi_n \left((uu^*)^{\otimes n} \right) - \tau^{\otimes \lfloor \alpha n \rfloor} \right\|_1 \\ &\qquad \leq \lim_{n \to \infty} \left(\left\| \Psi_n \left((uu^*)^{\otimes n} \right) - \Psi_n \left(y_{n,\varepsilon} y_{n,\varepsilon}^* \right) \right\|_1 + \left\| \Psi_n \left(y_{n,\varepsilon} y_{n,\varepsilon}^* \right) - \tau^{\otimes \lfloor \alpha n \rfloor} \right\|_1 \right) = 0, \end{aligned}$$

which establishes the above equation (17.5). Consequently, $E_d(uu^*) \geq H(p)$.

We have shown that

$$E_c(uu^*) \leq H(p) \leq E_d(uu^*).$$

As $E_d(uu^*) \leq E_c(uu^*)$, the equality in the statement of the theorem follows. □

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

Lecture 18: The partial transpose and its relationship to entanglement and distillation

In this lecture we will discuss the partial transpose mapping and its connection to entanglement and distillation. Through this study, we will find that there exist *bound-entangled states*, which are states that are entangled and yet have zero distillable entanglement.

18.1 The partial transpose and separability

Recall the Woronowicz–Horodecki criterion for separability: for complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, we have that a given operator $P \in \text{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is separable if and only if

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

for every choice of a positive unital mapping $\Phi \in \text{T}(\mathcal{X}, \mathcal{Y})$. We note, however, that the restriction of the mapping Φ to be both unital and to take the form $\Phi \in \text{T}(\mathcal{X}, \mathcal{Y})$ can be relaxed. Specifically, the Woronowicz–Horodecki criterion implies the truth of the following two facts:

1. If $P \in \text{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is separable, then for every choice of a complex Euclidean space $\mathcal{Z}$ and a positive mapping $\Phi \in \text{T}(\mathcal{X}, \mathcal{Z})$, we have
$$(\Phi \otimes \mathbb{1}_{\text{L}(\mathcal{Y})})(P) \in \text{Pos}(\mathcal{Z} \otimes \mathcal{Y}).$$
2. If $P \in \text{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is not separable, there exists a positive mapping $\Phi \in \text{T}(\mathcal{X}, \mathcal{Z})$ that reveals this fact, in the sense that
$$(\Phi \otimes \mathbb{1}_{\text{L}(\mathcal{Y})})(P) \notin \text{Pos}(\mathcal{Z} \otimes \mathcal{Y}).$$
Moreover, there exists such a mapping Φ that is unital and for which $\mathcal{Z} = \mathcal{Y}$.

It is clear that the criterion illustrates a connection between separability and positive mappings that are not completely positive, for if $\Phi \in \text{T}(\mathcal{X}, \mathcal{Z})$ is completely positive, then

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

for every completely positive mapping $\Phi \in \text{T}(\mathcal{X}, \mathcal{Z})$, regardless of whether P is separable or not.

Thus far, we have only seen one example of a mapping that is positive but not completely positive: the transpose. Let us recall that the transpose mapping $T \in \text{T}(\mathcal{X})$ on a complex Euclidean space $\mathcal{X}$ is defined as

$$T(X) = X^{\text{T}}$$

for all $X \in \text{L}(\mathcal{X})$. The positivity of T is clear: $X \in \text{Pos}(\mathcal{X})$ if and only if $X^{\text{T}} \in \text{Pos}(\mathcal{X})$ for every $X \in \text{L}(\mathcal{X})$. Assuming that $\mathcal{X} = \mathbb{C}^{\Sigma}$, we have

$$T(X) = \sum_{a,b \in \Sigma} E_{a,b} X E_{a,b} = \sum_{a,b \in \Sigma} E_{a,b} X E_{b,a}^{*}$$

for all $X \in \mathrm{L}(\mathcal{X})$. The Choi–Jamiołkowski representation of T is

$$J(T) = \sum_{a,b \in \Sigma} E_{b,a} \otimes E_{a,b} = W$$

where $W \in \mathrm{U}(\mathcal{X} \otimes \mathcal{X})$ denotes the swap operator. The fact that W is not positive semidefinite shows that T is not completely positive.

When we refer to the *partial transpose*, we mean that the transpose mapping is tensored with the identity mapping on some other space. We will use a similar notation to the partial trace: for given complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, we define

$$T_{\mathcal{X}} = T \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y})} \in \mathrm{T}(\mathcal{X} \otimes \mathcal{Y}).$$

More generally, the subscript refers to the space on which the transpose is performed.

Given that the transpose is positive, we may conclude the following from the Woronowicz–Horodecki criterion for any choice of $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$:

1. If P is separable, then $T_{\mathcal{X}}(P)$ is necessarily positive semidefinite.
2. If P is not separable, then $T_{\mathcal{X}}(P)$ might or might not be positive semidefinite, although nothing definitive can be concluded from the criterion.

Another way to view these observations is that they describe a sort of one-sided test for entanglement:

1. If $T_{\mathcal{X}}(P)$ is not positive semidefinite for a given $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$, then P is definitely not separable.
2. If $T_{\mathcal{X}}(P)$ is positive semidefinite for a given $P \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$, then P may or may not be separable.

We have seen a specific example where the transpose indeed does identify entanglement: if Σ is a finite, nonempty set of size n, and we take $\mathcal{X}_A = \mathbb{C}^{\Sigma}$ and $\mathcal{X}_B = \mathbb{C}^{\Sigma}$, then

$$P = \frac{1}{n} \sum_{a,b \in \Sigma} E_{a,b} \otimes E_{a,b} \in \mathrm{D}(\mathcal{X}_A \otimes \mathcal{X}_B)$$

is certainly entangled, because

$$T_{\mathcal{X}_A}(P) = \frac{1}{n} W \notin \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B).$$

We will soon prove that indeed there do exist entangled operators $P \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$ for which $T_{\mathcal{X}_A}(P) \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$, which means that the partial transpose does not give a simple test for separability. It turns out, however, that the partial transpose does have an interesting connection to entanglement distillation, as we will see later in the lecture.

For the sake of discussing this issue in greater detail, let us consider the following definition. For any choice of complex Euclidean spaces $\mathcal{X}_A$ and $\mathcal{X}_B$, we define

$$\mathrm{PPT}(\mathcal{X}_A : \mathcal{X}_B) = \{P \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B) \,:\, T_{\mathcal{X}_A}(P) \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)\}.$$

The acronym PPT stands for *positive partial transpose*.

It is the case that the set $\mathrm{PPT}(\mathcal{X}_A : \mathcal{X}_B)$ is a closed convex cone. Let us also note that this notion respects tensor products, meaning that if $P \in \mathrm{PPT}(\mathcal{X}_A : \mathcal{X}_B)$ and $Q \in \mathrm{PPT}(\mathcal{Y}_A : \mathcal{Y}_B)$, then

$$P \otimes Q \in \mathrm{PPT}(\mathcal{X}_A \otimes \mathcal{Y}_A : \mathcal{X}_B \otimes \mathcal{Y}_B).$$

Finally, notice that the definition of $\mathrm{PPT}(\mathcal{X}_A : \mathcal{X}_B)$ does not really depend on the fact that the partial transpose is performed on $\mathcal{X}_A$ as opposed to $\mathcal{X}_B$. This follows from the observation that

$$T(T_{\mathcal{X}_A}(X)) = T_{\mathcal{X}_B}(X)$$

for every $X \in \mathrm{L}(\mathcal{X}_A \otimes \mathcal{X}_B)$, and therefore

$$T_{\mathcal{X}_A}(X) \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B) \quad \Leftrightarrow \quad T_{\mathcal{X}_B}(X) \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B).$$

18.2 Examples of non-separable PPT operators

In this section we will discuss two examples of operators that are both entangled and PPT. This shows that the partial transpose test does not give an efficient test for separability, and also implies something interesting about entanglement distillation to be discussed in the next section.

18.2.1 First example

Let us begin by considering the following collection of operators, all of which act on the complex Euclidean space $\mathbb{C}^{\mathbb{Z}_n} \otimes \mathbb{C}^{\mathbb{Z}_n}$ for an integer $n \geq 2$. We let

$$W_n = \sum_{a,b \in \mathbb{Z}_n} E_{b,a} \otimes E_{a,b}$$

denote the swap operator, which we have now seen several times. It satisfies $W_n(u \otimes v) = v \otimes u$ for all $u, v \in \mathbb{C}^{\mathbb{Z}_n}$. Let us also define

$$\begin{aligned} P_n &= \frac{1}{n} \sum_{a,b \in \mathbb{Z}_n} E_{a,b} \otimes E_{a,b}\,, & R_n &= \frac{1}{2}\mathbb{1} \otimes \mathbb{1} - \frac{1}{2} W_n\,, \\ Q_n &= \mathbb{1} \otimes \mathbb{1} - P_n\,, & S_n &= \frac{1}{2}\mathbb{1} \otimes \mathbb{1} + \frac{1}{2} W_n. \end{aligned} \tag{18.1}$$

It holds that P_n, Q_n, R_n, and S_n are projection operators with $P_n + Q_n = R_n + S_n = \mathbb{1} \otimes \mathbb{1}$. The operator R_n is the projection onto the *anti-symmetric subspace* of $\mathbb{C}^{\mathbb{Z}_n} \otimes \mathbb{C}^{\mathbb{Z}_n}$ and S_n is the projection onto the *symmetric subspace* of $\mathbb{C}^{\mathbb{Z}_n} \otimes \mathbb{C}^{\mathbb{Z}_n}$.

We have that

$$(T \otimes \mathbb{1})(P_n) = \frac{1}{n} W_n \qquad \text{and} \qquad (T \otimes \mathbb{1})(\mathbb{1} \otimes \mathbb{1}) = \mathbb{1} \otimes \mathbb{1},$$

from which the following equations follow:

$$\begin{aligned} (T \otimes \mathbb{1})(P_n) &= -\frac{1}{n} R_n + \frac{1}{n} S_n, & (T \otimes \mathbb{1})(R_n) &= -\frac{n-1}{2} P_n + \frac{1}{2} Q_n, \\ (T \otimes \mathbb{1})(Q_n) &= \frac{n+1}{n} R_n + \frac{n-1}{n} S_n, & (T \otimes \mathbb{1})(S_n) &= \frac{n+1}{2} P_n + \frac{1}{2} Q_n. \end{aligned}$$

Now let us suppose we have registers X_2, Y_2, X_3, and Y_3, where

$$\mathcal{X}_2 = \mathbb{C}^{\mathbb{Z}_2}, \quad \mathcal{Y}_2 = \mathbb{C}^{\mathbb{Z}_2}, \quad \mathcal{X}_3 = \mathbb{C}^{\mathbb{Z}_3}, \quad \mathcal{Y}_3 = \mathbb{C}^{\mathbb{Z}_3}.$$

In other words, X_2 and Y_2 are qubit registers, while X_3 and Y_3 are qutrit registers. We will imagine the situation in which Alice holds registers X_2 and X_3, while Bob holds Y_2 and Y_3.

For every choice of $\alpha > 0$, define

$$X_\alpha = Q_3 \otimes Q_2 + \alpha P_3 \otimes P_2 \in \operatorname{Pos}\left(\mathcal{X}_3 \otimes \mathcal{Y}_3 \otimes \mathcal{X}_2 \otimes \mathcal{Y}_2\right).$$

Based on the above equations we compute:

$$\begin{aligned} T_{\mathcal{X}_3 \otimes \mathcal{X}_2}(X_\alpha) &= \left(\frac{4}{3}R_3 + \frac{2}{3}S_3\right) \otimes \left(\frac{3}{2}R_2 + \frac{1}{2}S_2\right) + \alpha \left(-\frac{1}{3}R_3 + \frac{1}{3}S_3\right) \otimes \left(-\frac{1}{2}R_2 + \frac{1}{2}S_2\right) \\ &= \frac{12+\alpha}{6} R_3 \otimes R_2 + \frac{4-\alpha}{6} R_3 \otimes S_2 + \frac{6-\alpha}{6} S_3 \otimes R_2 + \frac{2+\alpha}{6} S_3 \otimes S_2. \end{aligned}$$

Provided that $\alpha \leq 4$, we therefore have that $X_\alpha \in \operatorname{PPT}\left(\mathcal{X}_3 \otimes \mathcal{X}_2 : \mathcal{Y}_3 \otimes \mathcal{Y}_2\right)$.

On the other hand, we have that

$$X_\alpha \notin \operatorname{Sep}\left(\mathcal{X}_3 \otimes \mathcal{X}_2 : \mathcal{Y}_3 \otimes \mathcal{Y}_2\right)$$

for every choice of $\alpha > 0$, as we will now show. Define $\Psi \in \mathrm{T}\left(\mathcal{X}_2 \otimes \mathcal{Y}_2, \mathcal{X}_3 \otimes \mathcal{Y}_3\right)$ to be the unique mapping for which $J(\Psi) = X_\alpha$. Using the identity

$$\Psi(Y) = \operatorname{Tr}_{\mathcal{X}_2 \otimes \mathcal{Y}_2}\left[J(\Psi)\left(\mathbb{1} \otimes Y^{\mathrm{T}}\right)\right]$$

we see that $\Psi(P_2) = \alpha P_3$. So, for $\alpha > 0$ we have that Ψ increases min-rank and is therefore not a separable mapping. Thus, it is not the case that X_α is separable.

18.2.2 Unextendible product bases

The second example is based on the notion of an *unextendible product basis*. Although the construction works for any choice of an unextendible product basis, we will just consider one example. Let $\mathcal{X} = \mathbb{C}^{\mathbb{Z}_3}$ and $\mathcal{Y} = \mathbb{C}^{\mathbb{Z}_3}$, and consider the following 5 unit vectors in $\mathcal{X} \otimes \mathcal{Y}$:

$$\begin{aligned} u_1 &= |0\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ u_2 &= |2\rangle \otimes \left(\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right) \\ u_3 &= \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes |2\rangle \\ u_4 &= \left(\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right) \otimes |0\rangle \\ u_5 &= \left(\frac{|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}\right) \otimes \left(\frac{|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}\right) \end{aligned}$$

There are three relevant facts about this set for the purpose of our discussion:

1. The set $\{u_1, \ldots, u_5\}$ is an orthonormal set.
2. Each u_i is a product vector, meaning $u_i = x_i \otimes y_i$ for some choice of $x_1, \ldots, x_5 \in \mathcal{X}$ and $y_1, \ldots, y_5 \in \mathcal{Y}$.
3. It is impossible to find a sixth non-zero product vector $v \otimes w \in \mathcal{X} \otimes \mathcal{Y}$ that is orthogonal to $u_1, \ldots, u_5$.

To verify the third property, note that in order for a product vector $v \otimes w$ to be orthogonal to any u_i, it must be that $\langle v, x_i \rangle = 0$ or $\langle w, y_i \rangle = 0$. In order to have $\langle v \otimes w, u_i \rangle$ for $i = 1, \ldots, 5$ we must therefore have $\langle v, x_i \rangle = 0$ for at least three distinct choices of i or $\langle w, y_i \rangle = 0$ for at least three distinct choices of i. However, for any three distinct choices of indices $i, j, k \in \{1, \ldots, 5\}$ we have $\operatorname{span}\{x_i, x_j, x_k\} = \mathcal{X}$ and $\operatorname{span}\{y_i, y_j, y_k\} = \mathcal{Y}$, which implies that either $v = 0$ or $w = 0$, and therefore $v \otimes w = 0$.

