OPERATOR ALGEBRA METHODS IN QIT
WINTER 2020

VERN I. PAULSEN

Abstract. These notes are to accompany the course QIC890/PMATH950

1. Introduction

Broad Goals: What are C*-algebras, operator systems, operator spaces, cp maps, cb maps and how are they useful in QIT?

Specifics:

- Quick review of Hilbert spaces and operator theory.
- Brief introduction to states, measurement systems, density matrices and the quantum channel induced by a measurement system.
- Axiomatic definition of QC and proof that every QC induced by a measurement system with possibly infinitely many outcomes.
- Introduction to C*-algebras and Matrix Order.
- CP maps and Stinespring's theorem
- Other C*-algebras in QI and von Neumann algebras.
- Non-local games, families of POVM's and free group C*-algebras.
- Quantum spin chains and infinite tensor products.
- Operator systems, Arveson's extension theorem and quantum marginals.
- Knill-Laflamme protected subsystems
- One-shot zero error capacity
- Entanglement breaking and positive partial transpose maps
- Operator spaces and CB maps, Wittstock's decomposition, dual spaces and the diamond norm.

2. Hilbert Spaces

All vector spaces will be over $\mathbb{C}$ unless specified otherwise. Given a vector space V a map $B : V \times V \to \mathbb{C}$ is **sesquilinear** provided:

- $B(v_1 + v_2, w) = B(v_1, w) + B(v_2, w)$
- $B(v, w_1 + w_2) = B(v, w_1) + B(v, w_2)$,
- $\forall \lambda \in \mathbb{C},\ B(\lambda v, w) = \overline{B}(v, w),\ B(v, \lambda w) = \lambda B(v, w)$.

We call B **positive semidefinite** provided that $B(v, v) \geq 0, \forall v \in V$ and **positive**(or **positive definite**) provided that $B(v, v) > 0$ for all $v \neq 0$. A positive sesquilinear map is called an **inner product** and in this case we generally write

$$B(v, w) = \langle v|w\rangle.$$

Proposition 2.1 (Cauchy-Schwartz Inequality)**.** *Let $B : V \times V \to \mathbb{C}$ be sesquilinear and positive semidefinite, then $B(v,w) = \overline{B(w,v)}$ and*

$$|B(v,w)|^2 \leq B(v,v)B(w,w).$$

Corollary 2.2. *Let $B : V \times V \to \mathbb{C}$ be positive semidefinite and sesquilinear, then*

- *$\{x : B(x,x) = 0\} = \{x : B(x,w) = 0 \forall w\}$ is a subspace of V that we denote by $\mathcal{N}$,*
- *there is a well-defined inner product on the quotient space $V/\mathcal{N}$ given by*

$$\dot{B}\,(x + \mathcal{N}, y + \mathcal{N}) = B(x,y).$$

Givne an inner product on V if we set

$$\|v\| = \langle v|v\rangle^{1/2},$$

then this is a norm on V. When $(V, \|\cdot\|)$ is a complete normed space with respect to the norm coming from an inner product then we call V a **Hilbert space**.

If V is a HIlbert space then a set of vectors S is called **orthonormal(o.n.)** provided that $v \in S \implies \|v\| = 1$ and $v, w \in S, v \neq w \implies \langle v|w\rangle = 0$. A set S is called an **orthonormal basis(o.n.b.)** provided that it is an orthonormal set and it is maximal among all orthonormal sets. i.e., $S \subseteq T$ and T also o.n. implies that $S = T$.

Theorem 2.3 (Parseval)**.** *Let $\mathcal{H}$ be a HIlbert space, $\{e_a : a \in A\}$ an o.n.b., then for any $h \in \mathcal{H}$,*

(1) $\|h\|^2 = \sum_{a \in A} |\langle e_a|h\rangle|^2$,
(2) $h = \sum_{a \in A} \langle e_a|h\rangle e_a$.

We need to explain what these unordered sums mean. For example 2) means that given $\epsilon > 0$ there exists a finite set $F_0 \subseteq A$ such that if F is any finite set with $F_0 \subseteq F \subseteq A$, then

$$\|h - \sum_{a \in F} \langle e_a|h\rangle e_a\| < \epsilon.$$

While 1) gives that for any $\epsilon > 0$ there is a finite set F_0 such that for any finite set F, $F_0 \subseteq F \subseteq A$ we have that

$$0 \leq \|h\|^2 - \sum_{a \in F} |\langle e_a|h\rangle|^2 < \epsilon.$$

A good example to keep in mind is that

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n},$$

converges while

$$\sum_{n \in \mathbb{N}} \frac{(-1)^n}{n},$$

does not converge.

Proposition 2.4 (Hilbert Space Dimension)**.** *Let $\mathcal{H}$ be a HIlbert space and let $\{e_a : a \in A\}$ and $\{f_b : b \in B\}$ be two o.n.b.'s for $\mathcal{H}$. Then there is a one-to-one, onto function,*

$$g : A \to B.$$

The existence of such a function g is the definition of what it means for the sets A and B to have the same **cardinality**. So this statement is also written as

$$card(A) = card(B),$$

and we denote this number by $dim(\mathcal{H})$ or sometimes $dim_{HS}(\mathcal{H})$. We will sometimes use the following.

Proposition 2.5. *Let $\mathcal{H}$ be a Hilbert space. Then $\mathcal{H}$ ha an o.n.b. that is at most countable if and only if $\mathcal{H}$ is separable as a metric space, i.e., has a countable dense subset.*

2.1. **Direct Sums.** Given two Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, we set

$$\mathcal{H} \oplus \mathcal{K} = \{(h, k) : h \in \mathcal{H}, k \in \mathcal{K}\}.$$

This is a vector space with $(h_1, k_1) + (h_2, k_2) = (h_1 + h_2, k_1 + k_2)$, and $\lambda(h, k) = \lambda h, \lambda k)$. If we set

$$\langle (h_1, k_1) | (h_2, k_2) \rangle = \langle h_1 | h_2 \rangle_{\mathcal{H}} + \langle k_1 | k_2 \rangle_{\mathcal{K}},$$

then this is an inner product that makes the vector space $\mathcal{H} \oplus \mathcal{K}$ into a Hilbert space, called the **direct sum**. Note that

$$dim(\mathcal{H} \oplus \mathcal{K}) = dim(\mathcal{H}) + dim(\mathcal{K}),$$

which justifies the notation a bit.

We set

$$\mathcal{H}^{(n)} := \mathcal{H} \oplus \mathcal{H} \oplus \cdots \mathcal{H}(n\, copies),$$

which denotes the direct sum of n copies of $\mathcal{H}$ with itself. When we want to form a direct sum of infinitely many copies of $\mathcal{H}$ with itself we cannot use all posible tuples, because the inner products would not converge. Instead we set

$$\mathcal{H}^{(\infty)} := \{(h_1, h_2, \ldots) : h_n \in \mathcal{H} \text{ and } \sum_{n \in \mathbb{N}} \|h_n\|^2 < +\infty\},$$

with inner product,

$$\langle (h_1, h_2, \ldots) | (k_1, k_2, \ldots) \rangle := \sum_{n \in \mathbb{N}} \langle h_n | k_n \rangle.$$

2.2. **Tensor Products.** Given two Hilbert spaces, $\mathcal{H}$ and $\mathcal{K}$, let $\mathcal{H} \otimes \mathcal{K}$ denote the tensor product of these two vector spaces. Given $u = \sum_{i=1}^{n} h_i \otimes k_i$ and $v = \sum_{j=1}^{k} x_j \otimes y_j$ in $\mathcal{H} \otimes \mathcal{K}$, we set

$$\langle u|v\rangle = \sum_{i,j=1}^{n,k} \langle h_i|x_j\rangle_{\mathcal{H}} \cdot \langle k_i|y_j\langle_{\mathcal{K}}.$$

This turns out to define an inner product. If one of the two Hilbert spaces is finite dimensional, then this space is already complete in this inner product, but when they are both infinite dimensional, this space is not complete. However, we still use $clH \otimes \mathcal{K}$ to denote the Hilbert space that is the completion. (Some authors prefer to use $\mathcal{H} \otimes \mathcal{K}$ for the vector space tensor product and $\mathcal{H} \overline{\otimes} \mathcal{K}$ for the completion. Other authors use $\mathcal{H} \odot \mathcal{K}$ for the vector space tensor product and $\mathcal{H} \otimes \mathcal{K}$ for its completon.)

Te following summarizes some of the key properties of the tensor product.

Theorem 2.6. *Let $\mathcal{H}$ and $\mathcal{K}$ be Hilbert spaces.*

1. *If $\{e_a; a \in A\}$ is an o.n.b. for $\mathcal{H}$ and $\{f_b : b \in B\}$ is an o.n.b. for $\mathcal{K}$, then $\{e_a \otimes f_b : a \in A, b \in B\}$ is an o.n.b. for $\mathcal{H} \otimes \mathcal{K}$.*
2. *$dim(\mathcal{H} \otimes \mathcal{K}) = dim(\mathcal{H}) \cdot dim(\mathcal{K})$.*
3. *Given $u \in \mathcal{H} \otimes \mathcal{K}$ there exist unique vectors $h_h \in \mathcal{H}$ such that*

$$u = \sum_{b \in B} h_b \otimes f_b.$$

Similarly, there exist unique vectors $k_a \in \mathcal{K}$ such that

$$u = \sum_{a \in A} e_a \otimes k_a.$$

Also,

$$\|u\|^2 = \sum_{b \in B} \|h_b\|^2 = \sum_{a \in A} \|k_a\|^2.$$

2.3. **Identifying direct Sums and Tensor Products.** We shall often use the following identification. Let $\mathcal{H}$ be a Hilbert space and let $\mathbb{C}^n$ be the usual n dimensional Hilbert space. Fix some o.n.b. for $\mathbb{C}^n$, $f_1, ..., f_n$. We define

$$U : \mathcal{H}^{(n)} \to \mathcal{H} \otimes \mathbb{C}^n,$$

by setting

$$U((h_1, ..., h_n)) = \sum_{j=1}^{n} h_j \otimes f_j.$$

This map is one-to-one, onto and **inner product preserving**, namely

$$\langle U(h_1, ..., h_n))|U((k_1, ..., k_n))\rangle_{\mathcal{H} \otimes \mathbb{C}_n} = \sum_{j=1}^{n} \langle h_j|k_j\rangle_{\mathcal{H}} = \langle (h_1, ..., h_n)|(k_1, ..., k_n)\rangle_{\mathcal{H}^{(n)}}.$$

Thus, as Hilbert spaces these spaces are identical. The map U is an example of a unitary map, which we shall discuss more later.

2.4. **Subspaces.** Let $\mathcal{H}$ be a HIlbert space and let $\mathcal{M} \subseteq \mathcal{H}$ be a vector subspace that is also closed in the norm topology. In this case $\mathcal{M}$ is also a Hilbert space. If we set

$$\mathcal{M}^{\perp} := \{h \in \mathcal{H} : \langle h|m\rangle = 0, \forall m \in \mathcal{M}\},$$

then $\mathcal{M}^{\perp}$ is also a closed vector subspace of $\mathcal{H}$. Moreover, every $h \in \mathcal{H}$ has a unique decomposition as $h = m + n$ with $m \in \mathcal{M}$ and $n \in \mathcal{M}^{\perp}$.