Now, define a projection operator $P \in \operatorname{Pos}(\mathcal{X} \otimes \mathcal{Y})$ as

$$P = \mathbb{1}_{\mathcal{X} \otimes \mathcal{Y}} - \sum_{i=1}^{5} u_i u_i^*.$$

Let us first note that $P \in \operatorname{PPT}(\mathcal{X} : \mathcal{Y})$. For each $i = 1, \ldots, 5$ we have

$$T_{\mathcal{X}}(u_i u_i^*) = (x_i x_i^*)^{\mathsf{T}} \otimes y_i y_i^* = x_i x_i^* \otimes y_i y_i^* = u_i u_i^*.$$

The second equality follows from the fact that each x_i has only real coefficients, so $x_i = \overline{x_i}$. Thus,

$$T_{\mathcal{X}}(P) = T_{\mathcal{X}}(\mathbb{1}_{\mathcal{X} \otimes \mathcal{Y}}) - \sum_{i=1}^{5} T_{\mathcal{X}}(u_i u_i^*) = \mathbb{1}_{\mathcal{X} \otimes \mathcal{Y}} - \sum_{i=1}^{5} u_i u_i^* = P \in \operatorname{Pos}(\mathcal{X} \otimes \mathcal{Y}),$$

as claimed.

Now let us assume toward contradiction that P is separable. This implies that it is possible to write

$$P = \sum_{j=1}^{m} v_j v_j^* \otimes w_j w_j^*$$

for some choice of $v_1, \ldots, v_m \in \mathcal{X}$ and $w_1, \ldots, w_m \in \mathcal{Y}$. For each $i = 1, \ldots, 5$ we have

$$0 = u_i^* P u_i = \sum_{j=1}^{m} u_i^* (v_j v_j^* \otimes w_j w_j^*) u_i.$$

Therefore, for each $j = 1, \ldots, m$ we have $\langle v_j \otimes w_j, u_i \rangle = 0$ for $i = 1, \ldots, 5$. This implies that $v_1 \otimes w_1 = \cdots = v_m \otimes w_m = 0$, and thus $P = 0$, establishing a contradiction. Consequently P is not separable.

18.3 PPT states and distillation

The last part of this lecture concerns the relationship between the partial transpose and entanglement distillation. Our goal will be to prove that PPT states cannot be distilled, meaning that the distillable entanglement is zero.

Let us begin the discussion with some further properties of PPT states that will be needed. First we will observe that separable mappings respect the positivity of the partial transpose.

Theorem 18.1. *Suppose $P \in \mathrm{PPT}(\mathcal{X}_A : \mathcal{X}_B)$ and $\Phi \in \mathrm{SepT}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$ is a separable mapping. It holds that $\Phi(P) \in \mathrm{PPT}(\mathcal{Y}_A : \mathcal{Y}_B)$.*

Proof. Consider any choice of operators $A \in \mathrm{L}(\mathcal{X}_A, \mathcal{Y}_A)$ and $B \in \mathrm{L}(\mathcal{X}_B, \mathcal{Y}_B)$. Given that $P \in \mathrm{PPT}(\mathcal{X}_A : \mathcal{X}_B)$, we have

$$T_{\mathcal{X}_A}(P) \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$$

and therefore

$$(\mathbb{1}_{\mathcal{X}_A} \otimes B) T_{\mathcal{X}_A}(P) (\mathbb{1}_{\mathcal{X}_A} \otimes B^*) \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{Y}_B).$$

The partial transpose on $\mathcal{X}_A$ commutes with the conjugation by B, and therefore

$$T_{\mathcal{X}_A}\left((\mathbb{1}_{\mathcal{X}_A} \otimes B) P (\mathbb{1}_{\mathcal{X}_A} \otimes B^*)\right) \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{Y}_B).$$

This implies that

$$T\left(T_{\mathcal{X}_A}\left((\mathbb{1} \otimes B) P (\mathbb{1} \otimes B^*)\right)\right) = T_{\mathcal{Y}_B}\left((\mathbb{1} \otimes B) P (\mathbb{1} \otimes B^*)\right) \in \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{Y}_B)$$

as remarked in the first section of the lecture. Using the fact that conjugation by A commutes with the partial transpose on $\mathcal{Y}_B$, we have that

$$(A \otimes \mathbb{1}_{\mathcal{Y}_B}) T_{\mathcal{Y}_B}\left((\mathbb{1} \otimes B) P (\mathbb{1} \otimes B^*)\right) (A^* \otimes \mathbb{1}_{\mathcal{Y}_B}) = T_{\mathcal{Y}_B}\left((A \otimes B) P (A^* \otimes B^*)\right) \in \mathrm{Pos}(\mathcal{Y}_A \otimes \mathcal{Y}_B).$$

We have therefore proved that $(A \otimes B) P (A^* \otimes B^*) \in \mathrm{PPT}(\mathcal{Y}_A : \mathcal{Y}_B)$.

Now, for $\Phi \in \mathrm{SepT}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$, we have that $\Phi(P) \in \mathrm{PPT}(\mathcal{Y}_A : \mathcal{Y}_B)$ by the above observation together with the fact that $\mathrm{PPT}(\mathcal{Y}_A : \mathcal{Y}_B)$ is a convex cone. □

Next, let us note that PPT states cannot have a large inner product with a maximally entangled states.

Lemma 18.2. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $n = \min\{\dim(\mathcal{X}), \dim(\mathcal{Y})\}$. For any PPT density operator*

$$\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y}) \cap \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$$

we have $M(\rho) \leq 1/n$.

Proof. Let us assume, without loss of generality, that $\mathcal{Y} = \mathbb{C}^{\mathbb{Z}_n}$ and $\dim(\mathcal{X}) \geq n$. Every maximally entangled state on $\mathcal{X} \otimes \mathcal{Y}$ may therefore be written

$$(U \otimes \mathbb{1}_{\mathcal{Y}}) P_n (U \otimes \mathbb{1}_{\mathcal{Y}})^*$$

for $U \in \mathrm{U}(\mathcal{Y}, \mathcal{X})$ being a linear isometry, and where P_n is as defined in (18.1). We have that

$$\langle (U \otimes \mathbb{1}_{\mathcal{Y}}) P_n (U \otimes \mathbb{1}_{\mathcal{Y}})^*, \rho \rangle = \langle P_n, (U \otimes \mathbb{1}_{\mathcal{Y}})^* \rho (U \otimes \mathbb{1}_{\mathcal{Y}}) \rangle,$$

and that

$$(U \otimes \mathbb{1}_{\mathcal{Y}})^* \rho (U \otimes \mathbb{1}_{\mathcal{Y}}) \in \mathrm{PPT}(\mathcal{Y} : \mathcal{Y})$$

is a PPT operator with trace at most 1. To prove the lemma it therefore suffices to prove that

$$\langle P_n, \xi \rangle \leq \frac{1}{n}$$

for every $\xi \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{Y}) \cap \mathrm{PPT}(\mathcal{Y} : \mathcal{Y})$.

The partial transpose is its own adjoint and inverse, which implies that

$$\langle (T \otimes \mathbb{1})(A), (T \otimes \mathbb{1})(B) \rangle = \langle A, B \rangle$$

for any choice of operators $A, B \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{Y})$. It is also clear that the partial transpose preserves trace, which implies that $(T \otimes \mathbb{1})(\xi) \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{Y})$ for every $\xi \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{Y}) \cap \mathrm{PPT}(\mathcal{Y} : \mathcal{Y})$. Consequently we have

$$\langle P_n, \xi \rangle = |\langle P_n, \xi \rangle| = |\langle (T \otimes \mathbb{1})(P_n), (T \otimes \mathbb{1})(\xi) \rangle| = \frac{1}{n} |\langle W_n, (T \otimes \mathbb{1})(\xi) \rangle| \leq \frac{1}{n} \|(T \otimes \mathbb{1})(\xi)\|_1 = \frac{1}{n},$$

where the inequality follows from the fact that W_n is unitary and the last equality follows from the fact that $(T \otimes \mathbb{1})(\xi)$ is a density operator. □

Finally we are ready for the main result of the section, which states that PPT density operators have no distillable entanglement.

Theorem 18.3. *Let $\mathcal{X}_A$ and $\mathcal{X}_B$ be complex Euclidean spaces and let $\rho \in \mathrm{D}(\mathcal{X}_A \otimes \mathcal{X}_B) \cap \mathrm{PPT}(\mathcal{X}_A : \mathcal{X}_B)$. It holds that $E_d(\rho) = 0$.*

Proof. Let $\mathcal{Y}_A = \mathbb{C}^{\{0,1\}}$ and $\mathcal{Y}_B = \mathbb{C}^{\{0,1\}}$ be complex Euclidean spaces each corresponding to a single qubit, as in the definition of distillable entanglement, and let $\tau \in \mathrm{D}(\mathcal{Y}_A \otimes \mathcal{Y}_B)$ be the density operator corresponding to a perfect e-bit.

Let $\alpha > 0$ and let

$$\Phi_n \in \mathrm{LOCC}\left(\mathcal{X}_A^{\otimes n}, \mathcal{Y}_A^{\otimes \lfloor \alpha n \rfloor} : \mathcal{X}_B^{\otimes n}, \mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}\right)$$

be an LOCC channel for each $n \geq 1$. This implies that Φ_n is a separable channel. Now, if $\rho \in \mathrm{PPT}(\mathcal{X}_A : \mathcal{X}_B)$ then $\rho^{\otimes n} \in \mathrm{PPT}\left(\mathcal{X}_A^{\otimes n} : \mathcal{X}_B^{\otimes n}\right)$, and therefore

$$\Phi_n(\rho^{\otimes n}) \in \mathrm{D}\left(\mathcal{Y}_A^{\otimes \lfloor \alpha n \rfloor} \otimes \mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}\right) \cap \mathrm{PPT}\left(\mathcal{Y}_A^{\otimes \lfloor \alpha n \rfloor} : \mathcal{Y}_B^{\otimes \lfloor \alpha n \rfloor}\right).$$

By Lemma 18.2 we therefore have that

$$\left\langle \tau^{\otimes \lfloor \alpha n \rfloor}, \Phi_n(\rho^{\otimes n}) \right\rangle \leq 2^{-\lfloor \alpha n \rfloor}.$$

As we have assumed $\alpha > 0$, this implies that

$$\lim_{n \to \infty} \mathrm{F}\left(\Phi_n(\rho^{\otimes n}), \tau^{\otimes \lfloor \alpha n \rfloor}\right) = 0.$$

It follows that $E_d(\rho) < \alpha$, and from this we conclude that $E_d(\rho) = 0$. □

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

Lecture 19: LOCC and separable measurements

In this lecture we will discuss measurements that can be collectively performed by two parties by means of local quantum operations and classical communication. Much of this discussion could be generalized to measurements implemented by more than two parties—but, as we have been doing for the last several lectures, we will restrict our attention to the bipartite case.

19.1 Definitions and simple observations

Informally speaking, an LOCC measurement is one that can be implemented by two (or more) parties using only local quantum operations and classical communication. We must, however, choose a more precise mathematical definition if we are to prove mathematical statements concerning these objects.

There are many ways one could formally define LOCC measurements; for simplicity we will choose a definition that makes use of the definition of LOCC channels we have already studied. Specifically, we will say that a measurement

$$\mu : \Gamma \to \mathrm{Pos}\left(\mathcal{X}_A \otimes \mathcal{X}_B\right)$$

on a bipartite system having associated complex Euclidean spaces $\mathcal{X}_A$ and $\mathcal{X}_B$ is an *LOCC measurement* if there exists an LOCC channel

$$\Phi \in \mathrm{LOCC}\left(\mathcal{X}_A, \mathbb{C}^\Gamma : \mathcal{X}_B, \mathbb{C}\right)$$

such that

$$\langle E_{a,a}, \Phi(\rho)\rangle = \langle \mu(a), \rho\rangle \tag{19.1}$$

for every $a \in \Gamma$ and $\rho \in \mathrm{D}\left(\mathcal{X}_A \otimes \mathcal{X}_B\right)$. An equivalent condition to (19.1) holding for all $\rho \in \mathrm{D}\left(\mathcal{X}_A \otimes \mathcal{X}_B\right)$ is that

$$\mu(a) = \Phi^*(E_{a,a}).$$

The interpretation of this definition is as follows. Alice and Bob implement the measurement μ by first performing the LOCC channel Φ, which leaves Alice with a register whose classical states coincide with the set Γ of possible measurement outcomes, while Bob is left with nothing (meaning a trivial register, having a single state, whose corresponding complex Euclidean space is $\mathbb{C}$). Alice then measures her register with respect to the standard basis of $\mathbb{C}^\Gamma$ to obtain the measurement outcome. Of course there is nothing special about letting Alice perform the measurement rather than Bob; we are just making an arbitrary choice for the sake of arriving at a definition, which would be equivalent to one allowing Bob to make the final measurement rather than Alice.

As we did when discussing channels, we will also consider a relaxation of LOCC measurements that is often much easier to work with. A measurement

$$\mu : \Gamma \to \mathrm{Pos}\left(\mathcal{X}_A \otimes \mathcal{X}_B\right)$$

is said to be *separable* if, in addition to satisfying the usual requirements of being a measurement, it holds that $\mu(a) \in \text{Sep}(\mathcal{X}_A : \mathcal{X}_B)$ for each $a \in \Gamma$.

Proposition 19.1. *Let $\mathcal{X}_A$ and $\mathcal{X}_B$ be complex Euclidean spaces and let*

$$\mu : \Gamma \to \text{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$$

be an LOCC measurement. It holds that μ is a separable measurement.

Proof. Let $\Phi \in \text{LOCC}(\mathcal{X}_A, \mathcal{Y}_A : \mathcal{X}_B, \mathcal{Y}_B)$ be an LOCC channel for which

$$\mu(a) = \Phi^*(E_{a,a})$$

for each $a \in \Gamma$. As Φ is an LOCC channel, it is necessarily separable, and therefore so too is Φ^*. (This may be verified by considering the fact that Kraus operators for Φ^* may be obtained by taking adjoints of the Kraus operators of Φ.) As $E_{a,a} = E_{a,a} \otimes 1$ is an element of $\text{Sep}(\mathbb{C}^\Gamma : \mathbb{C})$ for every $a \in \Gamma$, we have that $\mu(a) = \Phi^*(E_{a,a})$ is separable for each $a \in \Gamma$ as required. □

It is the case that there are separable measurements that are not LOCC measurements—we will see such an example (albeit without a proof) later in the lecture. However, separable measurements can be simulated by LOCC measurement in a probabilistic sense: the LOCC measurement that simulates the separable measurement might fail, but it succeeds with nonzero probability, and if it succeeds it generates the same output statistics as the original separable measurement. This is implied by the following theorem.

Theorem 19.2. *Suppose $\mu : \Gamma \to \text{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$ is a separable measurement. There exists an LOCC measurement*

$$\nu : \Gamma \cup \{\text{fail}\} \to \text{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$$

with the property that $\nu(a) = \gamma\mu(a)$, for each $a \in \Gamma$, for some real number $\gamma > 0$.

Proof. A general separable measurement $\mu : \Gamma \to \text{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$ must have the form

$$\mu(a) = \sum_{b \in \Sigma} P_{a,b} \otimes Q_{a,b}$$

for some finite set Σ and two collections

$$\{P_{a,b} : a \in \Gamma,\, b \in \Sigma\} \subset \text{Pos}(\mathcal{X}_A),$$
$$\{Q_{a,b} : a \in \Gamma,\, b \in \Sigma\} \subset \text{Pos}(\mathcal{X}_B).$$

Choose sufficiently small positive real numbers $\alpha, \beta > 0$ such that

$$\alpha \sum_{a,b} P_{a,b} \leq \mathbb{1}_{\mathcal{X}_A} \qquad \text{and} \qquad \beta \sum_{a,b} Q_{a,b} \leq \mathbb{1}_{\mathcal{X}_B},$$

and define a measurement $\nu_A : (\Gamma \times \Sigma) \cup \{\text{fail}\} \to \text{Pos}(\mathcal{X}_A)$ as

$$\nu_A(a,b) = \alpha P_{a,b} \qquad \text{and} \qquad \nu(\text{fail}) = \mathbb{1}_{\mathcal{X}_A} - \alpha \sum_{a,b} P_{a,b},$$

and a measurement $\nu_B : (\Gamma \times \Sigma) \cup \{\text{fail}\} \to \text{Pos}(\mathcal{X}_B)$ as

$$\nu_B(a,b) = \beta Q_{a,b} \qquad \text{and} \qquad \nu(\text{fail}) = \mathbb{1}_{\mathcal{X}_B} - \beta \sum_{a,b} Q_{a,b}.$$

Now, consider the situation in which Alice performs ν_A and Bob independently performs ν_B. Let us suppose that Bob sends Alice his measurement outcome, and Alice compares this result with her own to determine the final result. If Bob's measurement outcome is "fail," or if Alice's measurement outcome is not equal to Bob's, Alice outputs "fail." If, on the other hand, Alice and Bob obtain the same measurement outcome $(a, b) \in \Gamma \times \Sigma$, Alice outputs a. The measurement ν that they implement is described by

$$\nu(a) = \sum_{b \in \Sigma} \nu_A(a, b) \otimes \nu_B(a, b) = \alpha\beta \sum_{b \in \Sigma} P_{a,b} \otimes Q_{a,b} = \alpha\beta\mu(a)$$

and

$$\nu(\text{fail}) = \mathbb{1}_{\mathcal{X}_A} \otimes \mathbb{1}_{\mathcal{X}_B} - \alpha\beta \sum_{a \in \Gamma} \mu(a).$$

Taking $\gamma = \alpha\beta$ completes the proof. □

It is the case that certain measurements are not separable, and therefore cannot be performed by means of local operations and classical communication. For instance, no LOCC measurement can perfectly distinguish any fixed entangled pure state from all orthogonal states, given that one of the required measurement operators would then necessarily be non-separable. This fact trivially implies that Alice and Bob cannot perform a measurement with respect to any orthonormal basis

$$\{u_a : a \in \Gamma\} \subset \mathcal{X}_A \otimes \mathcal{X}_B$$

of $\mathcal{X}_A \otimes \mathcal{X}_B$ unless that basis consists entirely of product vectors.

Another example along these lines is that Alice and Bob cannot perfectly distinguish symmetric and antisymmetric states of $\mathbb{C}^{\mathbb{Z}_n} \otimes \mathbb{C}^{\mathbb{Z}_n}$ by means of an LOCC measurement. Such a measurement is described by the two-outcome projective measurement $\{R_n, S_n\}$, where

$$R_n = \frac{1}{2}(\mathbb{1} - W_n) \qquad \text{and} \qquad S_n = \frac{1}{2}(\mathbb{1} + W_n),$$

for W_n denoting the swap operator (as was discussed in the previous lecture). The fact that R_n is not separable follows from the fact that it is not PPT:

$$(T \otimes \mathbb{1})(R_n) = -\frac{n-1}{2} P_n + \frac{1}{2} Q_n,$$

where P_n and Q_n are as defined in the previous lecture.

19.2 Impossibility of LOCC distinguishing some sets of states

When we force measurements to have non-separable measurement operators, it is clear that the measurements cannot be performed using local operations and classical communication. Sometimes, however, we may be interested in a task that potentially allows for many different implementations as a measurement.

One interesting scenario along these lines is the task of distinguishing certain sets of pure states. Specifically, suppose that $\mathcal{X}_A$ and $\mathcal{X}_B$ are complex Euclidean spaces and $\{u_1, \ldots, u_k\} \subset \mathcal{X}_A \otimes \mathcal{X}_B$ is a set of orthogonal unit vectors. Alice and Bob are given a pure state u_i for $i \in \{1, \ldots, k\}$ and their goal is to determine the value of i. It is assumed that they have complete knowledge of the set $\{u_1, \ldots, u_k\}$. Under the assumption that k is smaller than the total dimension of the space $\mathcal{X}_A \otimes \mathcal{X}_B$, there will be many measurements $\mu : \{1, \ldots, k\} \to \text{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$ that correctly distinguish the elements of the set $\{u_1, \ldots, u_k\}$, and the general question we consider is whether there is at least one such measurement that is LOCC.

19.2.1 Sets of maximally entangled states

Let us start with a simple general result that proves that sufficiently many maximally entangled pure states are hard to distinguish in the sense described. Specifically, assume that $\mathcal{X}_A$ and $\mathcal{X}_B$ both have dimension n, and consider a collection $U_1, \ldots, U_k \in \mathrm{U}(\mathcal{X}_B, \mathcal{X}_A)$ of pairwise orthogonal unitary operators, meaning that $\langle U_i, U_j \rangle = 0$ for $i \neq j$. The set

$$\left\{ \frac{1}{\sqrt{n}} \operatorname{vec}(U_1), \ldots, \frac{1}{\sqrt{n}} \operatorname{vec}(U_k) \right\}$$

therefore represents a set of maximally entangled pure states. We will show that such a set cannot be perfectly distinguished by a separable measurement, under the assumption that $k \geq n+1$.

Suppose $\mu : \{1, \ldots, k\} \to \mathrm{Pos}(\mathcal{X}_A \otimes \mathcal{X}_B)$ is a separable measurement, so that

$$\mu(j) = \sum_{i=1}^{m} P_{j,i} \otimes Q_{j,i}$$

for each $j = 1, \ldots, k$, for $\{P_{j,i}\} \subset \mathrm{Pos}(\mathcal{X}_A)$ and $\{Q_{j,i}\} \subset \mathrm{Pos}(\mathcal{X}_B)$ being collections of positive semidefinite operators. It follows that

$$\begin{aligned} \langle \mu(j), \operatorname{vec}(U_j) \operatorname{vec}(U_j)^* \rangle &= \sum_{i=1}^{m} \operatorname{Tr}\left(U_j^* P_{j,i} U_j Q_{j,i}^{\mathsf{T}} \right) \\ &\leq \sum_{i=1}^{m} \operatorname{Tr}\left(U_j^* P_{j,i} U_j \right) \operatorname{Tr}\left(Q_{j,i}^{\mathsf{T}} \right) = \sum_{i=1}^{m} \operatorname{Tr}\left(P_{j,i} \right) \operatorname{Tr}\left(Q_{j,i} \right) = \sum_{i=1}^{m} \operatorname{Tr}\left(P_{j,i} \otimes Q_{j,i} \right) = \operatorname{Tr}(\mu(j)) \end{aligned}$$

for each j (where the inequality holds because $\operatorname{Tr}(AB) \leq \operatorname{Tr}(A)\operatorname{Tr}(B)$ for $A, B \geq 0$). Thus, it holds that

$$\frac{1}{k} \sum_{j=1}^{k} \left\langle \mu(j), \frac{1}{n} \operatorname{vec}(U_j) \operatorname{vec}(U_j)^* \right\rangle \leq \frac{1}{nk} \sum_{j=1}^{k} \operatorname{Tr}(\mu(j)) = \frac{n}{k},$$

which implies that the correctness probability of any separable measurement to distinguish the k maximally entangled states is smaller than 1 for $k \geq n+1$.

Naturally, as any measurement implementable by an LOCC protocol is separable, it follows that no LOCC protocol can distinguish more than n maximally entangled states in $\mathcal{X}_A \otimes \mathcal{X}_B$ in the case that $\dim(\mathcal{X}_A) = \dim(\mathcal{X}_B) = n$.

19.2.2 Indistinguishable sets of product states

It is reasonable to hypothesize that large sets of maximally entangled states are not LOCC distinguishable because they are highly entangled. However, it turns out that entanglement is not an essential feature for this phenomenon. In fact, there exist orthogonal collections of *product states* that are not perfectly distinguishable by LOCC measurements.

One example is the following orthonormal basis of $\mathbb{C}^{\mathbb{Z}_3} \otimes \mathbb{C}^{\mathbb{Z}_3}$:

$$\begin{array}{lllll} |1\rangle \otimes |1\rangle & |0\rangle \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) & |2\rangle \otimes \left(\frac{|1\rangle + |2\rangle}{\sqrt{2}}\right) & \left(\frac{|1\rangle + |2\rangle}{\sqrt{2}}\right) \otimes |0\rangle & \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |2\rangle \\ & |0\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & |2\rangle \otimes \left(\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right) & \left(\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right) \otimes |0\rangle & \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes |2\rangle \end{array}$$

A measurement with respect to this basis is an example of a measurement that is separable but not LOCC.

The proof that the above set is not perfectly LOCC distinguishable is technical, and so a reference will have to suffice in place of a proof:

> C. H. Bennett, D. DiVincenzo, C. Fuchs, T. Mor, E. Rains, P. Shor, J. Smolin, and W. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070–1091, 1999.

Another family of examples of product states (but not product bases) that cannot be distinguished by LOCC measurements comes from an unextendible product set. For instance, the set discussed in the previous lecture cannot be distinguished by an LOCC measurement:

$$|0\rangle \otimes \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \qquad \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes |2\rangle \qquad \left(\tfrac{|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}\right) \otimes \left(\tfrac{|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}\right)$$

$$|2\rangle \otimes \left(\tfrac{|1\rangle - |2\rangle}{\sqrt{2}}\right) \qquad \left(\tfrac{|1\rangle - |2\rangle}{\sqrt{2}}\right) \otimes |0\rangle$$

This fact is proved in the following paper:

> D. DiVincenzo, T. Mor, P. Shor, J. Smolin and B. Terhal. Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement. *Communications in Mathematical Physics*, 238(3): 379–410, 2003.

19.3 Any two orthogonal pure states can be distinguished

Finally, we will prove an interesting and fundamental result in this area, which is that any two orthogonal pure states can always be distinguished by an LOCC measurement.

In order to prove this fact, we need a theorem known as the Toeplitz–Hausdorff theorem, which concerns the *numerical range* of an operator. The numerical range of an operator $A \in \mathrm{L}(\mathcal{X})$ is the set $\mathcal{N}(A) \subset \mathbb{C}$ defined as follows:

$$\mathcal{N}(A) = \{u^* A u \,:\, u \in \mathcal{X},\, \|u\| = 1\}.$$

This set is also sometimes called the *field of values* of A. It is not hard to prove that the numerical range of a normal operator is simply the convex hull of its eigenvalues. For non-normal operators, however, this is not the case—but the numerical range will nevertheless be a compact and convex set that includes the eigenvalues. The fact that the numerical range is compact and convex is what is stated by the Toeplitz-Hausdorff theorem.

Theorem 19.3 (The Toeplitz-Hausdorff theorem)**.** *For any complex Euclidean space $\mathcal{X}$ and any operator $A \in \mathrm{L}(\mathcal{X})$, the set $\mathcal{N}(A)$ is compact and convex.*

Proof. The proof of compactness is straightforward. Specifically, the function $f : \mathcal{X} \to \mathbb{C}$ defined by $f(u) = u^* A u$ is continuous, and the unit sphere $\mathcal{S}(\mathcal{X})$ is compact. Continuous functions map compact sets to compact sets, implying that $\mathcal{N}(A) = f(\mathcal{S}(\mathcal{X}))$ is compact.

The proof of convexity is the more difficult part of the proof. Let us fix some arbitrary choice of $\alpha, \beta \in \mathcal{N}(A)$ and $p \in [0,1]$. It is our goal to prove that $p\alpha + (1-p)\beta \in \mathcal{N}(A)$. We will assume that $\alpha \neq \beta$, as the assertion is trivial in case $\alpha = \beta$.

By the definition of the numerical range, we may choose unit vectors $u, v \in \mathcal{X}$ such that $u^* A u = \alpha$ and $v^* A v = \beta$. It follows from the fact that $\alpha \neq \beta$ that the vectors u and v are linearly independent.

Next, define

$$B = \frac{-\beta}{\alpha - \beta}\mathbb{1}_{\mathcal{X}} + \frac{1}{\alpha - \beta}A$$

so that $u^*Bu = 1$ and $v^*Bv = 0$. Let

$$X = \frac{1}{2}(B + B^*) \quad \text{and} \quad Y = \frac{1}{2i}(B - B^*).$$

It holds that $B = X + iY$, and both X and Y are Hermitian. It therefore follows that

$$\begin{aligned} u^*Xu &= 1, \qquad & v^*Xv &= 0, \\ u^*Yu &= 0, \qquad & v^*Yv &= 0. \end{aligned}$$

Without loss of generality we may also assume u^*Yv is purely imaginary (i.e., has real part equal to 0), for otherwise v may be replaced by $e^{i\theta}v$ for an appropriate choice of θ without changing any of the previously observed properties.

As u and v are linearly independent, we have that $tu + (1-t)v$ is a nonzero vector for every choice of t. Thus, for each $t \in [0,1]$ we may define

$$z(t) = \frac{tu + (1-t)v}{\|tu + (1-t)v\|},$$

which is of course a unit vector. Because $u^*Yu = v^*Yv = 0$ and u^*Yv is purely imaginary, we have $z(t)^*Yz(t) = 0$ for every t. Thus

$$z(t)^*Bz(t) = z(t)^*Xz(t) = \frac{t^2 + 2t(1-t)\Re(v^*Xu)}{\|tu + (1-t)v\|}.$$

This is a continuous real-valued function mapping 0 to 0 and 1 to 1. Consequently there must exist some choice of $t \in [0,1]$ such that $z(t)^*Bz(t) = p$. Let $w = z(t)$ for such a value of t, so that $w^*Bw = p$. We have that w is a unit vector, and

$$w^*Aw = (\alpha - \beta)\left(\frac{\beta}{\alpha - \beta} + w^*Bw\right) = \beta + p(\alpha - \beta) = p\alpha + (1-p)\beta.$$

Thus we have shown that $p\alpha + (1-p)\beta \in \mathcal{N}(A)$ as required. □

Corollary 19.4. *For any complex Euclidean space $\mathcal{X}$ and any operator $A \in \mathrm{L}(\mathcal{X})$ satisfying $\mathrm{Tr}(A) = 0$, there exists an orthonormal basis $\{x_1, \ldots, x_n\}$ of $\mathcal{X}$ for which $x_i^*Ax_i = 0$ for $i = 1, \ldots, n$.*

Proof. The proof is by induction on $n = \dim(\mathcal{X})$, and the base case $n = 1$ is trivial.

Suppose that $n \geq 2$. It is clear that $\lambda_1(A), \ldots, \lambda_n(A) \in \mathcal{N}(A)$, and thus $0 \in \mathcal{N}(A)$ because

$$0 = \frac{1}{n}\mathrm{Tr}(A) = \frac{1}{n}\sum_{i=1}^{n}\lambda_i(A),$$

which is a convex combination of elements of $\mathcal{N}(A)$. Therefore there exists a unit vector $u \in \mathcal{X}$ such that $u^*Au = 0$.

Now, let $\mathcal{Y} \subseteq \mathcal{X}$ be the orthogonal complement of u in $\mathcal{X}$, and let $\Pi_{\mathcal{Y}} = \mathbb{1}_{\mathcal{X}} - uu^*$ be the orthogonal projection onto $\mathcal{Y}$. It holds that

$$\mathrm{Tr}(\Pi_{\mathcal{Y}}A\Pi_{\mathcal{Y}}) = \mathrm{Tr}(A) - u^*Au = 0.$$

Moreover, because $\operatorname{im}(\Pi_{\mathcal{Y}} A \Pi_{\mathcal{Y}}) \subseteq \mathcal{Y}$, we may regard $\Pi_{\mathcal{Y}} A \Pi_{\mathcal{Y}}$ as an element of $\mathrm{L}(\mathcal{Y})$. By the induction hypothesis, we therefore have that there exists an orthonormal basis $\{v_1, \ldots, v_{n-1}\}$ of $\mathcal{Y}$ such that $v_i^* \Pi_{\mathcal{Y}} A \Pi_{\mathcal{Y}} v_i = 0$ for $i = 1, \ldots, n-1$. It follows that $\{u, v_1, \ldots, v_{n-1}\}$ is an orthonormal basis of $\mathcal{X}$ with the properties required by the statement of the corollary. □

Now we are ready to return to the problem of distinguishing orthogonal states. Suppose that

$$x, y \in \mathcal{X}_A \otimes \mathcal{X}_B$$

are orthogonal unit vectors. We wish to show that there exists an LOCC measurement that correctly distinguishes between x and y. Let $X, Y \in \mathrm{L}(\mathcal{X}_B, \mathcal{X}_A)$ be operators satisfying $x = \operatorname{vec}(X)$ and $y = \operatorname{vec}(Y)$, so that the orthogonality of x and y is equivalent to $\operatorname{Tr}(X^* Y) = 0$. By Corollary 19.4, we have that there exists an orthonormal basis $\{u_1, \ldots, u_n\}$ of $\mathcal{X}_B$ with the property that $u_i^* X^* Y u_i = 0$ for $i = 1, \ldots, n$.