2.5. **Bra–ket Notation.** Generally, when we have a vector in $\mathbb{C}^n$, for ease of typing, we write it as a row vector $v = (x_1, ..., x_n)$, yet when we think of vectors and matrices we actually need v to be a column vector. For this reason, matrix theorists really like to think of vectors as columns. Also given another vector $w = (y_1, ..., y_n)$, the inner product is

$$\langle w|v\rangle = \sum_{i=1}^{m} \overline{y_i} x_i.$$

Note that if we do think of v and w as columns, $v = (x_1, ..., x_n)^t$ and $w = (y_1, ..., y_n)^t$ where t denotes the transpose, then the inner product is:

$$\langle w|v\rangle = w^* v,$$

where of course $w^* = (\overline{y_1}, ..., \overline{y_n})$ is the **conjugate transpose** of the column vector w. The fact that matrix theory really wants vectors to be columns is also why we like to have our inner product conjugate linear on the left. If we had made it conjugate linear on the right, then we would have had $\langle w|v\rangle = v^* w$!

Physicists get around this ambiguity with their bra-ket notation. Formally, they always denote vectors by $|v\rangle$, called the "ket of v", and the linear functional

$$f_w : \mathcal{H} \to \mathbb{C},\ f_w(v) = \langle w|v\rangle,$$

induced by the vector w as $\langle w|$, called the "bra of w". This makes the inner product,

$$\langle w||v\rangle.$$

In my notation, $|v\rangle = v$ and $\langle w| = f_w = w^*$.

3. Operator Theory

Let $\mathcal{H}$ and $\mathcal{K}$ denote Hilbert spaces. We let $B(\mathcal{H},\mathcal{K})$ denote the set of **bounded**, linear maps from $\mathcal{H}$ to $\mathcal{K}$. Recall that $T:\mathcal{H}\to\mathcal{K}$ bounded means that,

$$\|T\| := \sup\{\|Th\|_{\mathcal{K}} : h\in\mathcal{H}, \|h\|_{\mathcal{H}}=1\} = \sup\{\frac{\|Th\|_{\mathcal{K}}}{\|h\|_{\mathcal{H}}} : h\neq 0\} < +\infty.$$

When $\mathcal{H}=\mathcal{K}$, we abbreviate, $B(\mathcal{H},\mathcal{H}) = B(\mathcal{H})$.

Given $T:\mathbb{C}^d\to\mathbb{C}^r$ we can always represent T as multiplication by an $r\times d$ matrix $(t_{i,j})$ where

$$t_{i,j} = \langle e_i|Te_j\rangle.$$

A useful bound is that

$$\|T\| \leq \big(\sum_{j=1}^{d}\sum_{i=1}^{r}|t_{i,j}|^2\big)^{1/2} := \|T\|_2,$$

where this latter quantity is the norm of the matrix viewed as a vector in the Hilbert space $\mathbb{C}^{rd}$.

3.1. **Adjoint.** Given $T\in B(\mathcal{H},\mathcal{K})$ there is a unique operator $R\in B(\mathcal{K},\mathcal{H})$ satisfying

$$\langle k|Th\rangle_{\mathcal{K}} = \langle Rk|h\rangle_{\mathcal{H}}.$$

This operator is called the **adjoint of T** and is denoted by $T^* := R$.

When T is represented by the matrix $(t_{i,j})$, then T^* is represented by the matrix that is the conjugate, transpose, $T^* = (\overline{t_{j,i}})$.

There are several different types of operators that play an important role. We review their names and some characterizations.

$V\in B(\mathcal{H},\mathcal{K})$ is an **isometry** provided $\|Vh\|_{\mathcal{K}} = \|h\|_{\mathcal{H}}, \forall h\in\mathcal{H}$.

Proposition 3.1. *T.F.A.E.*

1. *V is an isometry,*
2. *V is* **inner product preserving**, *i.e.,*

$$\langle Vh_1|Vh_2\rangle_{\mathcal{K}} = \langle h_1|h_2\rangle_{\mathcal{H}}, \forall h_1,h_2\in\mathcal{H},$$

3. *$V^*V = I_{\mathcal{H}}$.*

A map $U\in B(\mathcal{H},\mathcal{K})$ is called a **unitary** provided U is an isometry and is onto.

Proposition 3.2. *T.F.A¿E.*

1. *U is a unitary,*
2. *U and U^* are isometries,*
3. *$U^*U = I_{\mathcal{H}}$ and $UU^* = I_{\mathcal{K}}$.*
4. *U is invertible and $U^{-1} = U^*$.*

A map $H \in B(\mathcal{H})$ is called **Hermitian** or **self-adjoint** provided that $H = H^*$.

A map $N \in B(\mathcal{H})$ is called **normal** provided that $NN^* = N^*N$.

A map $P \in B(\mathcal{H})$ is called a **projection** provided that there is a closed subspace $\mathcal{M} \subseteq \mathcal{H}$ such that $Ph = m$ where $h = m + n$, $m \in \mathcal{M}, n \in \mathcal{M}^\perp$ is the unique decomposition of h.

Given $T \in B(\mathcal{H}, \mathcal{K})$ we set

$$\mathcal{R}(T) = \{Th : h \in \mathcal{H}\},$$

which is a subspace of $\mathcal{K}$ that we call the **range** of T.

Proposition 3.3. *P is a projection if and only if $P = P^* = P^2$ and in this case $\mathcal{M} = \mathcal{R}(P)$*

A map $F \in B(\mathcal{H}, \mathcal{K})$ is called **finite rank** provided that $\mathcal{R}(F)$ is finite dimensional.

Proposition 3.4. *F is finite rank if and only if there exist finitely many vectors, $h_1, ..., h_n \in \mathcal{H}$ and $k_1, ..., k_n \in \mathcal{K}$ such that*

$$Fh = \sum_{i=1}^{n} \langle h_i | h \rangle k_i.$$

In bra-ket notation, $F = \sum_{i=1}^{n} |k_i\rangle \langle h_i|$.

Back to matrices. If $h = (\alpha_1, ..., \alpha_n)^t \in \mathbb{C}^n$ and $k = (\beta_1, ..., \beta_m)^t \in \mathbb{C}^m$ then

$$kh^* = |k\rangle \langle h| = (\beta_i \overline{\alpha_j}),$$

which is an $m \times n$ rank one matrix.

When $\|h\| = 1$, then

$$hh^* = |h\rangle \langle h| = (\alpha_i \overline{\alpha_j}),$$

is the rank one projection onto the span of h. If $\{v_1, ..., v_n\}$ are orthonormal, then

$$\sum_{i=1}^{n} v_i v_i^* = \sum_{i=1}^{n} |v_i\rangle \langle v_i| ,$$

is the projection onto the n-dimensional subspace that they span.

A map $K \in B(\mathcal{H}, \mathcal{K})$ is called **compact** provided that there is a sequence of finite rank operators $F_n \in B(\mathcal{H}, \mathcal{K})$ such that

$$\lim_n \|K - F_n\| = 0.$$

We let $\mathbb{K}(\mathcal{H}, \mathcal{K})$ denote the set of compact operators from $\mathcal{H}$ to $\mathcal{K}$.

Proposition 3.5. *The set $\mathbb{K}(\mathcal{H}, \mathcal{K}) \subseteq B(\mathcal{H}, \mathcal{K})$ is closed subspace in the operator norm. If $T \in B(\mathcal{H}), K \in \mathbb{K}(\mathcal{H}, \mathcal{K})$ and $R \in B(\mathcal{K})$, then $RKT \in \mathbb{K}(\mathcal{H}, \mathcal{K})$.*

3.2. **Spectrum and Functional Calculus.** If $T \in B(\mathcal{H})$ with $\mathcal{H}$ infinite dimensional, then it is possible that T has no eigenvalues even when $T = T^*$.

For example, if

$$\mathcal{H} = \ell^2_{\mathbb{N}} := \{(a_1, a_2, ...) : \sum_{n\in\mathbb{N}} |a_n|^2 < +\infty\},$$

then this space has an o.n.b. given by $\{e_n : n \in \mathbb{N}\}$ where e_n is the vector that is 1 in the n-th coordinate and 0 elsewhere. The operator defined by

$$Se_n = e_{n+1}$$

is called the **forward unilateral shift** and it is easy to show that it has no non-zero eigenvector. However it's adjoint, S^* is the **backwards unilateral shift** and satisfies

$$S^*e_n = \begin{cases} 0 & n = 1 \\ e_{n-1} & n > 1 \end{cases}.$$

Given $\lambda \in \mathbb{C}$, $|\lambda| < 1$, if we set

$$v_\lambda = (1, \lambda, \lambda^2, ...) = \sum_{n\in\mathbb{N}} \lambda^{n-1} e_n,$$

then $S^*v_\lambda = \lambda v_\lambda$. Thus, although S has no eigenvectors, there is an eigenvector for S^* for every point in the open unit disk.

In infinite dimensions the spectrum plays the role of the eigenvectors. Given $T \in B(\mathcal{H})$ the **spectrum of T** is the set

$$\sigma(T) = \{\lambda \in \mathbb{C} | \ (T - \lambda I_{\mathcal{H}}) \text{ is not invertible } \}.$$

Theorem 3.6. *Let $T \in B(\mathcal{H})$, then $\sigma(T)$ is a non-empty compact set and*

$$\sigma(T) \subseteq \{\lambda \in \mathbb{C} : \ |\lambda| \leq \|T\|\}.$$

In fact,

$$\sup\{|\lambda| : \lambda \in \sigma(T)\} = \lim_n \|T^n\|^{1/n}.$$

This last equation is called the **spectral radius formula**.

Here are a few other facts about the spectrum that we shall often use. Given a polynomial, $p(z) = a_0 + a_1 z + \cdots + a_n z^n$ and $T \in B(\mathcal{H})$ we set $p(T) = a_0 I_{\mathcal{H}} + a_1 T + \cdots + a_n T^n$.

Theorem 3.7. *Let $T \in B(\mathcal{H})$.*

1. *$\sigma(p(T)) = \{p(\lambda) : \lambda \in \sigma(T)\}$.*
2. *If $T = T^*$, then $\sigma(T) \subseteq \mathbb{R}$.*
3. *If U is a unitary, then $\sigma(U) \subseteq \{\lambda : \ |\lambda| = 1\}$*

3.3. **The Continuous Functional Calculus for a Hermitian Operator.** Given a function $f : S \to \mathbb{C}$ we set

$$\|f\|_\infty = \sup\{|f(x)|;\, x \in S\}.$$

Of course, this norm depends on the domain of the function but this will always be clear from the context.

Proposition 3.8. *Let $H \in B(\mathcal{H}), H = H^*$. Then for every polynomial,*

$$\|p(H)\| = \sup\{|p(\lambda)| :\, \lambda \in \sigma(H)\}.$$

Thus, $\|p(H)\| = \|p\|_\infty$ where p is viewed as a function on $\sigma(H)$.

Let $C(\sigma(H))$ denote the set of continuous functions on $\sigma(H) \subseteq \mathbb{R}$. Recall by the Stone-Weierstrass theorem that the polynomials are dense in this set in $\|\cdot\|_\infty$. So given any continuous function f there is a sequence of polynomial $\{p_n\}$ with $\lim_n \|f - p_n\|_\infty = 0$. From this it follows that this sequence is Cauchy in norm, i.e., given $\epsilon > 0$, for m, n sufficiently large, $\|p_n - p_m\|_\infty < \epsilon$. But this means that the operators $\{p_n(H)\}$ are also Cauchy in norm, since

$$\|p_n(H) - p_m(H)\| = \|p_n - p_m\|_\infty.$$

Hence, there will be an operator there will be an operator to which they converge and this operator is denoted by $f(H)$.