Now, suppose that Bob measures his part of either xx^* or yy^* with respect to the orthonormal basis $\{\overline{u_1}, \ldots, \overline{u_n}\}$ of $\mathcal{X}_B$ and transmits the result of the measurement to Alice. Conditioned on Bob obtaining the outcome i, the (unnormalized) state of Alice's system becomes

$$(\mathbb{1}_{\mathcal{X}_A} \otimes u_i^{\mathsf{T}}) \operatorname{vec}(X) \operatorname{vec}(X)^* (\mathbb{1}_{\mathcal{X}_A} \otimes \overline{u_i}) = X u_i u_i^* X^*$$

in case the original state was xx^*, and $Y u_i u_i^* Y^*$ in case the original state was yy^*.

A necessary and sufficient condition for Alice to be able to correctly distinguish these two states, given knowledge of i, is that

$$\langle X u_i u_i^* X^*, Y u_i u_i^* Y^* \rangle = 0.$$

This condition is equivalent to $u_i^* X^* Y u_i = 0$ for each $i = 1, \ldots, n$. The basis $\{u_1, \ldots, u_n\}$ was chosen to satisfy this condition, which implies that Alice can correctly distinguish the two possibilities without error.

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

Lecture 20: Channel distinguishability and the completely bounded trace norm

This lecture is primarily concerned with the *distinguishability* of quantum channels, along with a norm defined on mappings between operator spaces that is closely related to this problem. In particular, we will define and study a norm called the *completely bounded trace norm* that plays an analogous role for channel distinguishability that the ordinary trace norm plays for density operator distinguishability.

20.1 Distinguishing between quantum channels

Recall from Lecture 3 that the trace norm has a close relationship to the optimal probability of distinguishing two quantum states. In particular, for every choice of density operators $\rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})$ and a scalar $\lambda \in [0,1]$, it holds that

$$\max_{P_0,P_1} \left[\lambda \langle P_0, \rho_0 \rangle + (1-\lambda) \langle P_1, \rho_1 \rangle\right] = \frac{1}{2} + \frac{1}{2} \left\| \lambda\rho_0 - (1-\lambda)\rho_1 \right\|_1,$$

where the maximum is over all $P_0, P_1 \in \mathrm{Pos}(\mathcal{X})$ satisfying $P_0 + P_1 = \mathbb{1}_{\mathcal{X}}$, i.e., $\{P_0, P_1\}$ representing a binary-valued measurement. In words, the optimal probability to distinguish (or correctly identify) the states ρ_0 and ρ_1, given with probabilities λ and $1-\lambda$, respectively, by means of a measurement is

$$\frac{1}{2} + \frac{1}{2} \left\| \lambda\rho_0 - (1-\lambda)\rho_1 \right\|_1.$$

One may consider a similar situation involving channels rather than density operators. Specifically, let us suppose that $\Phi_0, \Phi_1 \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ are channels, and that a bit $a \in \{0,1\}$ is chosen at random, such that

$$\Pr[a = 0] = \lambda \qquad \text{and} \qquad \Pr[a = 1] = 1 - \lambda.$$

A single evaluation of the channel Φ_a is made available, and the goal is to determine the value of a with maximal probability.

One approach to this problem is to choose $\xi \in \mathrm{D}(\mathcal{X})$ in order to maximize the quantity $\|\rho_0 - \rho_1\|_1$ for $\rho_0 = \Phi_0(\xi)$ and $\rho_1 = \Phi_1(\xi)$. If a register X is prepared so that its state is ξ, and X is input to the given channel Φ_a, then the output is a register Y that can be measured using an optimal measurement to distinguish the two possible outputs ρ_0 and ρ_1.

This, however, is not the most general approach. More generally, one may include an *auxiliary register* Z in the process—meaning that a pair of registers (X, Z) is prepared in some state $\xi \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Z})$, and the given channel Φ_a is applied to X. This results in a pair of registers (Y, Z) that will be in either of the states $\rho_0 = (\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(\xi)$ or $\rho_1 = (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(\xi)$, which may then be distinguished by a measurement on $\mathcal{Y} \otimes \mathcal{Z}$. Indeed, this more general approach can give a sometimes striking improvement in the probability to distinguish Φ_0 and Φ_1, as the following example illustrates.

Example 20.1. Let $\mathcal{X}$ be a complex Euclidean space and let $n = \dim(\mathcal{X})$. Define channels $\Phi_0, \Phi_1 \in \mathrm{T}(\mathcal{X})$ as follows:

$$\Phi_0(X) = \frac{1}{n+1}\left((\operatorname{Tr} X)\mathbb{1}_{\mathcal{X}} + X^{\mathsf{T}}\right),$$

$$\Phi_1(X) = \frac{1}{n-1}\left((\operatorname{Tr} X)\mathbb{1}_{\mathcal{X}} - X^{\mathsf{T}}\right).$$

Both Φ_0 and Φ_1 are indeed channels: the fact that they are trace-preserving can be checked directly, while complete positivity follows from a calculation of the Choi-Jamiołkowski representations of these mappings:

$$J(\Phi_0) = \frac{1}{n+1}\left(\mathbb{1}_{\mathcal{X}\otimes\mathcal{X}} + W\right) = \frac{2}{n+1}S,$$

$$J(\Phi_1) = \frac{1}{n-1}\left(\mathbb{1}_{\mathcal{X}\otimes\mathcal{X}} - W\right) = \frac{2}{n-1}R,$$

where $W \in \mathrm{L}(\mathcal{X}\otimes\mathcal{X})$ is the swap operator and $R, S \in \mathrm{L}(\mathcal{X}\otimes\mathcal{X})$ are the projections onto the symmetric and antisymmetric subspaces of $\mathcal{X}\otimes\mathcal{X}$, respectively.

Now, for any choice of a density operator $\xi \in \mathrm{D}(\mathcal{X})$ we have

$$\begin{aligned}\Phi_0(\xi) - \Phi_1(\xi) &= \left(\frac{1}{n+1} - \frac{1}{n-1}\right)\mathbb{1}_{\mathcal{X}} + \left(\frac{1}{n+1} + \frac{1}{n-1}\right)\xi^{\mathsf{T}} \\ &= -\frac{2}{n^2-1}\mathbb{1}_{\mathcal{X}} + \frac{2n}{n^2-1}\xi^{\mathsf{T}}.\end{aligned}$$

The trace norm of such an operator is maximized when ξ has rank 1, in which case the value of the trace norm is

$$\frac{2n-2}{n^2-1} + (n-1)\frac{2}{n^2-1} = \frac{4}{n+1}.$$

Consequently

$$\|\Phi_0(\xi) - \Phi_1(\xi)\|_1 \leq \frac{4}{n+1}$$

for all $\xi \in \mathrm{D}(\mathcal{X})$. For large n, this quantity is small, which is not surprising because both $\Phi_0(\xi)$ and $\Phi_1(\xi)$ are almost completely mixed for any choice of $\xi \in \mathrm{D}(\mathcal{X})$.

However, suppose that we prepare two registers $(\mathsf{X}_1, \mathsf{X}_2)$ in the maximally entangled state

$$\tau = \frac{1}{n}\operatorname{vec}(\mathbb{1}_{\mathcal{X}})\operatorname{vec}(\mathbb{1}_{\mathcal{X}})^* \in \mathrm{D}(\mathcal{X}\otimes\mathcal{X}).$$

We have

$$(\Phi_a \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\tau) = \frac{1}{n}J(\Phi_a)$$

for $a \in \{0,1\}$, and therefore

$$(\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\tau) = \frac{2}{n(n+1)}S \qquad \text{and} \qquad (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\tau) = \frac{2}{n(n-1)}R.$$

Because R and S are orthogonal, we have

$$\left\|(\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\tau) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\tau)\right\|_1 = 2,$$

meaning that the states $(\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\tau)$ and $(\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\tau)$, and therefore the channels Φ_0 and Φ_1, can be distinguished *perfectly*.

By applying Φ_0 or Φ_1 to part of a larger system, we have therefore completely eliminated the large error that was present when the limited approach of choosing $\xi \in \mathrm{D}(\mathcal{X})$ as an input to Φ_0 and Φ_1 was considered.

The previous example makes clear that auxiliary systems must be taken into account if we are to understand the optimal probability with which channels can be distinguished.

20.2 Definition and properties of the completely bounded trace norm

With the discussion from the previous section in mind, we will now discuss two norms: the *induced trace norm* and the *completely bounded trace norm*. The precise relationship these norms have to the notion of channel distinguishability will be made clear later in the section.

20.2.1 The induced trace norm

We will begin with the induced trace norm. This norm does not provide a suitable way to measure distances between channels, at least with respect to the issues discussed in the previous section, but it will nevertheless be helpful from a mathematical point of view for us to start with this norm.

For any choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, and for a given mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, the induced trace norm is defined as

$$\|\Phi\|_1 = \max\left\{\|\Phi(X)\|_1 \,:\, X \in \mathrm{L}(\mathcal{X}),\ \|X\|_1 \leq 1\right\}. \tag{20.1}$$

This norm is just one of many possible examples of induced norms; in general, one may consider the norm obtained by replacing the two trace norms in this definition with any other choice of norms that are defined on $\mathrm{L}(\mathcal{X})$ and $\mathrm{L}(\mathcal{Y})$. The use of the maximum, rather than the supremum, is justified in this context by the observation that every norm defined on a complex Euclidean space is continuous and its corresponding unit ball is compact.

Let us note two simple properties of the induced trace norm that will be useful for our purposes. First, for every choice of complex Euclidean spaces $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, and mappings $\Psi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ and $\Phi \in \mathrm{T}(\mathcal{Y}, \mathcal{Z})$, it holds that

$$\|\Phi\Psi\|_1 \leq \|\Phi\|_1 \|\Psi\|_1. \tag{20.2}$$

This is a general property of every induced norm, provided that the same norm on $\mathrm{L}(\mathcal{Y})$ is taken for both induced norms.

Second, the induced trace norm can be expressed as follows for a given mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$:

$$\|\Phi\|_1 = \max\{\|\Phi(uv^*)\|_1 \,:\, u, v \in \mathcal{S}(\mathcal{X})\}, \tag{20.3}$$

where $\mathcal{S}(\mathcal{X}) = \{x \in \mathcal{X} \,:\, \|x\| = 1\}$ denotes the unit sphere in $\mathcal{X}$. This fact holds because the trace norm (like every other norm) is a convex function, and the unit ball with respect to the trace norm can be represented as

$$\{X \in \mathrm{L}(\mathcal{X}) \,:\, \|X\|_1 \leq 1\} = \mathrm{conv}\{uv^* \,:\, u, v \in \mathcal{S}(\mathcal{X})\}.$$

Alternately, one can prove that (20.3) holds by considering a singular value decomposition of any operator $X \in \mathrm{L}(\mathcal{X})$ with $\|X\|_1 \leq 1$ that maximizes (20.1).

One undesirable property of the induced trace norm is that it is not multiplicative with respect to tensor products. For instance, for a complex Euclidean space $\mathcal{X}$, let us consider the transpose mapping $T \in \mathrm{T}(\mathcal{X})$ and the identity mapping $\mathbb{1}_{\mathrm{L}(\mathcal{X})} \in \mathrm{T}(\mathcal{X})$. It holds that

$$\|T\|_1 = 1 = \left\|\mathbb{1}_{\mathrm{L}(\mathcal{X})}\right\|_1$$

but

$$\left\|T \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})}\right\|_1 \geq \left\|(T \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(\tau)\right\|_1 = \frac{1}{n}\|W\|_1 = n \tag{20.4}$$

for $n = \dim(\mathcal{X})$, $\tau \in \mathrm{D}(\mathcal{X} \otimes \mathcal{X})$ defined as

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

and $W \in \mathrm{L}(\mathcal{X} \otimes \mathcal{X})$ denoting the swap operator, as in Example 20.1. (The inequality in (20.4) is really an equality, but it is not necessary for us to prove this at this moment.) Thus, we have

$$\left\|T \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})}\right\|_1 > \|T\|_1 \left\|\mathbb{1}_{\mathrm{L}(\mathcal{X})}\right\|_1,$$

assuming $n \geq 2$.

20.2.2 The completely bounded trace norm

We will now define the completely bounded trace norm, which may be seen as a modification of the induced trace norm that corrects for that norm's failure to be multiplicative with respect to tensor products.

For any choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$, and a mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, we define the *completely bounded trace norm* of Φ to be

$$|||\Phi|||_1 = \left\|\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})}\right\|_1.$$

(This norm is also commonly called the *diamond norm*, and denoted $\|\Phi\|_\diamond$.) The principle behind its definition is that tensoring Φ with the identity mapping has the effect of *stabilizing* its induced trace norm. This sort of stabilization endows the completely bounded trace norm with many nice properties, and allows it to be used in contexts where the induced trace norm is not sufficient. This sort of stabilization is also related to the phenomenon illustrated in the previous section, where tensoring with the identity channel had the effect of amplifying the difference between channels.

The first thing we must do is to explain why the definition of the completely bounded trace norm tensors Φ with the identity mapping on $\mathrm{L}(\mathcal{X})$, rather than some other space. The answer is that $\mathcal{X}$ has sufficiently large dimension—and replacing $\mathcal{X}$ with any complex Euclidean space with larger dimension would not change anything. The following lemma allows us to prove this fact, and includes a special case that will be useful later in the lecture.

Lemma 20.2. *Let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, and let $\mathcal{Z}$ be a complex Euclidean space. For every choice of unit vectors $u, v \in \mathcal{X} \otimes \mathcal{Z}$ there exist unit vectors $x, y \in \mathcal{X} \otimes \mathcal{X}$ such that*

$$\left\|(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(uv^*)\right\|_1 = \left\|(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(xy^*)\right\|_1.$$

In case $u = v$, we may in addition take $x = y$.

Proof. The lemma is straightforward when $\dim(\mathcal{Z}) \leq \dim(\mathcal{X})$; for any choice of a linear isometry $U \in \mathrm{U}(\mathcal{Z}, \mathcal{X})$ the vectors $x = (\mathbb{1}_{\mathcal{X}} \otimes U)u$ and $y = (\mathbb{1}_{\mathcal{X}} \otimes U)v$ satisfy the required conditions. Let us therefore consider the case where $\dim(\mathcal{Z}) > \dim(\mathcal{X}) = n$.

Consider the vector $u \in \mathcal{X} \otimes \mathcal{Z}$. Given that $\dim(\mathcal{X}) \leq \dim(\mathcal{Z})$, there must exist an orthogonal projection $\Pi \in \mathrm{L}(\mathcal{Z})$ having rank at most $n = \dim(\mathcal{X})$ that satisfies $u = (\mathbb{1}_{\mathcal{X}} \otimes \Pi)u$ and therefore there must exist a linear isometry $U \in \mathrm{U}(\mathcal{X}, \mathcal{Z})$ such that $u = (\mathbb{1}_{\mathcal{X}} \otimes UU^*)u$. Likewise there must exist a linear isometry $V \in \mathrm{U}(\mathcal{X}, \mathcal{Z})$ such that $v = (\mathbb{1}_{\mathcal{X}} \otimes VV^*)v$. Such linear isometries U and V can be obtained from Schmidt decompositions of u and v.