Thus, for each $f \in C(\sigma(H))$ we have an operator $f(H)$. We summarize a few of the properties of this construction below.

Theorem 3.9 (The Continuous Functional Calculus for a Self-Adjoint Operator)**.** *Let $H \in B(\mathcal{H}), H = H^*$. Then for every continuous function f on $\sigma(H)$, i.e., $f \in C(\sigma(H))$ there is an operator $f(H)$ these satisfy:*

- $\|f(H)\| = \|f\|_\infty$,
- $\sigma(f(H)) = \{f(\lambda) :\, \lambda \in \sigma(H)\}$,
- $f, g \in C(\sigma(H)) \implies (fg)(H) = f(H)g(H),\ (f+g)(H) = f(H) + g(H)$.

3.4. **Positive Operators.** An operator $P \in B(\mathcal{H})$ is **positive**, denoted $P \geq 0$ provided that

$$\langle h|Ph\rangle \geq 0,\ \forall h \in \mathcal{H}.$$

Proposition 3.10. *T.F.A.E.*

- $P \geq 0$,
- $P = P^*$ *and* $\sigma(P) \subseteq [0, +\infty)$,
- $\exists X \in B(\mathcal{H})$ *such that* $P = X^*X$.

Given $T \in B(\mathcal{H}, \mathcal{K})$ we use the continuous functional calculus tp define

$$|T| = (T^*T)^{1/2}.$$

Note that, unlike numbers, generally, $|T| \neq |T^*|$.

Define continuous functions $f_+, f_- : \mathbb{R} \to \mathbb{R}$ by

$$f_+(t) = \begin{cases} t & t \geq 0 \\ 0 & t < 0 \end{cases} \text{ and } f_-(t) = \begin{cases} 0 & t \geq 0 \\ -t & t < 0 \end{cases}.$$

If $H = H^*$ then we apply the continuous functional calculus to define $H^+ = f_+(H)$ and $H^- = f_-(H)$ and we see that

- $H^+ \geq 0,\ H^- \geq 0,$
- $H = H^+ - H^-$
- $|H| = H^+ + H^-,$
- $H^+H^- = 0.$

Theorem 3.11 (Polar Decomposition)**.** *Let $T \in B(\mathcal{H}, \mathcal{K})$, then there exists a unique unitary $W : \mathcal{R}(|T|)^- \to R(T)^-$ such that $T = W|T|$.*

The proof essentially follows from the fact that

$$\|Th\|^2 = \langle Th|Th\rangle = \langle h|T^*Th\rangle = \langle h||T|^2h\rangle = \langle |T|h||t|h\rangle = \||T|h\|^2.$$

We can always extend W to an operator $\hat{W} : \mathcal{H} \to \mathcal{K}$ by setting $\hat{W}$ equal to 0 on $\mathcal{R}(|T|)^\perp$, i.e.,

$$\hat{W}(|T|h + k) = Th,\ \forall k \in \mathcal{R}(|T|)^\perp$$

and we will still have $T = \hat{W}|T|$. This latter factorization is sometimes what is meant by the polar decomposition.

Moreover, if $dim(\mathcal{R}(|T|)^\perp) = dim(\mathcal{R}(T)^\perp)$ then one can also extend W to be a unitary $U : \mathcal{H} \to \mathcal{K}$ with $T = U|T|$. When $\mathcal{H} = \mathcal{K} = \mathbb{C}^n$, this is always the case, so we may always factor a $n \times n$ matrix T as $T = U|T|$ with U a unitary.

4. More about $\mathbb{K}(\mathcal{H})$

Theorem 4.1 (Positive Compact Operators)**.** *Let $P \in \mathbb{K}(\mathcal{H})$ with $P \geq 0$. Then there exists an o.n.b. $\{\psi_a : a \in A\}$ for $\mathcal{H}$ consisting of eigenvectors for P. Moreover, at most countably many of the corresponding eigenvalues are non-zero and we may arrange the non-zero eigenvalues in a decreasing sequence, $\lambda_1 \geq \lambda_2 \geq ...$ with either at most finitely many eigenvalues non-zero or $\lim_n \lambda_n = 0$.*

Given P as above, set $F_N = \sum_{n=1}^N \lambda_n |\psi_n\rangle \langle\psi_n|$. Then $F_N \geq 0$ and is finite rank, with

$$\|P - F_N\| = \lambda_{N+1} \to 0 \text{ as } N \to +\infty.$$

Thus, we may write

$$P = \sum_{n=1}^{\infty} \lambda_n |\psi_n\rangle \langle\psi_n|,$$

and the converge of this series is in the norm.

Given any $K \in \mathbb{K}(\mathcal{H}, \mathcal{K})$ by the polar decomposition we have that $K = W|K|$ and $|K| \geq 0$ and compact. The non-zero eigenvalues of $|K|$ written

in decreasing order $\lambda_1 \geq \lambda_2 \geq ....$ are called the **singular values of K** and we set

$$s_n(K) = \lambda_n.$$

If we let ψ_n denote the corresponding o.n. sequence of eigenvectors for $|K|$ and set $\phi_n = W\psi_n$ then these vectors are also o.n. and we may write

$$|K| = \sum_{n=1}^{\infty} s_n(K) \, |\psi_n\rangle \, \langle\psi_n| \, ,$$

which yields

$$K = W|K| = \sum_{n=1}^{\infty} s_n(K) \, |\phi_n\rangle \, \langle\psi_n| \, .$$

This latter form is called the **singular valued decomposition(SVD)** of K. It is essentially unique, except that in the case that a single non-zero eigenvalue has multiplicity, then one could choose different o.n. vectors for the corresponding eigenspace.

4.1. **The Schatten p-Classes.** For proofs of the results stated here see [5, XI.9] or [6, III, Section 7]. Given $1 < p < +\infty$, we set

$$\mathcal{C}_p(\mathcal{H}, \mathcal{K}) = \{K \in \mathbb{K}(\mathcal{H}, \mathcal{K}) : \sum_{n=1}^{\infty} s_n(K)^p < +\infty\},$$

and for $K \in \mathcal{C}_p(\mathcal{H}, \mathcal{K})$ we set

$$\|K\|_p = \big(\sum_{n=1}^{\infty} s_n(K)^p\big)^{1/p}.$$

Here are the key facts about these sets.

(1) For $1 < p < +\infty, \mathcal{C}_p(\mathcal{H}, \mathcal{K})$ is a vector space.
(2) $\|\cdot\|_p$ is a norm on $\mathcal{C}_p(\mathcal{H}, \mathcal{K})$ and it is complete in this norm, i.e., a Banach space.
(3) If $K \in \mathcal{C}_1(\mathcal{H})$ and we pick any o.n.b. $\{e_a : a \in A\}$ for $\mathcal{H}$, then

$$Tr(K) := \sum_{a \in A} \langle e_a | K e_a \rangle$$

converges and its value is independent of the o.n.b. chosen. We call this the **trace of K** and for this reason we call $\mathcal{C}_1(\mathcal{H})$ the **trace class operators**.
(4) If $1 < p, q < +\infty$ with $\frac{1}{p} + \frac{1}{q} = 1$(called Holder conjugates) with $T \in \mathcal{C}_p(\mathcal{H}, \mathcal{K}), R \in \mathcal{C}_q(\mathcal{K}, \mathcal{H})$, then $RT \in \mathcal{C}_1(\mathcal{H}), TR \in \mathcal{C}_1(\mathcal{K})$ and $Tr(RT) = Tr(TR)$. Moreover,

$$|Tr(RT)| \leq \|T\|_p \|R\|_q.$$

(5) Let p, q be Holder conjugates. If we fix R and define a linear functional
$$f_R : \mathcal{C}_p(\mathcal{H}, \mathcal{K}) \to \mathbb{C},\ f_R(T) = Tr(RT),$$
then f_R is a bounded, linear functional with $\|f_R\| = \|R\|_q$. Moreover, every bounded linear functional on $\mathcal{C}_p(\mathcal{H}, \mathcal{K})$ is of this form.

This identifies the dual space of $\mathcal{C}_p(\mathcal{H}, \mathcal{K})$ with $\mathcal{C}_q(\mathcal{K}, \mathcal{H})$ in an isometric manner.

(6) If $T \in B(\mathcal{H}, \mathcal{K})$ and $R \in \mathcal{C}_1(\mathcal{K}, \mathcal{H})$, then $RT \in \mathcal{C}_1(\mathcal{H})$ and $TR \in \mathcal{C}_1(\mathcal{K})$ with $Tr(RT) = Tr(TR)$. The linear functional $f_T : \mathcal{C}_1(\mathcal{K}, \mathcal{H}) \to \mathbb{C}$ is bounded with $\|f_T\| = \|T\|$ and every bounded linear functional on $\mathcal{C}_1(\mathcal{K}, \mathcal{H})$ arises in this manner. That is the dual space of $\mathcal{C}_1(\mathcal{K}, \mathcal{H})$ can be identified with $B(\mathcal{H}, \mathcal{K})$ in this manner.

However, not every bounded linear functional on $B(\mathcal{H}, \mathcal{K})$ is of the form f_R for some $R \in \mathcal{C}_1(\mathcal{K}, \mathcal{H})$.

(7) For each $R \in \mathcal{C}_1(\mathcal{K}, \mathcal{H})$ the linear functional $f_R : \mathbb{K}(\mathcal{H}, \mathcal{K}) \to \mathbb{C}$ defined by $f_R(K) = Tr(RK)$ is bounded with $\|f_R\| = \|R\|_1$ and every bounded linear functional on $\mathbb{K}(\mathcal{H}, \mathcal{K})$ is of this form. That is the dual space of $\mathbb{K}(\mathcal{H}, \mathcal{K})$ can be identified with $\mathcal{C}_1(\mathcal{K}, \mathcal{H})$ in this manner.

An operator $\rho \in B(\mathcal{H})$ is called a **density operator** provided that $\rho \in \mathcal{C}_1(\mathcal{H}),\ \rho \geq 0$ and $Tr(\rho) = 1$.

Proposition 4.2. *Every element of $\mathcal{C}_1(\mathcal{H})$ can be written as a linear combination of 4 density operators.*

Proof. We sketch the key ideas of this proof. First one shows that $T \in \mathcal{C}_1(\mathcal{H}) \implies T^* \in \mathcal{C}_1(\mathcal{H})$. From this it follows that $T = H + iK$ with $H = (T + T^*)/2 \in \mathcal{C}_1(\mathcal{H})$ and $K = (T - T^*)/2i \in \mathcal{C}_1(\mathcal{H})$. Next one shows that $H^+, H^-, K^+, K^- \in \mathcal{C}_1(\mathcal{H})$.

Finally, setting $\rho_1 = H^+/Tr(H^+)$, $\rho_2 = H^-/Tr(H^-)$, $\rho_3 = K^+/Tr(K^+)$, and $\rho_4 = K^-/Tr(K^-)$ defines the four density operators. □

4.2. **Tensor Products of Operators.** Let $R_i \in B(\mathcal{H}_i, \mathcal{K}_i), i = 1, 2$, then there exists a unique operator $R_1 \otimes R_2 \in B(\mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{K}_1 \otimes \mathcal{K}_2)$ satisfying
$$(R_1 \otimes R_2)(h_1 \otimes h_2) = (R_1 h_1) \otimes (R_2 h_2).$$
Moreover, $\|R_1 \otimes R_2\| = \|R_1\|\|R_2\|$.

In the case that $\mathcal{H} + \mathcal{H}_1 = \mathcal{K}_1$ and $\mathcal{K} = \mathcal{H}_2 = \mathcal{K}_2$, if either $dim(\mathcal{H})$ or $dim(\mathcal{K})$ is finite, then every element of $B(\mathcal{H} \otimes \mathcal{K})$ is a sum of such elementary tensors, but when they are both infinite dimensional this is not the case.

5. Basics of Quantum Viewpoint

5.1. **Postulates of Quantum Mechanics.** To each isolated physical system, there corresponds a Hilbert space $\mathcal{H}$, called the *state space*, and each unit vector in $\mathcal{H}$ represents a possible state, called the *state vector* or *pure state*.

Quantum Measurements. When we want to observe a system, i.e., connect to the "outside world", the system is no longer closed because we interact with it. By *closed*, we mean "not interacting with anything outside the system". By *open*, we mean it is a piece of a larger system.

Quantum measurements are always described by a class of operators $\{M_i\}_{i=\text{one of the outcomes}}$.
The probability that we observe the outcome i, given that the system is in state $|\psi\rangle$ before we measure, is given by $p_i = \|M_i\psi\|^2$ and if we observe the outcome i, then the system changes to the state $\frac{M_i\psi}{\|M_i\psi\|}$. Moreover, as the sum of the probabilities of all possible outcomes must equal 1, we have $\sum_i p_i = 1$.

Keeping in mind that quantum mechanics is inherently probabilistic, we consider a quantum experiment with at most k possible outcomes. Let $\mathcal{H}_s$ and $\mathcal{H}_o$ be Hilbert spaces representing the state space and the outcome space, respectively, and let $\{M_i \in \mathcal{B}(\mathcal{H}_s, \mathcal{H}_o) : 1 \leq i \leq k\}$ be a collection of bounded operators. If the system is in state $\psi \in \mathcal{H}_s, \|\psi\| = 1$ before we measure, then the probability that we observe the outcome i is given by $p_i = \|M_i\psi\|^2$ and if we observe the outcome i, then the system changes to the state $\frac{M_i\psi}{\|M_i\psi\|}$. Moreover, as the sum of the probabilities of all possible outcomes must equal 1, we have $\sum_i p_i = 1$. Hence,

$$1 = \sum_{i=1}^{k} p_i = \sum_{i=1}^{k} \|M_i\psi\|^2 = \sum_{i=1}^{k} \langle M_i\psi | M_i\psi\rangle = \sum_{i=1}^{k} \langle \psi | M_i^* M_i \psi\rangle .$$

Since the above equality holds for every $\psi \in \mathcal{H}$ with $\|\psi\| = 1$, the following lemma forces $\sum_{i=1}^{k} M_i^* M_i = I$. If $T \in \mathcal{B}(\mathcal{H})$, then $T = I \iff \langle\psi|T\psi\rangle = 1$ for every $\|\psi\| = 1$.

Theoretically, given any class of operators $\{M_i \in \mathcal{B}(\mathcal{H}_s, \mathcal{H}_o) : 1 \leq i \leq k\}$ such that $\sum_{i=1}^{k} M_i^* M_i = I$, there is a k-outcome quantum experiment with these measurement operators.

5.2. **Measurement Systems and Distinguishable States.** We include a bit more in the notes than we covered in class to help those who are new to this quantum viewpoint.

Definition 5.1. (Measurement System) Suppose that $\mathcal{H}$ and $\mathcal{K}$ are finite-dimensional Hilbert spaces. A finite family $\{M_i : 1 \leq i \leq k\}$ of operators $M_i : \mathcal{H} \to \mathcal{K}$ is called a *measurement system* if $\sum_i M_i^* M_i = I$. If $\mathcal{H} = \mathcal{K}$, we say that $\{M_i\}$ is a measurement system *on* $\mathcal{H}$.

Definition 5.2. (Perfectly Distinguishable States) A collection of states $\{\psi_1, \ldots, \psi_N\} \subseteq \mathcal{H}$ is called *perfectly distinguishable* if there exists a measurement system $\{M_i : 1 \leq i \leq k\}, k \geq N$ on $\mathcal{H}$ such that $\|M_i(\psi_j)\|^2 = \delta_{i,j}$ for $i, j \in \{1, ..., N\}$.

Theorem 5.3. *A collection of states $\{\psi_1, \ldots, \psi_N\} \subseteq \mathcal{H}$ is perfectly distinguishable if and only if $\psi_i \perp \psi_j$ for all $i \neq j$.*

Proof. ($\implies$) For the forward direction, let us assume that there is a measurement system $\{M_i : 1 \leq i \leq N\}$ such that $\|M_i(\psi_j)\| = \delta_{i,j}$ for $i, j \in \{1, ..., N\}$. Consider ψ_1 and ψ_2. ψ_2 can then be expressed as $\psi_2 = \alpha\psi_1 + \beta\eta$ where $\eta \perp \psi_1, \|\eta\| = 1$. Since $1 = \|\psi\|^2 = |\alpha|^2 + |\beta|^2$, we have $1 = \|M_2(\psi_2)\|^2 = \|M_2(\alpha\psi_1 + \beta\eta)\|^2 = |\beta|^2\|M_2(\eta)\|^2 \leq |\beta|^2\|\eta\|^2 = \|\beta\|^2 \leq 1$. This forces the above inequalities to be equalities so that $|\beta|^2 = 1$ which in turn implies that $\alpha = 0$ which means that ψ_2 and η are collinear and hence $\psi_2 \perp \psi_1$.

($\impliedby$) Let M_i be the (orthogonal) projection onto the one-dimensional subspace spanned by ψ_i. Then $M_i = M_i^* = M_i^* M_i$ for $i = 1, ..., N$ and $\sum_{i=1}^N M_i^* M_i$ is the orthogonal projection onto $\text{span}\{\psi_1, ..., \psi_N\}$. Let M_0 be the orthogonal projection onto $\{\psi_1, \ldots, \psi_N\}^\perp$. Then $\sum_{j=0}^N M_j^* M_j = \sum_{j=0}^N M_j = I$. Furthermore, $M_i(\psi_j) = \delta_{i,j}\psi_j$ for all $i, j \in \{1, ..., N\}$, so that $\|M_i(\phi_j)\|^2 = \delta_{i,j}$ for all $i, j \in \{1, ..., N\}$. This proves that $\{M_i\}_{i=0}^N$ is a measurement system. □

Corollary 5.4. *If* $\dim(\mathcal{H}_s) = N$, *then the system can have at most* N *perfectly distinguishable states.*

Theorem 5.5. *Suppose that* $\{\psi_1, \ldots, \psi_N\}$ *is a collection of linearly independent states. Then there exists a measurement system* $\{M_i : 0 \leq i \leq N\}$ *such that for* $i \neq 0$, $\|M_i(\psi_j)\| \neq 0$ *if and only if* $i = j$.

Proof. For $i = 1, ..., N$, let $V_i = \text{span}\{\psi_j : j \neq i\}$, and let E_i be the projection onto $V_i^\perp$. Then for $j \neq i$, $\psi_j \in V_i \implies E_i(\psi_j) = 0 \implies \|E_i(\psi_j)\|^2 = 0$. Now $0 \leq E_i \leq I \implies 0 \leq E_1 + \cdots + E_N \leq N \cdot I$. Let $M_i = \frac{1}{\sqrt{N}} E_i$ for $i = 1, ..., N$. Then $M_i^* M_i = \frac{1}{N} E_i$, so $\sum_{i=1}^N M_i^* M_i = \frac{1}{N}\sum_{i=1}^N E_i \leq I$, and hence $I - \sum_{i=1}^N M_i^* M_i \geq 0$. Now let $M_0 = (I - \sum_{i=1}^N M_i^* M_i)^{\frac{1}{2}}$. Then $\sum_{i=0}^N M_i^* M_i = \left((I - \sum_{i=1}^N M_i^* M_i)^{\frac{1}{2}}\right)^2 + \sum_{i=1}^N M_i^* M_i = I$, so $\{M_i\}_{i=0}^N$ is a measurement system. For $i \neq 0$, if $j \neq i$, then $\|M_i(\psi_j)\| = \frac{1}{\sqrt{N}}\|E_i(\psi_j)\| = 0$. Therefore by contrapositive, $\|M_i(\psi_j)\| \neq 0$ implies that $i = j$. Conversely, $\|M_i(\psi_i)\| = \frac{1}{\sqrt{N}}\|E_i(\psi_i)\| \neq 0$ since $\psi_i \notin V_i$ and so it has non-zero projection onto $V_i^\perp$. □

So far we have talked about pure states, now we will talk about ensembles (or mixed states).

5.3. **Ensembles or Mixed States.** As motivation for this topic, let $\{M_i : 1 \leq i \leq k\}$ be a measurement system with $M_i : \mathcal{H}_s \longrightarrow \mathcal{H}_o$. Suppose we have the state $\psi \in \mathcal{H}_s$ as input. Recall that $p_i = \|M_i(\psi)\|^2$ should be interpreted as the probability of observing the outcome i, and that if we do observe i, the system is now in the state, $\frac{M_i(\psi)}{\|M_i(\psi)\|}$. That is,

input:$\psi \in \mathcal{H}_s$; output: $\frac{M_i(\psi)}{\|M_i(\psi)\|}$ with probability $p_i = \|M_i(\psi)\|^2$.

So after observation, we will have what now looks like a mixed bag of states $\left\{\frac{M_i(\psi)}{\|M_i(\psi)\|}\right\}_i$, with $\frac{M_i(\psi)}{\|M_i(\psi)\|}$ occurring with probability p_i.

Definition 5.6. An *ensemble of states*, or a *mixed state*, is a finite collection $\{\psi_i, p_i : 1 \leq i \leq N\}$ of states ψ_i with probabilities p_i where $\|\psi_i\| = 1$, $p_i \geq 0$ and $\sum_{i=1}^{N} p_i = 1$.

Suppose we have a measurement system $\{M_i : 1 \leq i \leq N\}$ and an ensemble of states $\{\psi_j, p_j : 1 \leq j \leq k\}$ with $\sum_{j=1}^{k} p_j = 1$, then what is the probability of observing the outcome i?
If ψ_j is our input, then the probability getting outcome i is $\|M_i(\psi_j)\|^2$. So, the probability that we have outcome i is,

$$\sum_{j=1}^{k} p_j \|M_i(\psi_j)\|^2.$$

In the next subsection we discuss a better way to compute the probabilities of outcomes.