Now let $x = (\mathbb{1} \otimes U^*)u$ and $y = (\mathbb{1} \otimes V^*)v$. Notice that we therefore have $u = (\mathbb{1} \otimes U)x$ and $v = (\mathbb{1} \otimes V)y$, which shows that x and y are unit vectors. Moreover, given that $\|U\| = \|V\| = 1$, we have

$$\begin{aligned}
\Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(uv^*) \Big\|_1 &= \Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})((\mathbb{1} \otimes U)xy^*(\mathbb{1} \otimes V^*)) \Big\|_1 \\
&= \Big\| (\mathbb{1} \otimes U)(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(xy^*)(\mathbb{1} \otimes V^*) \Big\|_1 \\
&= \Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(xy^*) \Big\|_1
\end{aligned}$$

as required. In case $u = v$, we may take $U = V$, implying that $x = y$. □

The following theorem, which explains the choice of taking the identity mapping on $\mathrm{L}(\mathcal{X})$ in the definition of the completely bounded trace norm, is immediate from Lemma 20.2 together with (20.3).

Theorem 20.3. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be any mapping, and let $\mathcal{Z}$ be any complex Euclidean space for which $\dim(\mathcal{Z}) \geq \dim(\mathcal{X})$. It holds that*

$$\Big\| \Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})} \Big\|_1 = |||\Phi|||_1 .$$

One simple but important consequence of this theorem is that the completely bounded trace norm is multiplicative with respect to tensor products.

Theorem 20.4. *For every choice of mappings $\Phi_1 \in \mathrm{T}(\mathcal{X}_1, \mathcal{Y}_1)$ and $\Phi_2 \in \mathrm{T}(\mathcal{X}_2, \mathcal{Y}_2)$, it holds that*

$$|||\Phi_1 \otimes \Phi_2|||_1 = |||\Phi_1|||_1 \, |||\Phi_2|||_1 .$$

Proof. Let $\mathcal{W}_1$ and $\mathcal{W}_2$ be complex Euclidean spaces with $\dim(\mathcal{W}_1) = \dim(\mathcal{X}_1)$ and $\dim(\mathcal{W}_2) = \dim(\mathcal{X}_2)$, so that

$$\begin{aligned}
|||\Phi_1|||_1 &= \Big\| \Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1)} \Big\|_1 , \\
|||\Phi_2|||_1 &= \Big\| \Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_2)} \Big\|_1 , \\
|||\Phi_1 \otimes \Phi_2|||_1 &= \Big\| \Phi_1 \otimes \Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1 \otimes \mathcal{W}_2)} \Big\|_1 .
\end{aligned}$$

We have

$$\begin{aligned}
|||\Phi_1 \otimes \Phi_2|||_1 &= \Big\| \Phi_1 \otimes \Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1 \otimes \mathcal{W}_2)} \Big\|_1 \\
&= \Big\| \Big(\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y}_2)} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1 \otimes \mathcal{W}_2)} \Big) \Big(\mathbb{1}_{\mathrm{L}(\mathcal{X}_1)} \otimes \Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1 \otimes \mathcal{W}_2)} \Big) \Big\|_1 \\
&\leq \Big\| \Big(\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Y}_2)} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1 \otimes \mathcal{W}_2)} \Big) \Big\|_1 \, \Big\| \Big(\mathbb{1}_{\mathrm{L}(\mathcal{X}_1)} \otimes \Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1 \otimes \mathcal{W}_2)} \Big) \Big\|_1 \\
&= |||\Phi_1|||_1 \, |||\Phi_2|||_1 ,
\end{aligned}$$

where the last inequality follows by Theorem 20.3.

For the reverse inequality, choose operators $X_1 \in \mathrm{L}(\mathcal{X}_1 \otimes \mathcal{W}_1)$ and $X_2 \in \mathrm{L}(\mathcal{X}_2 \otimes \mathcal{W}_2)$ such that $\|X_1\|_1 = \|X_2\|_1 = 1$, $|||\Phi_1|||_1 = \|(\Phi_1 \otimes \mathbb{1}_{\mathcal{W}_1})(X_1)\|_1$, and $|||\Phi_2|||_1 = \|(\Phi_2 \otimes \mathbb{1}_{\mathcal{W}_2})(X_2)\|_1$. IT holds that $\|X_1 \otimes X_2\|_1 = 1$, and so

$$\begin{aligned}
|||\Phi_1 \otimes \Phi_2|||_1 &= \Big\| \Phi_1 \otimes \Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1 \otimes \mathcal{W}_2)} \Big\|_1 \\
&\geq \Big\| \Big(\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1)} \otimes \Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_2)} \Big) (X_1 \otimes X_2) \Big\|_1 \\
&= \Big\| \Big(\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1)} \Big) (X_1) \otimes \Big(\Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_2)} \Big) (X_2) \Big\|_1 \\
&= \Big\| \Big(\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_1)} \Big) (X_1) \Big\|_1 \, \Big\| \Big(\Phi_2 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W}_2)} \Big) (X_2) \Big\|_1 \\
&= |||\Phi_1|||_1 \, |||\Phi_2|||_1
\end{aligned}$$

as required. □

The final fact that we will establish about the completely bounded trace norm in this lecture concerns input operators for which the value of the completely bounded trace norm is achieved. In particular, we will establish that for Hermiticity-preserving mappings $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, there must exist a unit vector $u \in \mathcal{X} \otimes \mathcal{X}$ for which

$$|||\Phi|||_1 = \Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(uu^*) \Big\|_1 .$$

This fact will give us the final piece we need to connect the completely bounded trace norm to the distinguishability problem discussed in the beginning of the lecture.

Theorem 20.5. *Suppose that $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is Hermiticity-preserving. It holds that*

$$|||\Phi|||_1 = \max \Big\{ \Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(xx^*) \Big\|_1 \, : \, x \in \mathcal{S}(\mathcal{X} \otimes \mathcal{X}) \Big\} .$$

Proof. Let $X \in \mathrm{L}(\mathcal{X} \otimes \mathcal{X})$ be an operator with $\|X\|_1 = 1$ that satisfies

$$|||\Phi|||_1 = \Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(X) \Big\|_1 .$$

Let $\mathcal{Z} = \mathbb{C}^{\{0,1\}}$ and let

$$Y = \frac{1}{2} X \otimes E_{0,1} + \frac{1}{2} X^* \otimes E_{1,0} \in \mathrm{Herm}(\mathcal{X} \otimes \mathcal{X} \otimes \mathcal{Z}) .$$

We have $\|Y\| = \|X\| = 1$ and

$$\begin{aligned}
\Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X} \otimes \mathcal{Z})})(Y) \Big\|_1 &= \frac{1}{2} \Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(X) \otimes E_{0,1} + (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(X^*) \otimes E_{1,0} \Big\|_1 \\
&= \frac{1}{2} \Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(X) \otimes E_{0,1} + ((\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(X))^* \otimes E_{1,0} \Big\|_1 \\
&= \Big\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(X) \Big\|_1 \\
&= |||\Phi|||_1 ,
\end{aligned}$$

where the second equality follows from the fact that Φ is Hermiticity-preserving. Now, because Y is Hermitian, we may consider a spectral decomposition

$$Y = \sum_j \lambda_j u_j u_j^*.$$

By the triangle inequality we have

$$|||\Phi|||_1 = \left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X}\otimes\mathcal{Z})})(Y) \right\| \leq \sum_j |\lambda_j| \left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X}\otimes\mathcal{Z})})(u_j u_j^*) \right\|_1.$$

As $\|Y\| = 1$, we have $\sum_j |\lambda_j| = 1$, and thus

$$\left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X}\otimes\mathcal{Z})})(u_j u_j^*) \right\|_1 \geq |||\Phi|||_1$$

for some index j. We may therefore apply Lemma 20.2 to obtain a unit vector $x \in \mathcal{X} \otimes \mathcal{X}$ such that

$$\left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(xx^*) \right\|_1 = \left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X}\otimes\mathcal{Z})})(u_j u_j^*) \right\|_1 \geq |||\Phi|||_1.$$

Thus

$$|||\Phi|||_1 \leq \max\left\{ \left\| (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(xx^*) \right\|_1 : x \in \mathcal{S}(\mathcal{X} \otimes \mathcal{X}) \right\}.$$

It is clear that the maximum cannot exceed $|||\Phi|||_1$, and so the proof is complete. □

Let us note that at this point we have established the relationship between the completely bounded trace norm and the problem of channel distinguishability that we discussed at the beginning of the lecture; in essence, the relationship is an analogue of Helstrom's theorem for channels.

Theorem 20.6. *Let $\Phi_0, \Phi_1 \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ be channels and let $\lambda \in [0, 1]$. It holds that*

$$\sup_{\xi, P_0, P_1} \left[\lambda \left\langle P_0, (\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(\xi) \right\rangle + (1-\lambda) \left\langle P_1, (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{Z})})(\xi) \right\rangle \right] = \frac{1}{2} + \frac{1}{2} |||\lambda\Phi_0 - (1-\lambda)\Phi_1|||_1,$$

where the supremum is over all complex Euclidean spaces $\mathcal{Z}$, density operators $\xi \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Z})$, and binary valued measurements $\{P_0, P_1\} \subset \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z})$. Moreover, the supremum is achieved for $\mathcal{Z} = \mathcal{X}$ and $\xi = uu^*$ being a pure state.

20.3 Distinguishing unitary and isometric channels

We started the lecture with an example of two channels $\Phi_0, \Phi_1 \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ for which an auxiliary system was necessary to optimally distinguish Φ_0 and Φ_1. Let us conclude the lecture by observing that this phenomenon does not arise for mappings induced by linear isometries.

Theorem 20.7. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $U, V \in \mathrm{U}(\mathcal{X}, \mathcal{Y})$ be linear isometries, and suppose*

$$\Phi_0(X) = UXU^* \quad \text{and} \quad \Phi_1(X) = VXV^*$$

for all $X \in \mathrm{L}(\mathcal{X})$. There exists a unit vector $u \in \mathcal{X}$ such that

$$\|\Phi_0(uu^*) - \Phi_1(uu^*)\|_1 = |||\Phi_0 - \Phi_1|||_1.$$

Proof. Recall that the numerical range of an operator $A \in \mathrm{L}(\mathcal{X})$ is defined as

$$\mathcal{N}(A) = \{u^* A u \,:\, u \in \mathcal{S}(\mathcal{X})\}.$$

Let us define $\nu(A)$ to be the *smallest* absolute value of any element of $\mathcal{N}(A)$:

$$\nu(A) = \min\{|\alpha| \,:\, \alpha \in \mathcal{N}(A)\}.$$

Now, for any choice of a unit vector $u \in \mathcal{X}$ we have

$$\|\Phi_0(uu^*) - \Phi_1(uu^*)\|_1 = \|Uuu^*U^* - Vuu^*V^*\|_1 = 2\sqrt{1 - |u^*U^*Vu|^2}.$$

Maximizing this quantity over $u \in \mathcal{S}(\mathcal{X})$ gives

$$\max\{\|\Phi_0(uu^*) - \Phi_1(uu^*)\|_1 \,:\, u \in \mathcal{S}(\mathcal{X})\} = 2\sqrt{1 - \nu(U^*V)^2}.$$

Along similar lines, we have

$$|||\Phi_0 - \Phi_1|||_1 = \max_{u \in \mathcal{S}(\mathcal{X}\otimes\mathcal{X})} \Big\|(\Phi_0 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(uu^*) - (\Phi_1 \otimes \mathbb{1}_{\mathrm{L}(\mathcal{X})})(uu^*)\Big\|_1 = 2\sqrt{1 - \nu(U^*V \otimes \mathbb{1}_{\mathcal{X}})^2},$$

where here we have also made use of Theorem 20.5.

To complete the proof it therefore suffices to prove that

$$\nu(A \otimes \mathbb{1}_{\mathcal{X}}) = \nu(A)$$

for every operator $A \in \mathrm{L}(\mathcal{X})$. It is clear that $\nu(A \otimes \mathbb{1}_{\mathcal{X}}) \leq \nu(A)$, so we just need to prove $\nu(A \otimes \mathbb{1}_{\mathcal{X}}) \geq \nu(A)$. Let $u \in \mathcal{X} \otimes \mathcal{X}$ be any unit vector, and let

$$u = \sum_{j=1}^{r} \sqrt{p_j}\, x_j \otimes y_j$$

be a Schmidt decomposition of u. It holds that

$$u^*(A \otimes \mathbb{1}_{\mathcal{X}})u = \sum_{j=1}^{r} p_j x_j^* A x_j.$$

For each j we have $u_j^* A u_j \in \mathcal{N}(A)$, and therefore

$$u^*(A \otimes \mathbb{1}_{\mathcal{X}})u = \sum_{j=1}^{r} p_j x_j^* A x_j \in \mathcal{N}(A)$$

by the Toeplitz–Hausdorff theorem. Consequently

$$|u^*(A \otimes \mathbb{1}_{\mathcal{X}})u| \geq \nu(A)$$

for every $u \in \mathcal{S}(\mathcal{X} \otimes \mathcal{X})$, which completes the proof. □

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

Lecture 21: Alternate characterizations of the completely bounded trace norm

In the previous lecture we discussed the completely bounded trace norm, its connection to the problem of distinguishing channels, and some of its basic properties. In this lecture we will discuss a few alternate ways in which this norm may be characterized, including a semidefinite programming formulation that allows for an efficient calculation of the norm.

21.1 Maximum output fidelity characterization

Suppose $\mathcal{X}$ and $\mathcal{Y}$ are complex Euclidean spaces and $\Phi_0, \Phi_1 \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ are completely positive (but not necessarily trace-preserving) maps. Let us define the *maximum output fidelity* of Φ_0 and Φ_1 as

$$\mathrm{F}_{\max}(\Phi_0, \Phi_1) = \max\left\{\mathrm{F}(\Phi_0(\rho_0), \Phi_1(\rho_1)) \,:\, \rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})\right\}.$$

In other words, this is the maximum fidelity between an output of Φ_0 and an output of Φ_1, ranging over all pairs of density operator inputs.

Our first alternate characterization of the completely bounded trace norm is based on the maximum output fidelity, and is given by the following theorem.

Theorem 21.1. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be an arbitrary mapping. Suppose further that $\mathcal{Z}$ is a complex Euclidean space and $A_0, A_1 \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ satisfy*

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(A_0 X A_1^*)$$

for all $X \in \mathrm{L}(\mathcal{X})$. For completely positive mappings $\Psi_0, \Psi_1 \in \mathrm{T}(\mathcal{X}, \mathcal{Z})$ defined as

$$\Psi_0(X) = \mathrm{Tr}_{\mathcal{Y}}(A_0 X A_0^*),$$
$$\Psi_1(X) = \mathrm{Tr}_{\mathcal{Y}}(A_1 X A_1^*),$$

for all $X \in \mathrm{L}(\mathcal{X})$, we have $|||\Phi|||_1 = \mathrm{F}_{\max}(\Psi_0, \Psi_1)$.

Remark 21.2. Note that it is the space $\mathcal{Y}$ that is traced-out in the definition of Ψ_0 and Ψ_1, rather than the space $\mathcal{Z}$.

To prove this theorem, we will begin with the following lemma that establishes a simple relationship between the fidelity and the trace norm. (This appeared as a problem on problem set 1.)