5.4. **Von Neumann's Notation: Density Matrices.** For a given state $\psi \in \mathcal{H}_s, \|\psi\| = 1$, a typical unit vector in the one-dimensional subspace spanned by ψ is given by $e^{i\theta}\psi$. In general $e^{i\theta}\psi \neq \psi$ but for any measurement M_j, we can see that $\|M_j(\psi)\|^2 = \|M_j(e^{i\theta}\psi)\|^2$. This shows that measurements don't distinguish between different unit vectors from the one-dimensional subspace spanned by the given state vector ψ and hence states should really refer to one-dimensional subspace and not just a unit vector. This means that *the probabilities of outcomes really depend on the one-dimensional subspace generated by a vector.*

Replacing states by rank one projections and lengths by trace: Recall that given a matrix $A = (a_{ij}) \in M_n$, the *trace* of that matrix is the sum of the diagonal entries: $Tr(Y) = \sum_i a_{ii}$. It is a popular fact that given any two square matrices A and B of the same size, $Tr(AB) = Tr(BA)$. The next proposition establishes this fact for compatible non-square matrices as well. Next, if $\psi \in \mathbb{C}^n, \|\psi\| = 1$, and P_ψ denotes the orthogonal projection onto the subspace spanned by ψ, then $P_\psi = \psi\psi^* = |\psi\rangle\langle\psi|$. ($P_\psi h = \psi\psi^* h = \langle\psi|h\rangle\psi$ where $\langle\psi|h\rangle$ is the component of h in the direction of ψ.) Furthermore,

$$Tr(P_\psi) = Tr(\psi\psi^*) = Tr(\psi^*\psi) = (\psi^*\psi) = \langle\psi|\psi\rangle = 1.$$

Back to Ensemble: Let's get back to the situation where we had a measurement system $\{M_i : 1 \leq i \leq N\}$ and an ensemble of states $\{\psi_j, p_j : 1 \leq j \leq k\}$ with $\sum_{j=1}^{k} p_j = 1$. We know that the probability of observing the outcome i is,

$$\sum_{j=1}^{k} p_j \|M_i(\psi_j)\|^2.$$

Simplifying this expression, we get

$$\begin{aligned}\sum_{j=1}^{k} p_j \|M_i(\psi_j)\|^2 &= \sum_{j=1}^{k} p_j (M_i\psi_j)^*(M_i\psi_j) \\ &= \sum_{j=1}^{k} p_j Tr((M_i\psi_j)^*(M_i\psi_j)) \\ &= \sum_{j=1}^{k} p_j Tr((M_i\psi_j)(M_i\psi_j)^*) \\ &= \sum_{j=1}^{k} p_j Tr(M_i\psi_j\psi_j^* M_i^*) \\ &= \sum_{j=1}^{k} p_j Tr(M_i^* M_i\psi_j\psi_j^*) \\ &= \sum_{j=1}^{k} Tr\left(M_i^* M_i(p_j\psi_j\psi_j^*)\right) \\ &= Tr\left(M_i^* M_i\left(\sum_{j=1}^{k} p_j\psi_j\psi_j^*\right)\right).\end{aligned}$$

Note that $\psi_j\psi_j^* = P_{\psi_j}$. If we set $P = \sum_{j=1}^{k} p_j\psi_j\psi_j^*$, then we have shown that:

Theorem 5.7. *Given an ensemble of states $\{\psi_j, p_j : 1 \leq j \leq k\}$ and a measurement system $\{M_i : 1 \leq i \leq N\}$, the probability of observing the i-th outcome is $Tr\,(M_i^* M_i P)$ where $P = \sum_{j=1}^{k} p_j\psi_j\psi_j^*$.*

The operator $P = \sum_{j=1}^{k} p_j\psi_j\psi_j^*$ associated to an ensemble of states is called the **Von Neumann density operator of the given ensemble**.

We observe that:

(1) If two ensembles have the same density matrix, then we get the same probability for outcomes for any measurement system.
(2) If $\{M_i : 1 \leq i \leq k\}$ and $\{\tilde{M}_i : 1 \leq i \leq k\}$ are two measurement systems such that for every i, $M_i^* M_i = \tilde{M}_i^* \tilde{M}_i$, then also we get the same probability for outcomes for any ensemble.

The following example illustrates the first observation.

Example 5.8. If $\{u_1, ..., u_N\}$ is an orthonormal basis for $\mathbb{C}^N$, then the density matrix P for the ensemble $\{u_j, \frac{1}{N} : 1 \leq j \leq N\}$ is given by $P = \sum_{j=1}^{N} \frac{1}{N} u_j u_j^* = \frac{1}{N} I_N$. If $\{\tilde{u}_1, ..., \tilde{u}_N\}$ is another orthonormal basis for $\mathbb{C}^N$, then the density matrix $\tilde{P}$ for the ensemble $\{\tilde{u}_j, \frac{1}{N} : 1 \leq j \leq N\}$ also turns

out to be $\tilde{P} = \sum_{j=1}^{N} \frac{1}{N} \tilde{u}_j \tilde{u}_j^* = \frac{1}{N} I_N$. This example guarantees the existence of two different ensembles with same density matrix.

Problem 5.9. *Fix $N \geq 3$ and let $u_j = \begin{pmatrix} \cos(\frac{2\pi j}{N}) \\ \sin(\frac{2\pi j}{N}) \end{pmatrix} \in \mathbb{C}^2$. Prove that the density matrix for the ensemble $\{u_j, \frac{1}{N} : 1 \leq j \leq N\}$ is given by $\frac{1}{2} I_2$.*

The above example shows that the density matrix does not distinguish between standard orthonormal basis or any other orthonormal basis as input. So, for computing probabilities, it is the density matrix which is important and not the ensemble.

At this point, let us pause for a while and try to visualise quantum experiments in terms of density matrices. Recall that, if a system is initially in the state ψ, that is, $\psi \in \mathcal{H}_s, \|\psi\| = 1$, and if there is given a measurement system $\{M_i : 1 \leq i \leq k\}$, then after measurement, the system becomes the ensemble $\left\{ \frac{M_i(\psi)}{\|M_i(\psi)\|}, \|M_i\psi\|^2 : 1 \leq i \leq k \right\}$. By associating density matrices with the states of the system before and after the measurement we note that the input is the state ψ and the density matrix corresponding to it is given by $P = \psi\psi^*$. After the measurement, the system becomes the ensemble $\left\{ \frac{M_i(\psi)}{\|M_i(\psi)\|}, \|M_i\psi\|^2 : 1 \leq i \leq k \right\}$, and hence the output is this ensemble which is identified by the density matrix

$$\begin{aligned} &\sum_{i=1}^{k} \|M_i\psi\|^2 \left(\frac{M_i(\psi)}{\|M_i(\psi)\|} \right) \left(\frac{M_i(\psi)}{\|M_i(\psi)\|} \right)^* \\ &= \sum_{i=1}^{k} (M_i\psi)(M_i\psi)^* = \sum_{i=1}^{k} (M_i\psi)(\psi^* M_i^*) \\ &= \sum_{i=1}^{k} M_i(\psi\psi^*)M_i^* = \sum_{i=1}^{k} M_i P M_i^*. \end{aligned}$$

Thus, in terms of density matrices, we observed that if input is identified by the density matrix P, then after measurement, the output is identified by the density matrix $\sum_{i=1}^{k} M_i P M_i^*$. This observation is the key to our next theorem.

Theorem 5.10. *Given an ensemble of states $\{\psi_j, p_j : 1 \leq j \leq J\}$ and a measurement system $\{M_i : 1 \leq i \leq k\}$ on $\mathcal{H}_s$ with density matrix $P = \sum_{j=1}^{J} p_j \psi_j \psi_j^*$, then after measurement, the system becomes the ensemble $\left\{ \frac{M_i(\psi_j)}{\|M_i(\psi_j)\|}, p_j \|M_i\psi_j\|^2 : 1 \leq i \leq k, 1 \leq j \leq J \right\}$ with density matrix $\sum_{i=1}^{k} M_i P M_i^*$.*

Proof. The density matrix for the output ensemble is given by

$$\sum_{j=1}^{J}\sum_{i=1}^{k} p_j||M_i\psi_j||^2 \left(\frac{M_i\psi_j}{||M_i\psi_j||}\right)\left(\frac{M_i\psi_j}{||M_i\psi_j||}\right)^* = \sum_{j=1}^{J}\sum_{i=1}^{k} p_j(M_i\psi_j)(M_i\psi_j)^*$$
$$= \sum_{i=1}^{k}\sum_{j=1}^{J} M_i(\psi_j p_j \psi_j^*)M_i^*$$
$$= \sum_{n=1}^{N} M_i P M_i^*. \qquad \square$$

So, a measurement system takes density matrix as input and yields another density matrix as output.

5.5. **Axiomatization of Quantum Channels.** We are now in a position to axiomatize *quantum channels*.

(1) A quantum channel should be a linear map,

$$\Phi : \mathcal{C}_1(\mathcal{H}_i) \to \mathcal{C}_1(\mathcal{H}_o).$$

(2) If $\rho \in \mathcal{C}_1(\mathcal{H}_i)$ is a density operator, then $\Phi(\rho) \in \mathcal{C}_1(\mathcal{H}_o)$ is a density operator.

The next axiom has to do with how quantum systems combine. Suppose we have two laboratories A and B (for Alice and Bob respectively). We will denote by $\mathcal{H}_{s,A}, \mathcal{H}_{s,B}, \mathcal{H}_{o,A}, \mathcal{H}_{o,B}$, respectively, the state space of lab A, the state space of lab B, the outcome space of lab A, and the outcome space of lab B.

Suppose that each lab has a measurement system. Let $\{M_i : \mathcal{H}_{s,A} \longrightarrow H_{o,A}\}_{i=1}^{K}$ be the measurement system of A and $\{N_j : \mathcal{H}_{s,B} \longrightarrow H_{o,B}\}_{j=1}^{J}$ be the measurement system of B. These define quantum channels,

$$\Phi_A(\rho_A) = \sum_{i=1}^{K} M_i\rho_A M_i^* \;\; \Phi_B(\rho_B) = \sum_{j=1}^{J} N_j\rho_B N_j^*.$$

If we wish to view these two labs as one single lab, say lab AB, then the state space of this lab is $\mathcal{H}_{s,AB} = \mathcal{H}_{s,A} \otimes \mathcal{H}_{s,B}$ and the output space would be $\mathcal{H}_{o,AB} = \mathcal{H}_{o,A} \otimes \mathcal{H}_{o,B}$ with measurement operators $\{M_i \otimes N_j : \mathcal{H}_{s,AB} \longrightarrow H_{o,AB}\}$, so that there are KJ outcomes. Note that $\sum_{i,j}(M_i \otimes N_j)^*(M_i \otimes N_j) = I$. This measurement system of lab AB, then, defines a quantum channel $\Phi_{AB} : \mathcal{C}_1(\mathcal{H}_{s,AB}) \longrightarrow \mathcal{C}_1(\mathcal{H}_{o,AB})$ given by

$$\Phi_{AB}(W) = \sum_{i,j}(M_i \otimes N_j)W(M_i \otimes N_j)^*.$$

This motivates the next axiom.

(3) Given quantum channels, $\Phi_A : \mathcal{C}_1(\mathcal{H}_{A,i}) \to \mathcal{C}_1(\mathcal{H}_{A,o})$ and $|Phi_B : \mathcal{C}_1(\mathcal{H}_{B,i}) \to \mathcal{C}_1(\mathcal{H}_{B,o})$ there should exist a quantum channel

$$\Phi_{AB} : \mathcal{C}_1(\mathcal{H}_{A,i} \otimes \mathcal{H}_{B,i}) \to \mathcal{C}_1(\mathcal{H}_{A,o} \otimes \mathcal{H}_{B,o})$$

satisfying $\Phi_{AB}(\rho_A \otimes \rho_B) = \Phi_A(\rho_A) \otimes \Phi_B(\rho_B)$.

Finally, doing nothing should be a quantum channel:

(4) Given any Hilbert space, the identity map from $id : \mathcal{C}_1(\mathcal{H}) \to \mathcal{C}_1(\mathcal{H})$ is a quantum channel.

Since every positive operator in $\mathcal{C}_1(\mathcal{H})$ is a positive multiple of a density operator, the first two axioms imply that a quantum channel must send positive operators to positive operators, such a map is called a **positive map**. The fact that density operators span $\mathcal{C}_1(\mathcal{H})$ together with the fact that density operators are mapped to density operators implies that a quantum channel must preserve traces, i.e.,

$$Tr(\Phi(W)) = Tr(W).$$

We will see that axioms 3 and 4 imply that a quantum channel must be "completely" positive. A concept that we need to first discuss.

6. Matrix Norm, Matrix Order, and Operator Matrices

Suppose that $T : V_1 \longrightarrow W_1$ and $R : V_2 \longrightarrow W_2$ are linear maps between vector spaces, then there is a linear map $T \otimes R : V_1 \otimes V_2 \longrightarrow W_1 \otimes W_2$ defined by $(T \otimes R)(v_1 \otimes v_2) = T(v_1) \otimes R(v_2)$ for all $v_1 \in V_1$ and $v_2 \in V_2$. If $\mathcal{H}$ and $\mathcal{K}$ are finite-dimensional Hilbert spaces with $X : \mathcal{H} \to \mathcal{H}$ and $Y : \mathcal{K} \to \mathcal{K}$, linear. Then there is a well-defined linear map denoted $X \otimes Y : \mathcal{H} \otimes \mathcal{K} \to \mathcal{H} \otimes \mathcal{K}$ satisfying $(X \otimes Y)(h \otimes k) = X(h) \otimes Y(k)$.

If $T : \mathcal{H} \longrightarrow \mathcal{H}$, possibly infinite dimensional, and $R : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ are linear, then we can define $T \otimes R : \mathcal{H} \otimes \mathbb{C}^n \longrightarrow \mathcal{H} \otimes \mathbb{C}^n$, in a similar way. Our goal in this subsection is to find a matrix representation for the map $T \otimes R$ in this setting. To do this, let us first address the following question:

I. What is a natural identification of a typical element of $\mathcal{H} \otimes \mathbb{C}^n$?

Recall that if we take the canonical orthonormal basis $\{e_1, ..., e_n\}$ for $\mathbb{C}^n$, then every vector $u \in \mathcal{H} \otimes \mathbb{C}^n$ has a unique representation given by $u = \sum_{i=1}^n h_i \otimes e_i$ where $h_i \in \mathcal{H}$, and

$$\|u\|^2 = \left\langle \sum_{i=1}^n h_i \otimes e_i | \sum_{j=1}^n h_j \otimes e_j \right\rangle = \sum_{i,j=1}^n \langle h_i | h_j \rangle \langle e_i | e_j \rangle = \sum_{i=1}^n \|h_i\|^2 = \|(h_1, ..., h_n)\|^2.$$

In other words, we have the Hilbert space isomorphism

$$\mathcal{H} \otimes \mathbb{C}^n \simeq \underbrace{\mathcal{H} \oplus \cdots \oplus \mathcal{H}}_{n \text{ times}} = \mathcal{H}^{(n)}$$

via the natural identification $\sum_{i=1}^n (h_i \otimes e_i) \simeq \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}$.
The next question which we want to address is:

II. What is a natural identification of a linear map in $B(\mathcal{H} \otimes \mathbb{C}^n)$?
Given $A_{ij} \in B(\mathcal{H})$ for $1 \leq i, j \leq n$, we can consider $A = (A_{ij}) \in M_n(B(\mathcal{H}))$ as an operator defined by

$$A \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n A_{1j} h_j \\ \vdots \\ \sum_{j=1}^n A_{nj} h_j \end{pmatrix} \in \underbrace{\mathcal{H} \oplus \cdots \oplus \mathcal{H}}_{n \text{ times}}.$$

It is not hard to see that every such map is bounded. Therefore, we have $M_n(B(\mathcal{H})) \hookrightarrow B(\mathcal{H} \otimes \mathbb{C}^n)$ in a natural way. In fact, every linear map on $\mathcal{H} \otimes \mathbb{C}^n$ has such a matrix representation. The proof is "grubby" but here is the idea: If $A : \mathcal{H} \oplus \cdots \oplus \mathcal{H} \to \mathcal{H} \oplus \cdots \oplus \mathcal{H}$ is linear, then $A \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}$.
The map $\begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} \mapsto k_1$ is linear. Similarly, mapping the column vector to k_2 is linear, and so on and so forth. The map $\begin{pmatrix} h_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \mapsto k_1$ is linear, so there is $A_{11} : \mathcal{H} \to \mathcal{H}$ enacting this transformation. If we continue to do this for every h_i and k_j, then we get linear maps $A_{ij} : \mathcal{H} \to \mathcal{H}$ and one can check that $A = (A_{ij})$.
Hence, we have a natural identification $B(\mathcal{H} \otimes \mathbb{C}^n) \simeq M_n(B(\mathcal{H}))$ via $A \simeq (A_{ij})$, thereby allowing us to identify any linear operator $A \in B(\mathcal{H} \otimes \mathbb{C}^n)$ by an $n \times n$ block matrix $(A_{ij}) \in M_n(B(\mathcal{H}))$ whose entries are given by linear maps.

This means, in particular, that when we write down a matrix of operators, then $(A_{i,j})$ has a well-defined norm, namely, its norm as an operator on $\mathcal{H}^{(n)}$ and we can say if it defines a positive operator or not. This is what is meant by the natural **matrix norm** and **matrix order** on $M_n(B(\mathcal{H}))$.

III. Matrix Representation of $T \otimes R$: Suppose that $T : \mathcal{H} \longrightarrow \mathcal{H}$ and $R : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ are linear, $R \in M_n(\mathbb{C}), R = (r_{ij})$, then $T \otimes R : \mathcal{H} \otimes \mathbb{C}^n \longrightarrow \mathcal{H} \otimes \mathbb{C}^n$ has a natural representation as an $n \times n$ block matrix $T \otimes R \in M_n(\mathcal{L}(\mathcal{H}))$ whose entries are given by linear maps.

We know that $(T \otimes R)(h \otimes y) = T(h) \otimes R(y)$, therefore,

$$(T \otimes R)(h \otimes e_j) = T(h) \otimes R(e_j) = T(h) \otimes \left(\sum_{i=1}^{n} r_{ij} e_i \right)$$

$$= \sum_{i=1}^{n} r_{ij} T(h) \otimes e_i \simeq \begin{pmatrix} r_{1j}Th \\ \vdots \\ r_{nj}Th \end{pmatrix} = (r_{ij}T) \begin{pmatrix} 0 \\ \vdots \\ h \\ \vdots \\ 0 \end{pmatrix},$$

where h is in the j-th position and there are 0's everywhere else in the column vector. The ***Kronecker product*** of T and R, then, is the block matrix in $M_n(B(\mathcal{H}))$ given by $(r_{ij}T)$ (so, there are n blocks, each block is of size equal to the dimension of $\mathcal{H}$, and the (i,j)-block is $r_{ij}T$). In other words, the Kronecker product is equal to the tensor product of the linear maps (with respect to the canonical basis for $\mathbb{C}^n$).

A special case is when $R = I_n$ then we have that

$$T \otimes I_n = \begin{pmatrix} T & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & & T \end{pmatrix}.$$

If $T \in M_k$ and $R \in M_n$. Then $T \otimes R$ has matrix representation given by $T \otimes R = \begin{pmatrix} r_{11}T & \cdots & r_{1n}T \\ \vdots & \ddots & \vdots \\ r_{n1}T & \cdots & r_{nn}T \end{pmatrix}$, a block matrix with n blocks, each of size k.

Another way to view operator matrices is as sums of tensors. If we set

$$E_{i,j} = |e_i\rangle \langle e_j|,$$

then

$$(A_{i,j}) = \sum_{i,j=1}^{k} A_{i,j} \otimes E_{i,j} \in B(\mathcal{H}) \otimes M_k.$$

Given subspaces, $V \subseteq B(\mathcal{H})$ and $W \subseteq B(\mathcal{K})$ we can regard $M_k(V) \subseteq M_k(B(\mathcal{H}))$ and $M_k(W) \subseteq M_k(B(\mathcal{K}))$. This means that these subspaces are also endowed with a canonical matrix norm and matrix order, via these inclusions.

Given a linear map $\Phi : V \to W$ we get linear maps, $\Phi^{(k)} : M_k(V) to M_k(W)$ via

$$\Phi^{(k)}((A_{i,j})) = (\Phi(A_{i,j})).$$

We say that Φ is **k-positive** if $\Phi^{(k)}$ maps positive elements of $M_k(V)$ to positive elements of $M_k(W)$. We say that Φ is **completely positive** if it is k-positive for all k.

Similarly, each map $\Phi^{(k)}$ has a norm, but it turns out that these can vary with k. So we call Φ **completely bounded** provided that

$$\|\Phi\|_{cb} := \sup\{\|\Phi^{(k)}\|; k \in \mathbb{N}\} < +\infty.$$

Here is one example. Let $V = W = B(\mathbb{C}^2)$ and define $\Phi(X) = X^t$, the transpose. It is a linear map. It is easy to check that $P \geq 0 \iff P^t \geq 0$, os it is a positive map. Also, $\|X\| + \|X^t\|$ is easily chekced. So Φ is an isometric map.

Now consider the "matrix of matrix units",

$$Q = \begin{pmatrix} E_{1,1} & E_{1,2} \\ E_{2,1} & E_{2,2} \end{pmatrix} \in M_2(B(\mathbb{C}^2)) = B(\mathbb{C}^4).$$

Since $Q = Q^*$ and $Q^2 = 2Q$ we see that the spectrum of Q is $\{0, 2\}$ and so $Q \geq 0$. But

$$\Phi^{(2)}(Q) = \begin{pmatrix} E_{1,1} & E_{2,1} \\ E_{1,2} & E_{2,2} \end{pmatrix} := R.$$

We have that $det(R) = -1$, so it has negative eigenvalues. Hence, R is not positive and Φ is not 2-positive and so not completely positive.

Also, $R^2 = I$ and so $\|R\| = 1$ and $\Phi^{(2)}(R) = Q$ which has norm 2. Thus, $\|Phi^{(2)}\| \geq 2$. In fact, $\|\Phi\|_{cb} = 2$. So this example shows that in general $\|Phi\| \neq \|\Phi\|_{cb}$.

If one considers the transpose map on M_n one can show that it has norm one and cb-norm of n. Thus, the cb-norm of a map can be arbitrarily larger than its norm. In fact, if we consider the transpose map on $B(\ell^2_{\mathbb{N}})$ it is an isometric map with infinite cb-norm.

7. Introduction to C*-algebras

Developments and proofs of many of the results stated in this section can be found in [3, 4, 8]. Recall that $\mathcal{A}$ is an **algebra** if it is a vector space and also has a product that satisfies:

- $(AB)C = A(BC)$
- $(A + B)C = AC + BC, C(A + B) = CA + CB$,
- $\lambda \in \mathbb{C}, A, B \in \mathcal{A} \implies \lambda(AB) = (\lambda A)B = A(\lambda B)$.