Lemma 21.3. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $u, v \in \mathcal{X} \otimes \mathcal{Y}$. It holds that*

$$\mathrm{F}\left(\mathrm{Tr}_{\mathcal{Y}}(uu^*), \mathrm{Tr}_{\mathcal{Y}}(vv^*)\right) = \left\|\mathrm{Tr}_{\mathcal{X}}(uv^*)\right\|_1.$$

Proof. It is the case that $u \in \mathcal{X} \otimes \mathcal{Y}$ is a purification of $\mathrm{Tr}_{\mathcal{Y}}(uu^*)$ and $v \in \mathcal{X} \otimes \mathcal{Y}$ is a purification of $\mathrm{Tr}_{\mathcal{Y}}(vv^*)$. By the unitary equivalence of purifications (Theorem 4.3 in the lecture notes), it holds that every purification of $\mathrm{Tr}_{\mathcal{Y}}(uu^*)$ in $\mathcal{X} \otimes \mathcal{Y}$ takes the form $(\mathbb{1}_{\mathcal{X}} \otimes U)u$ for some choice of a unitary operator $U \in \mathrm{U}(\mathcal{Y})$. Consequently, by Uhlmann's theorem we have

$$\mathrm{F}(\mathrm{Tr}_{\mathcal{Y}}(uu^*), \mathrm{Tr}_{\mathcal{Y}}(vv^*)) = \mathrm{F}(\mathrm{Tr}_{\mathcal{Y}}(vv^*), \mathrm{Tr}_{\mathcal{Y}}(uu^*)) = \max\{|\langle v, (\mathbb{1}_{\mathcal{X}} \otimes U)u\rangle| \,:\, U \in \mathrm{U}(\mathcal{Y})\}.$$

For any unitary operator U it holds that

$$\langle v, (\mathbb{1}_{\mathcal{X}} \otimes U)u\rangle = \mathrm{Tr}\left((\mathbb{1}_{\mathcal{X}} \otimes U)uv^*\right) = \mathrm{Tr}\left(U \,\mathrm{Tr}_{\mathcal{X}}(uv^*)\right),$$

and therefore

$$\max\{|\langle v, (\mathbb{1}_{\mathcal{X}} \otimes U)u\rangle| \,:\, U \in \mathrm{U}(\mathcal{Y})\} = \max\{|\mathrm{Tr}\left(U \,\mathrm{Tr}_{\mathcal{X}}(uv^*)\right)| \,:\, U \in \mathrm{U}(\mathcal{Y})\} = \|\mathrm{Tr}_{\mathcal{X}}(uv^*)\|_1$$

as required. □

Proof of Theorem 21.1. Let us take $\mathcal{W}$ to be a complex Euclidean space with the same dimension as $\mathcal{X}$, so that

$$\begin{aligned}
|||\Phi|||_1 &= \max\left\{\left\|(\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{W})})(uv^*)\right\|_1 \,:\, u, v \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W})\right\} \\
&= \max\left\{\|\mathrm{Tr}_{\mathcal{Z}}\left[(A_0 \otimes \mathbb{1}_{\mathcal{W}})\, uv^*\, (A_1^* \otimes \mathbb{1}_{\mathcal{W}})\right]\|_1 \,:\, u, v \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W})\right\}.
\end{aligned}$$

For any choice of vectors $u, v \in \mathcal{X} \otimes \mathcal{W}$ we have

$$\begin{aligned}
\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{W}}\left[(A_0 \otimes \mathbb{1}_{\mathcal{W}})uu^*(A_0^* \otimes \mathbb{1}_{\mathcal{W}})\right] &= \Psi_0\left(\mathrm{Tr}_{\mathcal{W}}\left(uu^*\right)\right), \\
\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{W}}\left[(A_1 \otimes \mathbb{1}_{\mathcal{W}})vv^*(A_1^* \otimes \mathbb{1}_{\mathcal{W}})\right] &= \Psi_1\left(\mathrm{Tr}_{\mathcal{W}}\left(vv^*\right)\right),
\end{aligned}$$

and therefore by Lemma 21.3 it follows that

$$\|\mathrm{Tr}_{\mathcal{Z}}\left[(A_0 \otimes \mathbb{1}_{\mathcal{W}})uv^*(A_1^* \otimes \mathbb{1}_{\mathcal{W}})\right]\|_1 = \mathrm{F}(\Psi_0(\mathrm{Tr}_{\mathcal{W}}(uu^*)), \Psi_1(\mathrm{Tr}_{\mathcal{W}}(vv^*))).$$

Consequently

$$\begin{aligned}
|||\Phi|||_1 &= \max\left\{\mathrm{F}\left(\Psi_0(\mathrm{Tr}_{\mathcal{W}}(uu^*)), \Psi_1(\mathrm{Tr}_{\mathcal{W}}(vv^*))\right) \,:\, u, v \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W})\right\} \\
&= \max\left\{\mathrm{F}(\Psi_0(\rho_0), \Psi_1(\rho_1)) \,:\, \rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})\right\} \\
&= \mathrm{F}_{\max}(\Psi_0, \Psi_1)
\end{aligned}$$

as required. □

The following corollary follows immediately from this characterization along with the fact that the completely bounded trace norm is multiplicative with respect to tensor products.

Corollary 21.4. *Let $\Phi_1, \Psi_1 \in \mathrm{T}(\mathcal{X}_1, \mathcal{Y}_1)$ and $\Phi_2, \Psi_2 \in \mathrm{T}(\mathcal{X}_2, \mathcal{Y}_2)$ be completely positive. It holds that*

$$\mathrm{F}_{\max}(\Phi_1 \otimes \Phi_2, \Psi_1 \otimes \Psi_2) = \mathrm{F}_{\max}(\Phi_1, \Psi_1) \cdot \mathrm{F}_{\max}(\Phi_2, \Psi_2).$$

This is a simple but not obvious fact: it says that the maximum fidelity between the outputs of any two completely positive product mappings is achieved for product state inputs. In contrast, several other quantities of interest based on quantum channels fail to respect tensor products in this way.

21.2 A semidefinite program for the completely bounded trace norm (squared)

The square of the completely bounded trace norm of an arbitrary mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ can be expressed as the optimal value of a semidefinite program, as we will now verify. This provides a means to efficiently approximate the completely bounded trace norm of a given mapping—because there exist efficient algorithms to approximate the optimal value of very general classes of semidefinite programs (which includes our particular semidefinite program) to high precision.

Let us begin by describing the semidefinite program, starting first with its associated primal and dual problems. After doing this we will verify that its value corresponds to the square of the completely bounded trace norm. Throughout this discussion we assume that a Stinespring representation

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(A_0 X A_1^*)$$

of an arbitrary mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ has been fixed.

21.2.1 Description of the semidefinite program

The primal and dual problems for the semidefinite program we wish to consider are as follows:

Primal problem		Dual problem	
maximize:	$\langle A_1 A_1^*, X \rangle$	minimize:	$\| A_0^* (\mathbb{1}_{\mathcal{Y}} \otimes Y) A_0 \|$
subject to:	$\mathrm{Tr}_{\mathcal{Y}}(X) = \mathrm{Tr}_{\mathcal{Y}}(A_0 \rho A_0^*)$,	subject to:	$\mathbb{1}_{\mathcal{Y}} \otimes Y \geq A_1 A_1^*$,
	$\rho \in \mathrm{Pos}(\mathcal{X})$,		$Y \in \mathrm{Pos}(\mathcal{Z})$.
	$X \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z})$.		

This pair of problems may be expressed more formally as a semidefinite program in the following way. Define $\Xi \in \mathrm{T}((\mathcal{Y} \otimes \mathcal{Z}) \oplus \mathcal{X}, \mathbb{C} \oplus \mathcal{Z})$ as follows:

$$\Xi \begin{pmatrix} X & \cdot \\ \cdot & \rho \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}(\rho) & 0 \\ 0 & \mathrm{Tr}_{\mathcal{Y}}(X) - \mathrm{Tr}_{\mathcal{Y}}(A_0 \rho A_0^*) \end{pmatrix}.$$

(The submatrices indicated by $\cdot$ are ones we do not care about and do not bother to assign a name.) We see that the primal problem above asks for the maximum (or supremum) value of

$$\left\langle \begin{pmatrix} A_1 A_1^* & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} X & \cdot \\ \cdot & \rho \end{pmatrix} \right\rangle$$

subject to the constraints

$$\Xi \begin{pmatrix} X & \cdot \\ \cdot & \rho \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} X & \cdot \\ \cdot & \rho \end{pmatrix} \in \mathrm{Pos}((\mathcal{Y} \otimes \mathcal{Z}) \oplus \mathcal{X}).$$

The dual problem is therefore to minimize the inner product

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \lambda & \cdot \\ \cdot & Y \end{pmatrix} \right\rangle,$$

for $\lambda \geq 0$ and $Y \in \mathrm{Pos}(\mathcal{Z})$, subject to the constraint

$$\Xi^* \begin{pmatrix} \lambda & \cdot \\ \cdot & Y \end{pmatrix} \geq \begin{pmatrix} A_1 A_1^* & 0 \\ 0 & 0 \end{pmatrix}.$$

One may verify that

$$\Xi^* \begin{pmatrix} \lambda & \cdot \\ \cdot & Y \end{pmatrix} = \begin{pmatrix} \mathbb{1}_{\mathcal{Y}} \otimes Y & 0 \\ 0 & \lambda \mathbb{1}_{\mathcal{X}} - A_0^*(\mathbb{1}_{\mathcal{Y}} \otimes Y) A_0 \end{pmatrix}.$$

Given that Y is positive semidefinite, the minimum value of λ for which $\lambda \mathbb{1}_{\mathcal{X}} - A_0^*(\mathbb{1}_{\mathcal{Y}} \otimes Y) A_0 \geq 0$ is equal to $\| A_0^*(\mathbb{1}_{\mathcal{Y}} \otimes Y) A_0 \|$, and so we have obtained the dual problem as it is originally stated.

21.2.2 Analysis of the semidefinite program

We will now analyze the semidefinite program given above. Before we discuss its relationship to the completely bounded trace norm, let us verify that it satisfies strong duality. The dual problem is strictly feasible, for we may choose

$$Y = (\| A_1 A_1^* \| + 1) \mathbb{1}_{\mathcal{Z}} \qquad \text{and} \qquad \lambda = \| A_1 A_1^* \| \, \| A_0 A_0^* \| + 1$$

to obtain a strictly feasible solution. The primal problem is of course feasible, for we may choose $\rho \in \mathrm{D}(\mathcal{X})$ arbitrarily and take $X = A_0 \rho A_0^*$ to obtain a primal feasible operator. Thus, by Slater's theorem, strong duality holds for our semidefinite program, and we also have that the optimal primal value is obtained by a primal feasible operator.

Now let us verify that the optimal value associated with this semidefinite program corresponds to $\|\!|\!| \Phi |\!|\!|_1^2$. Let us define a set

$$\mathcal{A} = \{ X \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{Z}) \, : \, \mathrm{Tr}_{\mathcal{Y}}(X) = \mathrm{Tr}_{\mathcal{Y}}(A_0 \rho A_0^*) \text{ for some } \rho \in \mathrm{D}(\mathcal{X}) \}.$$

It holds that the optimal primal value α of the semidefinite program is given by

$$\alpha = \max_{X \in \mathcal{A}} \langle A_1 A_1^*, X \rangle .$$

For any choice of a complex Euclidean space $\mathcal{W}$ for which $\dim(\mathcal{W}) \geq \dim(\mathcal{X})$, we have

$$\begin{aligned}
\|\!|\!| \Phi |\!|\!|_1^2 &= \max_{u,v \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W})} \| \mathrm{Tr}_{\mathcal{Z}} \left[(A_0 \otimes \mathbb{1}_{\mathcal{W}}) u v^* (A_1 \otimes \mathbb{1}_{\mathcal{W}})^* \right] \|_1^2 \\
&= \max_{\substack{u,v \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W}) \\ U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W})}} | \mathrm{Tr} \left[(U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}}) u v^* (A_1 \otimes \mathbb{1}_{\mathcal{W}})^* \right] |^2 \\
&= \max_{\substack{u,v \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W}) \\ U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W})}} | v^* (A_1 \otimes \mathbb{1}_{\mathcal{W}})^* (U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}}) u |^2 \\
&= \max_{\substack{u \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W}) \\ U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W})}} \| (A_1 \otimes \mathbb{1}_{\mathcal{W}})^* (U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}}) u \|^2 \\
&= \max_{\substack{u \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W}) \\ U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W})}} \mathrm{Tr} \left[(A_1 A_1^* \otimes \mathbb{1}_{\mathcal{W}})(U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}}) u u^* (A_0 \otimes \mathbb{1}_{\mathcal{W}})^* (U \otimes \mathbb{1}_{\mathcal{Z}})^* \right] \\
&= \max_{\substack{u \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W}) \\ U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W})}} \left\langle A_1 A_1^*, \mathrm{Tr}_{\mathcal{W}} \left[(U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}}) u u^* (A_0 \otimes \mathbb{1}_{\mathcal{W}})^* (U \otimes \mathbb{1}_{\mathcal{Z}})^* \right] \right\rangle .
\end{aligned}$$

It now remains to prove that

$$\mathcal{A} = \{ \mathrm{Tr}_{\mathcal{W}} \left[(U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}}) u u^* (A_0 \otimes \mathbb{1}_{\mathcal{W}})^* (U \otimes \mathbb{1}_{\mathcal{Z}})^* \right] \, : \, u \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W}), \; U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W}) \}$$

for some choice of $\mathcal{W}$ with $\dim(\mathcal{W}) \geq \dim(\mathcal{X})$. We will choose $\mathcal{W}$ such that

$$\dim(\mathcal{W}) = \max\{\dim(\mathcal{X}), \dim(\mathcal{Y} \otimes \mathcal{Z})\}.$$

First consider an arbitrary choice of $u \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W})$ and $U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W})$, and let

$$X = \mathrm{Tr}_{\mathcal{W}}\left[(U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}})uu^*(A_0 \otimes \mathbb{1}_{\mathcal{W}})^*(U \otimes \mathbb{1}_{\mathcal{Z}})^*\right].$$

It follows that $\mathrm{Tr}_{\mathcal{Y}}(X) = \mathrm{Tr}_{\mathcal{Y}}\left(A_0 \,\mathrm{Tr}_{\mathcal{W}}(uu^*)A_0^*\right)$, and so $X \in \mathcal{A}$. Now consider an arbitrary element $X \in \mathcal{A}$, and let $\rho \in \mathrm{D}(\mathcal{X})$ satisfy $\mathrm{Tr}_{\mathcal{Y}}(X) = \mathrm{Tr}_{\mathcal{Y}}(A_0\rho A_0^*)$. Let $u \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W})$ purify ρ and let $x \in \mathcal{Y} \otimes \mathcal{Z} \otimes \mathcal{W}$ purify X. We have

$$\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{W}}(xx^*) = \mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{W}}\left((A_0 \otimes \mathbb{1}_{\mathcal{W}})uu^*(A_0 \otimes \mathbb{1}_{\mathcal{W}})^*\right),$$

so there exists $U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W})$ such that $(U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}})u = x$, and therefore

$$X = \mathrm{Tr}_{\mathcal{W}}(xx^*) = \mathrm{Tr}_{\mathcal{W}}\left[(U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}})uu^*(A_0 \otimes \mathbb{1}_{\mathcal{W}})^*(U \otimes \mathbb{1}_{\mathcal{Z}})^*\right].$$

We have therefore proved that

$$\mathcal{A} = \left\{\mathrm{Tr}_{\mathcal{W}}\left[(U \otimes \mathbb{1}_{\mathcal{Z}})(A_0 \otimes \mathbb{1}_{\mathcal{W}})uu^*(A_0 \otimes \mathbb{1}_{\mathcal{W}})^*(U \otimes \mathbb{1}_{\mathcal{Z}})^*\right] : u \in \mathcal{S}(\mathcal{X} \otimes \mathcal{W}),\ U \in \mathrm{U}(\mathcal{Y} \otimes \mathcal{W})\right\},$$

and so we have that the optimal primal value of our semidefinite program is $\alpha = |||\Phi|||_1^2$ as claimed.

21.3 Spectral norm characterization of the completely bounded trace norm

We will now use the semidefinite program from the previous section to obtain a different characterization of the completely bounded trace norm. Let us begin with a definition, followed by a theorem that states the characterization precisely.