An algebra is called a **Banach algebra** if it has a norm, it is complete in the norm, i.e., a Banach space, and the norm is submultiplicative:

$$\|AB\| \leq \|A\|\|B\|.$$

An algebra is a ***-algebra** if it also has a map $A \to A^*$ satisfying

- $(A^*)^* = A$,
- $(A + B)^* = A^* + B^*$,
- $\lambda \in \mathbb{C}, A \in \mathcal{A} \implies (\lambda A)^* = \overline{\lambda} A^*$,

- $(AB)^* = B^*A^*$.

These properties are reflecting the behaviour of the adjoint of Hilbert space operators.

A *-algebra is a **C*-algebra** if the norm also satisfies

$$\|A^*\| = \|A\| \text{ and } \|A\|^2 = \|A^*A\|.$$

We call $\mathcal{A}$ a **unital C*-algebra** if it also has a unit element, I. In the case one can show that necessarily, $I^* = I$ and $\|I\| = 1$.

The axioms are set up so that any norm closed subalgebra $\mathcal{A} \subseteq B(\mathcal{H})$ such that $A \in \mathcal{A} \implies A^* \in \mathcal{A}$ is a C*-algebra. We will call these **concrete C*-algebras.**

One key theorem is that every abstract C*-algebra is "identical" to a concrete C*-algebra, where means *-isomorphic, a concept that we will define shortly.

Here are some non-concrete C*-algebras. Let X be a compact Hausdorff space and set

$$C(X) = \{f : X \to \mathbb{C} | \text{ f is continuous } \},$$

and set

$$\|f\| = \sup\{|f(x)| : x \in X\},$$

which is finite since X is compact. Define a *-operation by

$$f^*(x) = \overline{f(x)}.$$

Then it is not hard to see that this is a C*-algebra.

Here are a few basic facts about C*algebras.

Cartesian Decomposition: Given $A \in \mathcal{A}$ we have that $H = \frac{A+A^*}{2} = H^* \in \mathcal{A}$ and $K = \frac{A-A^*}{2i} = K^* \in \mathcal{A}$ and $A = H + iK$.

Spectrum: Given a unital C*-algebra $\mathcal{A}$ and $A \in \mathcal{A}$ we set

$$\sigma_{\mathcal{A}}(A) = \{\lambda \in \mathbb{C} | \ (\lambda I - A) \text{ has no inverse in } \mathcal{A}\}.$$

Then $\sigma_{\mathcal{A}}(A)$ is a non-empty compact set and we have

$$\sup\{|\lambda| : \lambda \in \sigma_{\mathcal{A}}(A)\} = \lim_n \|A^n\|^{1/n}.$$

Spectral Permanence: If $\mathcal{A}$ is a C*-subalgebra of $\mathcal{B}$ with $I \in \mathcal{A} \subseteq \mathcal{B}$, then for any $X \in \mathcal{A}$, $\sigma_{\mathcal{A}}(X) = \sigma_{\mathcal{B}}(X)$.

- if $H = H^*$, then $\sigma_{\mathcal{A}}(H) \subseteq \mathbb{R}$.
- If $U^*U = UU^* = I$, then $\sigma_{\mathcal{A}}(U) \subseteq \mathbb{T}$.
- If $P = P^*$, then $P = A^*A$ for some A if and only if $\sigma_{\mathcal{A}}(P) \subseteq [0, +\infty)$.

This last property is used to define the **positive** elements of a C*-algebra.

Given two C*-algebras, $\mathcal{A}, \mathcal{B}$ a map $\pi : \mathcal{A} \to \mathcal{B}$ is called a ***-homomorphism** provided:

- π is linear,
- $\pi(XY) = \pi(X)\pi(Y)$, i.e., is multiplicative,
- $\pi(X^*) = \pi(X)^*$.

We call π a ***-isomorphism** if in addition it is one-to-one and onto.

Proposition 7.1. *If π is a *-homomorphism, then $\|\pi(X)\| \leq \|X\|$ and the range of π, $\mathcal{R}(\pi)$ is closed. Consequently, if π is a *-isomorphism, then π is an isometry.*

Corollary 7.2 (Uniqueness of Norm)**.** *Let $\mathcal{A}$ be a *-algebra and suppose that $\|\cdot\|_1$, $\|\cdot\|_2$ are two norms, both of which make $\mathcal{A}$ into a C*-algebra. Then $\|X\|_1 = \|X\|_2$, $\forall X \in \mathcal{A}$.*

The following theorem characterizes all **abelian,** i.e., $X, Y \in \mathcal{A} \implies XY = YX$, C*-algebras.

Theorem 7.3 (Gelfand-Naimark)**.** *Each unital abelian C*-algebra is *-isomorphic to $C(X)$ for some compact, Hausdorff space X.*

7.1. **States and the GNS Construction.** By a **state** on a unital C*-algebra $\mathcal{A}$ we mean a linear functional, $s : \mathcal{A} \to \mathbb{C}$ such that $s(I) = 1$ and $s(X^*X) \geq 0$, $\forall X \in \mathcal{A}$.

The following alternative characterization of states is often useful.

Proposition 7.4. *Let $s : \mathcal{A} \to \mathbb{C}$ be a linear functional with $s(I) = 1$. Then s is a state if and only if $\|s\| = 1$.*

Theorem 7.5 (The GNS Construction)**.** *Let $\mathcal{A}$ be a unital C*-algebra and let $s : \mathcal{A} \to \mathbb{C}$ be a state. Then there exists a Hilbert space $\mathcal{H}$, a unit vector $\phi \in \mathcal{H}$ and a unital *-homomorphism, $\pi : \mathcal{A} \to B(\mathcal{H})$ such that*

$$s(A) = \langle \phi | \pi(A)\phi \rangle, \ \forall A \in \mathcal{A}.$$

We outline the key ideas of the proof. First define a map

$$B : \mathcal{A} \times \mathcal{A} \to \mathbb{C} \text{ by } B(X, Y) = s(X^*Y).$$

It is easy to check that this map is sesquilinear and positive semidefinite. Thus, if we let

$$\mathcal{N} = \{X \in \mathcal{A} | B(X, X) = 0\},$$

then $\mathcal{N}$ is a subspace and we have a well-defined inner product on $\mathcal{A}/\mathcal{N}$ defined by

$$\langle X + \mathcal{N} | Y + \mathcal{N} \rangle = s(X^*Y).$$

We will get our HIlbert space $\mathcal{H}$ by completing this inner product space.

Next note that for each $A \in \mathcal{A}$ we have a linear map

$$L_A : \mathcal{A} \to \mathcal{A}, \ L_A(X) = AX,$$

given by left multiplication by the element A.

We claim that $L_A(\mathcal{N}) \subseteq \mathcal{N}$. To see this we first show that

$$0 \leq X^*A^*AX \leq \|A\|^2 X^*X.$$

Hence, if $X \in \mathcal{N}$ then

$$0 \leq s(X^*A^*AX) \leq \|A\|^2 s(X^*X) = 0.$$

This implies that $s((AX)^*(AX)) = s(X^*A^*AX) = 0$ and so $AX \in \mathcal{N}$ and the claim is done.

General algebra then tells us that we have a well-defined quotient map,

$$\widehat{L_A} : \mathcal{A}/\mathcal{N} \to \mathcal{A}/\mathcal{N},\ \widehat{L_A}(X+\mathcal{N}) = AX+\mathcal{N}.$$

The above inequality also tells us that this map is bounded on the inner product space $\mathcal{A}/\mathcal{N}$, since,

$$\|\widehat{L_A}(X+\mathcal{N})\|^2 = \langle AX+\mathcal{N}|AX+\mathcal{N}\rangle = s(X^*A^*AX) \leq \|A\|^2 s(X^*X) = \|A\|^2\|X+\mathcal{N}\|^2.$$

By HW1, we can extend this linear map by continuity to a bounded linear map, $\widetilde{L_A} : \mathcal{H} \to \mathcal{H}$ with $\|\widetilde{L_A}\| = \|\widehat{L_A}\|$.

Thus, we have a map, $\pi : \mathcal{A} \to B(\mathcal{H})$, $\pi(A) = \widetilde{L_A}$.

Some checking shows that the map π is a *-homomorphism.

To define the vector, we set $\phi = I + \mathcal{N}$. Then $\|\phi\|^2 = \langle\phi|\phi\rangle = s(I^*I) = s(I) = 1$.

Finally,

$$\langle\phi|\pi(A)\phi\rangle = \langle I+\mathcal{N}|A+\mathcal{N}\rangle = s(A).$$

This completes the outline of the proof.

This construction also leads to the following important theorem.

Theorem 7.6 (GNS Representation Theorem)**.** *Let $\mathcal{A}$ be a unital C*-algebra. Then there exists a Hilbert space and an isometric *-homomorphism, $\pi : \mathcal{A} \to B(\mathcal{H})$. Hence, $\mathcal{A}$ and the concrete C*-subalgebra $\mathcal{B} = \pi(\mathcal{A})$ are *-isomorphic.*

The idea of the proof is to for each state get a *-homomorphism and then take a direct sum of these *-homomorphisms and prove that there are enough states that this direct sum must be isometric.

7.2. **GNS and State Purification.** Suppose that we are given a density operator $\rho \in \mathcal{C}_1(\mathcal{H})$. This defines a linear functional,

$$s_\rho : B(\mathcal{H}) \to \mathbb{C} \text{ via } s_\rho(X) = Tr(X\rho).$$

Note that $s_\rho(I) = Tr(\rho) = 1$ and for any positive X^*X,

$$s_\rho(X^*X\rho) = Tr(X^*X\rho) = Tr(X\rho X^*) \geq 0,$$

since $X\rho X^* \geq 0$. Thus, s_ρ is a state and by GNS has a representation,

$$s_\rho(X) = \langle\phi|\pi(X)\phi\rangle.$$

In the case that $\rho = \sum_{i=1}^N \lambda_i |\phi_i\rangle\langle\phi_i|$ we can make this very explicit. Set $\phi = (\sqrt{\lambda_1}\phi_1, \ldots, \sqrt{\lambda_N}\phi_N) \in \mathcal{H}^{(N)}$, which is a unit vector, and let

$$\pi(X) = Diag(X) \in M_N(B(\mathcal{H})) = B(\mathcal{H}^{(N)}),$$

where by $Diag(X)$ we mean the diagonal operator matrix with X for the diagonal entry.

It is easily seen that $\pi : B(\mathcal{H}) \to M_N(B(\mathcal{H}))$ is a *-homomorphism and that $s_\rho(X) = \langle\phi|\pi(X)\phi\rangle$.

Thus, we have a very concrete GNS-like, in this case. This construction is generally referred to as **state purification**, as in the phrase, "by purifying

the state ensemble, we may regard it as a pure state on a larger HIlbert space". In this sense, the GNS representation shows that every state can be "purified".

Later we will talk about what it means for a state on a C*-algebra to be "pure". GNS does not say that every state is pure, just that it can be represented as a vector state, and we will see that vector states are pure states on $B(\mathcal{H})$.

A natural question is whether or not this concrete construction is the GNS, in an appropriate sense. The following result tells us how to recognize the GNS representation of a state.