Consider any mapping $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, for complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$. For a given choice of a complex Euclidean space $\mathcal{Z}$, we have that there exists a Stinespring representation

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}\left(A_0 X A_1^*\right),$$

for some choice of $A_0, A_1 \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ if and only if $\dim(\mathcal{Z}) \geq \mathrm{rank}(J(\Phi))$. Under the assumption that $\dim(\mathcal{Z}) \geq \mathrm{rank}(J(\Phi))$, we may therefore consider the non-empty set of pairs (A_0, A_1) that represent Φ in this way:

$$\mathcal{S}_\Phi = \left\{(A_0, A_1) : A_0, A_1 \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z}),\ \Phi(X) = \mathrm{Tr}_{\mathcal{Z}}\left(A_0 X A_1^*\right) \text{ for all } X \in \mathrm{L}(\mathcal{X})\right\}.$$

The characterization of the completely bounded trace norm that is established in this section concerns the spectral norm of the operators in this set, and is given by the following theorem.

Theorem 21.5. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces, let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, and let $\mathcal{Z}$ be a complex Euclidean space with dimension at least* $\mathrm{rank}(J(\Phi))$*. It holds that*

$$|||\Phi|||_1 = \inf\left\{\|A_0\|\,\|A_1\| : (A_0, A_1) \in \mathcal{S}_\Phi\right\}.$$

Proof. For any choice of operators $A_0, A_1 \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ and unit vectors $u, v \in \mathcal{X} \otimes \mathcal{W}$, we have

$$\begin{aligned}\left\| \mathrm{Tr}_{\mathcal{Z}} \left[(A_0 \otimes \mathbb{1}_{\mathcal{W}}) uv^* (A_1^* \otimes \mathbb{1}_{\mathcal{W}}) \right] \right\|_1 &\leq \left\| (A_0 \otimes \mathbb{1}_{\mathcal{W}}) uv^* (A_1^* \otimes \mathbb{1}_{\mathcal{W}}) \right\|_1 \\ &\leq \| A_0 \otimes \mathbb{1}_{\mathcal{W}} \| \, \| uv^* \|_1 \, \| A_1 \otimes \mathbb{1}_{\mathcal{W}} \| = \| A_0 \| \, \| A_1 \|,\end{aligned}$$

which implies that $|||\Phi|||_1 \leq \| A_0 \| \, \| A_1 \|$ for all $(A_0, A_1) \in \mathcal{S}_\Phi$, and consequently

$$|||\Phi||| \leq \inf \{ \| A_0 \| \, \| A_1 \| \, : \, (A_0, A_1) \in \mathcal{S}_\Phi \}.$$

It remains to establish the reverse inequality. Let $(B_0, B_1) \in \mathcal{S}_\Phi$ be an arbitrary pair of operators in $\mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ giving a Stinespring representation for Φ. Given the description of $|||\Phi|||_1^2$ by the semidefinite program from the previous section, along with the fact that strong duality holds for that semidefinite program, we have that $|||\Phi|||_1^2$ is equal to the infimum value of $\| B_0^* (\mathbb{1}_{\mathcal{Y}} \otimes Y) B_0 \|$ over all choices of $Y \in \mathrm{Pos}(\mathcal{Z})$ for which $\mathbb{1}_{\mathcal{Y}} \otimes Y \geq B_1 B_1^*$. This infimum value does not change if we restrict Y to be positive definite, so that

$$|||\Phi|||_1^2 = \inf \{ \| B_0^* (\mathbb{1}_{\mathcal{Y}} \otimes Y) B_0 \| \, : \, \mathbb{1}_{\mathcal{Y}} \otimes Y \geq B_1 B_1^*, \; Y \in \mathrm{Pd}(\mathcal{Z}) \}.$$

For any $\varepsilon > 0$ we may therefore choose $Y \in \mathrm{Pd}(\mathcal{Z})$ such that $\mathbb{1}_{\mathcal{Y}} \otimes Y \geq B_1 B_1^*$ and

$$\left\| \left(\mathbb{1}_{\mathcal{Y}} \otimes Y^{1/2} \right) B_0 \right\|^2 = \| B_0^* (\mathbb{1}_{\mathcal{Y}} \otimes Y) B_0 \| \leq \left(|||\Phi|||_1 + \varepsilon \right)^2.$$

Note that the inequality $\mathbb{1}_{\mathcal{Y}} \otimes Y \geq B_1 B_1^*$ is equivalent to

$$\left\| \left(\mathbb{1}_{\mathcal{Y}} \otimes Y^{-1/2} \right) B_1 \right\|^2 = \left\| \left(\mathbb{1}_{\mathcal{Y}} \otimes Y^{-1/2} \right) B_1 B_1^* \left(\mathbb{1}_{\mathcal{Y}} \otimes Y^{-1/2} \right) \right\| \leq 1.$$

We therefore have that

$$\left\| \left(\mathbb{1}_{\mathcal{Y}} \otimes Y^{1/2} \right) B_0 \right\| \, \left\| \left(\mathbb{1}_{\mathcal{Y}} \otimes Y^{-1/2} \right) B_1 \right\| \leq |||\Phi|||_1 + \varepsilon.$$

It holds that

$$\left(\left(\mathbb{1}_{\mathcal{Y}} \otimes Y^{1/2} \right) B_0, \, \left(\mathbb{1}_{\mathcal{Y}} \otimes Y^{-1/2} \right) B_1 \right) \in \mathcal{S}_\Phi,$$

so

$$\inf \{ \| A_0 \| \, \| A_1 \| \, : \, (A_0, A_1) \in \mathcal{S}_\Phi \} \leq |||\Phi|||_1 + \varepsilon.$$

This inequality holds for all $\varepsilon > 0$, and therefore

$$\inf \{ \| A_0 \| \, \| A_1 \| \, : \, (A_0, A_1) \in \mathcal{S}_\Phi \} \leq |||\Phi|||_1$$

as required. □

21.4 A different semidefinite program for the completely bounded trace norm

There are alternate ways to express the completely bounded trace norm as a semidefinite program from the one described previously. Here is one alternative based on the maximum output fidelity characterization from the start of the lecture.

As before, let $\mathcal{X}$ and $\mathcal{Y}$ be complex Euclidean spaces and let $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be an arbitrary mapping. Suppose further that $\mathcal{Z}$ is a complex Euclidean space and $A_0, A_1 \in \mathrm{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ satisfy

$$\Phi(X) = \mathrm{Tr}_{\mathcal{Z}}(A_0 X A_1^*)$$

for all $X \in \mathrm{L}(\mathcal{X})$. Define completely positive mappings $\Psi_0, \Psi_1 \in \mathrm{T}(\mathcal{X}, \mathcal{Z})$ as

$$\Psi_0(X) = \mathrm{Tr}_{\mathcal{Y}}(A_0 X A_0^*),$$
$$\Psi_1(X) = \mathrm{Tr}_{\mathcal{Y}}(A_1 X A_1^*),$$

for all $X \in \mathrm{L}(\mathcal{X})$, and consider the following semidefinite program:

Primal problem		Dual problem	
maximize:	$\frac{1}{2}\mathrm{Tr}(Y) + \frac{1}{2}\mathrm{Tr}(Y^*)$	minimize:	$\frac{1}{2}\left\|\Psi_0^*(Z_0)\right\| + \frac{1}{2}\left\|\Psi_1^*(Z_1)\right\|$
subject to:	$\begin{pmatrix} \Psi_0(\rho_0) & Y \\ Y^* & \Psi_1(\rho_1) \end{pmatrix} \geq 0$	subject to:	$\begin{pmatrix} Z_0 & -\mathbb{1}_{\mathcal{Z}} \\ -\mathbb{1}_{\mathcal{Z}} & Z_1 \end{pmatrix} \geq 0$
	$\rho_0, \rho_1 \in \mathrm{D}(\mathcal{X})$		$Z_0, Z_1 \in \mathrm{Pos}(\mathcal{Z})$.
	$Y \in \mathrm{L}(\mathcal{Z})$.		

I will leave it to you to translate this semidefinite program into the formal definition we have been using, and to verify that the dual problem is as stated. Note that the discussion of the semidefinite program for the fidelity function from Lecture 8 is helpful for this task. In light of that discussion, it is not difficult to see that the optimal primal value equals $\mathrm{F}_{\max}(\Psi_0, \Psi_1) = \left|\!\left|\!\left|\Phi\right|\!\right|\!\right|_1$. It may also be proved that strong duality holds, leading to an alternate proof of Theorem 21.5.

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

Lecture 22: The finite quantum de Finetti theorem

The main goal of this lecture is to prove a theorem known as the *quantum de Finetti theorem*. There are, in fact, multiple variants of this theorem, so to be more precise it may be said that we will prove a theorem of the quantum de Finetti type. This type of theorem states, in effect, that if a collection of identical quantum registers have a state that is invariant under permutations, then the reduced state of a comparatively small number of these registers must be close to a convex combination of identical product states.

There will be three main parts of this lecture. First, we will introduce various concepts concerning quantum states of multiple register systems that are invariant under permutations of these registers. We will then very briefly discuss integrals defined with respect to the unitarily invariant measure on the unit sphere of a given complex Euclidean space, which will supply us with a useful tool we need for the last part of the lecture. The last part of the lecture is the statement and proof of the quantum de Finetti theorem.

It is inevitable that some details regarding integrals over unitarily invariant measure will be absent from the lecture (and from these notes). The main reason for this is that we have very limited time remaining in the course, and certainly not enough time for a proper discussion of the details. Also, the background knowledge needed to formalize the details is rather different from what was required for other lectures. Nevertheless, I hope there will be enough information for you to follow up on this lecture on your own, in case you choose to do this.

22.1 Symmetric subspaces and exchangeable operators

Let us fix a finite, nonempty set Σ, and let $d = |\Sigma|$ for the remainder of this lecture. Also let n be a positive integer, and let $\mathsf{X}_1, \ldots, \mathsf{X}_n$ be identical quantum registers, with associated complex Euclidean spaces $\mathcal{X}_1, \ldots, \mathcal{X}_n$ taking the form $\mathcal{X}_k = \mathbb{C}^\Sigma$ for $1 \leq k \leq n$.

22.1.1 Permutation operators

For each permutation $\pi \in S_n$, we define a unitary operator

$$W_\pi \in \mathrm{U}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right)$$

by the action

$$W_\pi(u_1 \otimes \cdots \otimes u_n) = u_{\pi^{-1}(1)} \otimes \cdots \otimes u_{\pi^{-1}(n)}$$

for every choice of vectors $u_1, \ldots, u_n \in \mathbb{C}^\Sigma$. In other words, W_π permutes the contents of the registers $\mathsf{X}_1, \ldots, \mathsf{X}_n$ according to π. It holds that

$$W_\pi W_\sigma = W_{\pi\sigma} \qquad \text{and} \qquad W_\pi^{-1} = W_\pi^* = W_{\pi^{-1}} \tag{22.1}$$

for all $\pi, \sigma \in S_n$.

22.1.2 The symmetric subspace

Some vectors in $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$ are invariant under the action of W_π for every choice of $\pi \in S_n$, and it holds that the set of all such vectors forms a subspace. This subspace is called the *symmetric subspace*, and will be denoted in these notes as $\mathcal{X}_1 \circledcirc \cdots \circledcirc \mathcal{X}_n$. In more precise terms, this subspace is defined as

$$\mathcal{X}_1 \circledcirc \cdots \circledcirc \mathcal{X}_n = \{u \in \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n \,:\, u = W_\pi u \text{ for every } \pi \in S_n\}.$$

One may verify that the orthogonal projection operator that projects onto this subspace is given by

$$\Pi_{\mathcal{X}_1 \circledcirc \cdots \circledcirc \mathcal{X}_n} = \frac{1}{n!} \sum_{\pi \in S_n} W_\pi.$$

Let us now construct an orthonormal basis for the symmetric subspace. First, consider the set $\mathrm{Urn}(n, \Sigma)$ of functions of the form $\phi : \Sigma \to \mathbb{N}$ (where $\mathbb{N} = \{0, 1, 2, \ldots\}$) that satisfy

$$\sum_{a \in \Sigma} \phi(a) = n.$$

The elements of this set describe *urns* containing n marbles, where each marble is labelled by an element of Σ. (There is no order associated with the marbles—all that matters is how many marbles with each possible label are contained in the urn. Urns are also sometimes called *bags*, and may alternately be described as multisets of elements of Σ having n items in total.)

Now, to say that a string $a_1 \cdots a_n \in \Sigma$ is *consistent* with a particular function $\phi \in \mathrm{Urn}(n, \Sigma)$ means simply that $a_1 \cdots a_n$ is one possible ordering of the marbles in the urn described by ϕ. One can express this formally by defining a function

$$f_{a_1 \cdots a_n}(b) = \big|\{j \in \{1, \ldots, n\} \,:\, b = a_j\}\big|,$$

and by defining that $a_1 \cdots a_n$ is consistent with ϕ if and only if $f_{a_1 \cdots a_n} = \phi$. The number of distinct strings $a_1 \cdots a_n \in \Sigma^n$ that are consistent with a given function $\phi \in \mathrm{Urn}(n, \Sigma)$ is given by the multinomial coefficient

$$\binom{n}{\phi} \triangleq \frac{n!}{\prod_{a \in \Sigma} (\phi(a)!)}.$$

Finally, we define an orthonormal basis of $\mathcal{X}_1 \circledcirc \cdots \circledcirc \mathcal{X}_n$ as $\{u_\phi \,:\, \phi \in \mathrm{Urn}(n, \Sigma)\}$, where

$$u_\phi = \binom{n}{\phi}^{-1/2} \sum_{\substack{a_1 \cdots a_n \in \Sigma^n \\ f_{a_1 \cdots a_n} = \phi}} e_{a_1} \otimes \cdots \otimes e_{a_n}.$$

In other words, u_ϕ is the uniform pure state over all of the strings that are consistent with the function ϕ.

For example, taking $n = 3$ and $\Sigma = \{0, 1\}$, we obtain the following four vectors:

$$\begin{aligned}
u_0 &= e_0 \otimes e_0 \otimes e_0 \\
u_1 &= \frac{1}{\sqrt{3}} \left(e_0 \otimes e_0 \otimes e_1 + e_0 \otimes e_1 \otimes e_0 + e_1 \otimes e_0 \otimes e_0\right) \\
u_2 &= \frac{1}{\sqrt{3}} \left(e_0 \otimes e_1 \otimes e_1 + e_1 \otimes e_0 \otimes e_1 + e_1 \otimes e_1 \otimes e_0\right) \\
u_3 &= e_1 \otimes e_1 \otimes e_1,
\end{aligned}$$

where the vectors are indexed by integers rather than functions $\phi \in \mathrm{Urn}(3, \{0,1\})$ in a straightforward way.

Using simple combinatorics, it can be shown that $|\mathrm{Urn}(n, \Sigma)| = \binom{n+d-1}{d-1}$, and therefore

$$\dim(\mathcal{X}_1 \circledcirc \cdots \circledcirc \mathcal{X}_n) = \binom{n+d-1}{d-1}.$$

Notice that for small d and large n, the dimension of the symmetric subspace is therefore very small compared with the entire space $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$.

It is also the case that

$$\mathcal{X}_1 \circledcirc \cdots \circledcirc \mathcal{X}_n = \mathrm{span}\left\{ u^{\otimes n} \,:\, u \in \mathbb{C}^{\Sigma} \right\}.$$

This follows from an elementary fact concerning the theory of symmetric functions, but I will not prove it here.

22.1.3 Exchangeable operators and their relation to the symmetric subspace

Along similar lines to vectors in the symmetric subspace, we say that a positive semidefinite operator $P \in \mathrm{Pos}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right)$ is *exchangeable* if it is the case that

$$P = W_\pi P W_\pi^*$$

for every $\pi \in S_n$.

It is the case that every positive semidefinite operator whose image is contained in the symmetric subspace is exchangeable, but this is not a necessary condition. For instance, the identity operator $\mathbb{1}_{\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n}$ is exchangeable and its image is all of $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$. We may, however, relate exchangeable operators and the symmetric subspace by means of the following lemma.

Lemma 22.1. *Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ and $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ be copies of the complex Euclidean space $\mathbb{C}^{\Sigma}$, and suppose that*

$$P \in \mathrm{Pos}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n\right)$$

is an exchangeable operator. There exists a symmetric vector

$$u \in (\mathcal{X}_1 \otimes \mathcal{Y}_1) \circledcirc \cdots \circledcirc (\mathcal{X}_n \otimes \mathcal{Y}_n)$$

that purifies P, i.e., $\mathrm{Tr}_{\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n}(uu^*) = P$.

Proof. Consider a spectral decomposition

$$P = \sum_{j=1}^{k} \lambda_j Q_j, \tag{22.2}$$

where $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of P and $Q_1, \ldots, Q_k$ are orthogonal projection operators onto the associated eigenspaces. As $W_\pi P W_\pi^* = P$ for each permutation $\pi \in S_n$, it follows that $W_\pi Q_j W_\pi^* = Q_j$ for each $j = 1, \ldots, k$, owing to the fact that the decomposition (22.2) is unique. The operator $\sqrt{P}$ is therefore also exchangeable, so that

$$(W_\pi \otimes W_\pi)\,\mathrm{vec}\left(\sqrt{P}\right) = \mathrm{vec}\left(W_\pi \sqrt{P} W_\pi^{\mathsf{T}}\right) = \mathrm{vec}\left(W_\pi \sqrt{P} W_\pi^*\right) = \mathrm{vec}\left(\sqrt{P}\right).$$

Now let us view the operator $\sqrt{P}$ as taking the form

$$\sqrt{P} \in \mathrm{L}\left(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n\right)$$

by identifying $\mathcal{Y}_j$ with $\mathcal{X}_j$ for $j = 1, \ldots, n$. We therefore have

$$\operatorname{vec}\left(\sqrt{P}\right) \in \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n \otimes \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n.$$

Let us take $u \in (\mathcal{X}_1 \otimes \mathcal{Y}_1) \otimes \cdots \otimes (\mathcal{X}_n \otimes \mathcal{Y}_n)$ to be equal to this vector, but with the tensor factors re-ordered in a way that is consistent with the names of the associated spaces. It holds that $\operatorname{Tr}_{\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n}(uu^*) = P$, and given that

$$(W_\pi \otimes W_\pi) \operatorname{vec}\left(\sqrt{P}\right) = \operatorname{vec}\left(\sqrt{P}\right)$$

for all $\pi \in S_n$ it follows that $u \in (\mathcal{X}_1 \otimes \mathcal{Y}_1) \circledcirc \cdots \circledcirc (\mathcal{X}_n \otimes \mathcal{Y}_n)$ as required. □

22.2 Integrals and unitarily invariant measure

For the proof of the main result in the next section, we will need to be able to express certain linear operators as integrals. Here is a very simple expression that will serve as an example for the sake of this discussion:

$$\int uu^* \, \mathrm{d}\mu(u).$$

Now, there are two very different questions one may have about such an operator:

1. What does it mean in formal terms?
2. How is it calculated?

The answer to the first question is a bit complicated—and although we will not have time to discuss it in detail, I would like to say enough to at least give you some clues and key-words in case you wish to learn more on your own.

In the above expression, μ refers to the normalized *unitarily invariant measure* defined on the Borel sets of the unit sphere $\mathcal{S} = \mathcal{S}(\mathcal{X})$ in some chosen complex Euclidean space $\mathcal{X}$. (The space $\mathcal{X}$ is implicit in the above expression, and generally would be determined by the context of the expression.) To say that μ is *normalized* means that $\mu(\mathcal{S}) = 1$, and to say that μ is *unitarily invariant* means that $\mu(\mathcal{A}) = \mu(U(\mathcal{A}))$ for every Borel set $\mathcal{A} \subseteq \mathcal{S}$ and every unitary operator $U \in \mathrm{U}(\mathcal{X})$. It turns out that there is only one measure with the properties that have just been described. Sometimes this measure is called *Haar measure*, although this term is considerably more general than what we have just described. (There is a uniquely defined Haar measure on many different sorts of measure spaces with groups acting on them in a particular way.)

Informally speaking, you may think of the measure described above as a way of assigning an infinitesimally small probability to each point on the unit sphere in such a way that no one vector is weighted more or less than any other. So, in an integral like the one above, we may view that it is an average of operators uu^* over the entire unit sphere, with each u being given equal weight. Of course it does not really work this way, which is why we must speak of Borel sets rather than arbitrary sets—but it is a reasonable guide for the simple uses of it in this lecture.

In formal terms, there is a process involving several steps for building up the meaning of an integral like the one above starting from the measure μ. It starts with characteristic functions for

Borel sets (where the value of the integral is simply the set's measure), then it defines integrals for positive linear combinations of characteristic functions in the obvious way, then it introduces limits to define integrals of more functions, and continues for a few more steps until we finally have integrals of operators. Needless to say, this process does not provide an efficient means to calculate a given integral.

This leads us to the second question, which is how to calculate such integrals. There is certainly no general method: just like ordinary integrals you are lucky when there is a closed form. For some, however, the fact that the measure is unitarily invariant leads to a simple answer. For instance, the integral above must satisfy

$$\int uu^* \, \mathrm{d}\mu(u) = U \left(\int uu^* \, \mathrm{d}\mu(u) \right) U^*$$

for every unitary operator $U \in \mathrm{U}(\mathcal{X})$, and must also satisfy

$$\mathrm{Tr}\left(\int uu^* \, \mathrm{d}\mu(u) \right) = \int \mathrm{d}\mu(u) = \mu(\mathcal{S}) = 1.$$

There is only one possibility:

$$\int uu^* \, \mathrm{d}\mu(u) = \frac{1}{\dim(\mathcal{X})} \mathbb{1}_{\mathcal{X}}.$$

Now, what we need for the next part of the lecture is a generalization of this fact—which is that for every $n \geq 1$ we have

$$\binom{n+d-1}{d-1} \int (uu^*)^{\otimes n} \, \mathrm{d}\mu(u) = \Pi_{\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n},$$

the projection onto the symmetric subspace. This is yet another fact for which a complete proof would be too much of a diversion at this point in the course. The main result we need is a fact from algebra that states that every operator in the space $\mathrm{L}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$ that commutes with $U^{\otimes n}$ for every unitary operator $U \in \mathrm{U}\left(\mathbb{C}^{\Sigma}\right)$ must be a linear combination of the operators $\{W_\pi : \pi \in S_n\}$. Given this fact, along with the fact that the operator expressed by the integral has the correct trace and is invariant under multiplication by every W_π, the proof follows easily.

22.3 The quantum de Finetti theorem

Now we are ready to state and prove (one variant of) the quantum de Finetti theorem, which is the main goal of this lecture. The statement and proof follow.

Theorem 22.2. *Let $\mathsf{X}_1, \ldots, \mathsf{X}_n$ be identical quantum registers, each having associated space $\mathbb{C}^{\Sigma}$ for $|\Sigma| = d$, and let $\rho \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$ be an exchangeable density operator representing the state of these registers. For any choice of $k \in \{1, \ldots, n\}$, there exists a finite set Γ, a probability vector $p \in \mathbb{R}^{\Gamma}$, and a collection of density operators $\{\xi_a : a \in \Gamma\} \subset \mathrm{D}\left(\mathbb{C}^{\Sigma}\right)$ such that*

$$\left\| \rho^{\mathsf{X}_1 \cdots \mathsf{X}_k} - \sum_{a \in \Gamma} p(a) \xi_a^{\otimes k} \right\|_1 < \frac{4d^2 k}{n}.$$

Proof. First we will prove a stronger bound for the case where $\rho = vv^*$ is pure (which requires $v \in \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$). This will then be combined with Lemma 22.1 to complete the proof.

For the sake of clarity, let us write $\mathcal{Y} = \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k$ and $\mathcal{Z} = \mathcal{X}_{k+1} \otimes \cdots \otimes \mathcal{X}_n$. Let us also write

$$S^{(m)} = \binom{m+d-1}{d-1} \int (uu^*)^{\otimes m} \, \mathrm{d}\mu(u),$$

which is the projection onto the symmetric subspace of m copies of $\mathbb{C}^\Sigma$ for any choice of $m \geq 1$.

Now consider a unit vector $v \in \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$. As v is invariant under every permutation of its tensor factors, it holds that

$$v = \left(\mathbb{1}_{\mathcal{Y}} \otimes S^{(n-k)}\right) v.$$

Therefore, for $\sigma \in \mathrm{D}(\mathcal{Y})$ defined as $\sigma = \mathrm{Tr}_{\mathcal{Z}}(vv^*)$ we must have

$$\sigma = \mathrm{Tr}_{\mathcal{Z}} \left(\left(\mathbb{1}_{\mathcal{Y}} \otimes S^{(n-k)}\right) vv^* \right).$$

Defining a mapping $\Phi_u \in \mathrm{T}(\mathcal{Y} \otimes \mathcal{Z}, \mathcal{Y})$ for each vector $u \in \mathbb{C}^\Sigma$ as

$$\Phi_u(X) = \left(\mathbb{1}_{\mathcal{Y}} \otimes u^{\otimes(n-k)}\right)^* X \left(\mathbb{1}_{\mathcal{Y}} \otimes u^{\otimes(n-k)}\right)$$

for every $X \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{Z})$, we have

$$\sigma = \binom{n-k+d-1}{d-1} \int \Phi_u(vv^*) \, \mathrm{d}\mu(u).$$

Now, our goal is to approximate σ by a density operator taking the form

$$\sum_{a \in \Gamma} p(a) \xi_a^{\otimes k},$$

so we will guess a suitable approximation:

$$\tau = \binom{n+d-1}{d-1} \int \left\langle (uu^*)^{\otimes k}, \Phi_u(vv^*) \right\rangle (uu^*)^{\otimes k} \, \mathrm{d}\mu(u).$$

It holds that τ has trace 1, because

$$\mathrm{Tr}(\tau) = \binom{n+d-1}{d-1} \int \left\langle (uu^*)^{\otimes n}, vv^* \right\rangle \mathrm{d}\mu(u) = \left\langle S^{(n)}, vv^* \right\rangle = 1,$$

and τ also has the correct form:

$$\tau \in \mathrm{conv} \left\{ (ww^*)^{\otimes k} \,:\, w \in \mathcal{S}\left(\mathbb{C}^\Sigma\right) \right\}.$$

(It is intuitive that this should be so, but we have not proved it formally. Of course it can be proved formally, but it requires details about measure and integration beyond what we have discussed.)

We will now place an upper bound on $\|\sigma - \tau\|_1$. To make the proof more readable, let us write

$$c_m = \binom{m+d-1}{d-1}$$

for each $m \geq 0$. We begin by noting that

$$\|\sigma - \tau\|_1 \leq \left\| \sigma - \frac{c_{n-k}}{c_n}\tau \right\|_1 + \left\| \frac{c_{n-k}}{c_n}\tau - \tau \right\|_1 = c_{n-k} \left\| \frac{1}{c_{n-k}}\sigma - \frac{1}{c_n}\tau \right\|_1 + \left(1 - \frac{c_{n-k}}{c_n}\right). \tag{22.3}$$

Next, by making use of the operator equality

$$A - BAB = A(\mathbb{1} - B) + (\mathbb{1} - B)A - (\mathbb{1} - B)A(\mathbb{1} - B),$$

and writing $\Delta_u = (uu^*)^{\otimes k}$, we obtain

$$\begin{aligned}
\left\| \frac{1}{c_{n-k}}\sigma - \frac{1}{c_n}\tau \right\|_1 &= \left\| \int (\Phi_u(vv^*) - \Delta_u \Phi_u(vv^*)\Delta_u)\, \mathrm{d}\mu(u) \right\|_1 \\
&\leq \left\| \int \Phi_u(vv^*)(\mathbb{1} - \Delta_u)\, \mathrm{d}\mu(u) \right\|_1 + \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)\, \mathrm{d}\mu(u) \right\|_1 \\
&\quad + \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)(\mathbb{1} - \Delta_u)\, \mathrm{d}\mu(u) \right\|_1.
\end{aligned}$$

It holds that

$$\left\| \int \Phi_u(vv^*)(\mathbb{1} - \Delta_u)\, \mathrm{d}\mu(u) \right\|_1 = \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)\, \mathrm{d}\mu(u) \right\|_1,$$

while

$$\begin{aligned}
\left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)(\mathbb{1} - \Delta_u)\, \mathrm{d}\mu(u) \right\|_1 &= \mathrm{Tr} \left(\int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)(\mathbb{1} - \Delta_u)\, \mathrm{d}\mu(u) \right) \\
&= \mathrm{Tr} \left(\int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)\, \mathrm{d}\mu(u) \right) \\
&\leq \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)\, \mathrm{d}\mu(u) \right\|_1.
\end{aligned}$$

Therefore we have

$$\left\| \frac{1}{c_{n-k}}\sigma - \frac{1}{c_n}\tau \right\|_1 \leq 3 \left\| \int (\mathbb{1} - \Delta_u)\Phi_u(vv^*)\, \mathrm{d}\mu(u) \right\|_1.$$

At this point we note that

$$\int \Phi_u(vv^*)\, \mathrm{d}\mu(u) = \frac{1}{c_{n-k}}\sigma$$

while

$$\int \Delta_u \Phi_u(vv^*)\, \mathrm{d}\mu(u) = \mathrm{Tr}_{\mathcal{Z}} \int (uu^*)^{\otimes n} vv^*\, \mathrm{d}\mu(u) = \frac{1}{c_n}\sigma.$$

Therefore we have

$$\left\| \frac{1}{c_{n-k}}\sigma - \frac{1}{c_n}\tau \right\|_1 \leq 3 \left(\frac{1}{c_{n-k}} - \frac{1}{c_n} \right),$$

and so

$$\|\sigma - \tau\|_1 \leq 3\, c_{n-k} \left(\frac{1}{c_{n-k}} - \frac{1}{c_n} \right) + \left(1 - \frac{c_{n-k}}{c_n} \right) = 4 \left(1 - \frac{c_{n-k}}{c_n} \right).$$

To finish off the upper bound, we observe that

$$\frac{c_{n-k}}{c_n} = \frac{(n-k+d-1)(n-k+d-2)\cdots(n-k+1)}{(n+d-1)(n+d-2)\cdots(n+1)} \geq \left(\frac{n-k+1}{n+1}\right)^{d-1} > 1 - \frac{dk}{n},$$

and so

$$\|\sigma - \tau\|_1 < \frac{4dk}{n}.$$

This establishes essentially the bound given in the statement of the theorem, albeit only for pure states, but with d^2 replaced by d.

To prove the bound in the statement of the theorem for an arbitrary exchangeable density operator $\rho \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$, we first apply Lemma 22.1 to obtain a symmetric purification

$$v \in (\mathcal{X}_1 \otimes \mathcal{Y}_1) \circledcirc \cdots \circledcirc (\mathcal{X}_n \otimes \mathcal{Y}_n)$$

of ρ, where $\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ represent isomorphic copies of $\mathcal{X}_1, \ldots, \mathcal{X}_n$. By the argument above, we have

$$\|\sigma - \tau\|_1 < \frac{4d^2k}{n},$$

where $\sigma = \mathrm{Tr}_{\mathcal{Z}}(vv^*)$ for $\mathcal{Z} = (\mathcal{X}_{k+1} \otimes \mathcal{Y}_{k+1}) \otimes \cdots \otimes (\mathcal{X}_n \otimes \mathcal{Y}_n)$ and where

$$\tau \in \mathrm{conv}\left\{(uu^*)^{\otimes k} \,:\, u \in \mathcal{S}\left(\mathbb{C}^\Sigma \otimes \mathbb{C}^\Sigma\right)\right\}.$$

Taking the partial trace over $\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_k$ then gives the result. □