Proposition 7.7. *Let $\mathcal{A}$ be a unital C*-algbra, let $s : \mathcal{A} \to \mathbb{C}$ be a state and let $\pi_s : \mathcal{A} \to B(\mathcal{H}_s)$, $\phi_s \in \mathcal{H}_s$ be the GNS representation of the state. Then*

$$\pi_s(\mathcal{A}) := \{\pi_s(A)\phi_s : A \in \mathcal{A}\}$$

*is a dense subset of $\mathcal{H}_s$. Moreover, let $\pi : \mathcal{A} \to B(\mathcal{H})$ be a unital *-homomorphims and let $\phi \in \mathcal{H}$ be a unit vector such that $\langle\phi|\pi(A)\phi\rangle = s(A)$ and such that $\pi(\mathcal{A})\phi$ is dense in $\mathcal{H}$, then there is a unitary $U : \mathcal{H}_s \to \mathcal{H}$ with $U\phi_s = \phi$ and $\pi(A) = U\pi_s(A)U^*$.*

Given a *-homomorphism π a vector ϕ is called **cyclic** if $\pi(\mathcal{A})\phi$ is dense in $\mathcal{H}$. Thus, the proposition says that, up to a unitary equivalence, any (π, ϕ) that gives rise to the state via the formula, $s(A) = \langle\phi|\pi(A)\phi\rangle$ with ϕ cyclic, is the GNS.

In the case that $\rho = \sum_{i=1}^N \lambda_i |\phi_i\rangle \langle\phi_i|$ considered above, with the representation $\pi(A) = Diag(A)$, the vector $\phi = (\sqrt{\lambda_1}\phi_1, ..., \sqrt{\lambda_N}\phi_N)$ might not be cyclic, so this might not be the GNS of the state on $\mathcal{A} = B(\mathcal{H})$. For example, if the vectors $\phi_1, ..., \phi_N$ are not linearly independent, then ϕ won't be cyclic.

However, if we use the spectral decomposition of ρ, then the vectors $\phi_1, ..., \phi_N$ will be orthonormal and in this case one can see that the vector ϕ is cyclic. This is because when the vectors are o.n., then given any set of vectors $h_1, ..., h_N$ we can always find an operator A such that $h_i = A(\sqrt{\lambda_i}\phi_i)$, $\forall i$.

7.3. **The C*-algebra $M_n(\mathcal{A})$.** Given a unital C*-algebra $\mathcal{A}$, we want to discuss how to make $M_n(\mathcal{A})$ into a C*-algebra. First note that it is always a vector space with operations, scalar multiplication $\lambda(A_{I,j}) = (\lambda A_{i,j})$ and addition $(A_{i,j}) + (B_{i,j}) = (A_{i,j} + B_{i,j})$. There is a natural way to make it an algebra too via the formula for matrix multiplication, $(A_{i,j}) \cdot (B_{i,j}) = (\sum_{k=1}^n A_{i,k}B_{k,j})$. If we set $(A_{i,j})^* = (A^*_{j,i})$ then we have a *-algebra. all that we are lacking to make it into a C*-algebra is a norm.

To find a norm, we use the GNS theorem. Take any $\pi : \mathcal{A} \to B(\mathcal{H})$ an isometric *-homomorphism, so that $\|A\| = \|\pi(A)\|$. We now define

$$\|(A_{i,j})\|_\pi := \|(\pi(A_{i,j})\|_{B(\mathcal{H}^{(n)})}.$$

It is easily checked that this norm makes $M_n(\mathcal{A})$ into a C*-algebra.

However, we have that the norm on a C*-algebra is unique, so any other way that we tried to create a norm, as long as it was a C*-norm, would necessarily be this norm.

Now that we know that every $M_n(\mathcal{A})$ is itself a C*-algebra, it makes sense to talk about completely positive maps between any two C*-algebras. Namely, if $\Phi : \mathcal{A} \to \mathcal{B}$ is a linear map, then we say that it is **n-positive** if whenever $(A_{i,j})$ is a positive element of the C*-algebra $M_n(\mathcal{A})$ then $(\Phi(A_{i,j}))$ is a positive element of the C*-algebra $M_n(\mathcal{B})$. As before a map is **completely positive** provided that it is n-positive for every n.

7.4. **Stinespring's dilation Theorem.**

Theorem 7.8 (Stinespring(1955))**.** *Let $\mathcal{A}$ be a unital C*-algebra, $\mathcal{H}$ a Hilbert space, and $\Phi : \mathcal{A} \to B(\mathcal{H})$ a completely positive map. Then there is a Hilbert space $\mathcal{K}$, a unital *-homomorphism $\pi : \mathcal{A} \to B(\mathcal{K})$ and $V \in B(\mathcal{H}, \mathcal{K})$ such that*

$$\Phi(A) = V^*\pi(A)V.$$

Moreover, every map of this form is completely positive.

For a complete proof see either [**?**] or [7].

We sketch the key ideas of the proof. First we take the vector space $\mathcal{A}\otimes\mathcal{H}$ and define a sesquilinear form by

$$B(\sum_i X_i \otimes h_i | \sum_j Y_j \otimes k_j) = \sum_{i,j} \langle h_i | \Phi(X_i^* Y_j) k_j.$$

One checks that this is positive semidefinite. To see, note that

$$(*) := B(\sum_{i=1}^N A_i \otimes h_i | \sum_{j=1}^N A_j \otimes h_j) = \langle h | (\Phi(A_i^* A_j)h\rangle,$$

where $h = (h_1, ..., h_n) \in \mathcal{H}^{(N)}$ and $(\Phi(A_i^*A_j)) = \Phi^{(N)}((A_i^*A_j)) \geq 0$, since Φ is N-positive and since $(A_i^*A_j) = X^*X \geq 0$, with X the matrix that has $A_1, ..., A_N$ for its first row and all other rows equal to 0. This shows that $(*) \geq 0$ and so B is positive semidefinite.

Let $\mathcal{N}$ be the null space of B. Our Hilbert space $\mathcal{K}$ will be the completion of the inner product space $(\mathcal{A} \otimes \mathcal{H})/\mathcal{N}$.

Now as in GNS for each $A \in \mathcal{A}$ we define a linear map $L_A : \mathcal{A}\otimes\mathcal{H} \to \mathcal{A}\otimes\mathcal{H}$ via $L_A(\sum_i X_i \otimes h_i) = \sum_i (AX_i)\otimes h_i$ and check that $L_A(\mathcal{N}) \subseteq \mathcal{N}$. This allows us to define a linear map on the quotient, $\widehat{L_A} : (\mathcal{A} \otimes \mathcal{H})/\mathcal{N} \to (\mathcal{A} \otimes \mathcal{H})/\mathcal{N}$ which we show is bounded and so extends to an operator, $\pi(A) : \mathcal{K} \to \mathcal{K}$. This defines our *-homomorphism.

To define $V : \mathcal{H} \to \mathcal{K}$ we set $V(h) = I_{\mathcal{A}} \otimes h + \mathcal{N}$ and check that it is linear and bounded.

Finally, to see that this gives us what we want we compute,

$$\begin{aligned}\langle h | V^*\pi(A)Vk\rangle_{\mathcal{H}} = \langle Vh | \pi(A)Vk\rangle_{\mathcal{K}} &= \langle I_{\mathcal{A}} \otimes h + \mathcal{N} | A \otimes k + \mathcal{N}\rangle_{\mathcal{K}} \\ &= B(I_{\mathcal{A}} \otimes h | A \otimes k) = \langle h | \Phi(A)k\rangle_{\mathcal{H}}.\end{aligned}$$

Since this is true for all pairs of vectors, we have that $V^*\pi(A)V = \Phi(A)$.

7.5. **More on Tensor Products.** Given $A = (a_{i,j}) : \mathbb{C}^n \to \mathbb{C}^n$ and $B = (b_{k,l}) : \mathbb{C}^d \to \mathbb{C}^d$ we have a linear map $A \otimes B : \mathbb{C}^n \otimes \mathbb{C}^d \to \mathbb{C}^n \otimes \mathbb{C}^d$. We would like to look at matrix representations of htis map. Recall that to write down a matrix for a linear map one wants an **ordered** basis for the space. If $\{e_i : 1 \leq i \leq n\}$ and $\{f_k : 1 \leq k \leq d\}$ are the canonical onb's, then we know that $\{e_i \otimes f_k : 1 \leq i \leq n, 1 \leq k \leq d\}$ is an orthonormal basis for $\mathbb{C}^n \otimes \mathbb{C}^d$.

There are two natural ways to order this basis, one is as

$$e_1 \otimes f_1, e_2 \otimes f_1, ..., e_n \otimes f_1, e_1 \otimes f_2, ..., e_n \otimes f_2, ..., e_n \otimes f_d,$$

when we group these into blocks of n, this corresponds to the decomposition

$$\mathbb{C}^n \otimes \mathbb{C}^d \sim (\mathbb{C}^n \otimes f_1) \oplus \cdots \oplus (\mathbb{C}^n \otimes f_d) \sim (\mathbb{C}^n)^{(d)}.$$

With respect to this ordering,

$$A \otimes B \sim (b_{k,l}A) \in M_d(M_n).$$

Alternatively, we may order the basis as,

$$e_1 \otimes f_1, e_1 \otimes f_2, ..., e_1 \otimes f_d, e_2 \otimes f_1, ..., e_2 \otimes f_d, ..., e_n \otimes f_d,$$

when we group these into blocks of size d this corresponds to the decomposition

$$\mathbb{C}^n \otimes \mathbb{C}^d \sim (e_1 \otimes \mathbb{C}^d) \oplus \cdots (e_n \otimes \mathbb{C}^d) \sim (\mathbb{C}^d)^{(n)}.$$

With repsect to this ordering,

$$A \otimes B \sim (a_{i,j}B) \in M_n(M_d).$$

In particular these two $(nd) \times (nd)$ matrices are unitarily equivalent by the permutation unitary that takes one ordering to the other.

When $B = I_d$ this gives us two matrix representations,

$$A \otimes I_d \sim Diag(A) \sim (a_{i,j}I_d).$$

7.6. **The Finite Dimensional Version of Stinespring.** We want to look at what Stinespring's theorem says in the case that $\mathcal{A} = M_d$ and $\mathcal{H} = \mathbb{C}^r$, so that we have a CP map $\Phi : M_d \to B(\mathbb{C}^r) = M_r$.

In this case the Hilbert space $\mathcal{K}$ is obtained by completing $(M_d \otimes \mathbb{C}^r)/\mathcal{N}$. But this space is finite dimensional and every finite dimensional inner product space is already complete, so that $\mathcal{K} = (M_d \otimes \mathbb{C}^r)/\mathcal{N}$ and in particular,

$$dim(\mathcal{K}) \leq d^2 r.$$

Now let $\{E_{i,j} = |e_i\rangle \langle e_j| : 1 \leq i, j \leq d\}$ be the canonical basis for M_d and let the Stinespring representation, be $\Phi(X) = V^*\pi(X)V$ with $V : \mathbb{C}^r \to \mathcal{K}$ and $\pi : M_d \to B(\mathcal{K})$. Because π is a unital *-homomorphism, it follows that $\pi(E_{i,i})$ is the orthogonal projection onto some subspace $\mathcal{M}_i$ of $\mathcal{K}$. Because

$$I_{\mathcal{K}} = \pi(I_d) = \sum_i \pi(E_{i,i}),$$

we see that

$$\mathcal{K} = \mathcal{M}_1 \oplus \mathcal{M}_2 \oplus \cdots \mathcal{M}_d.$$

Moreover, because $E^*_{i,j}E_{j,j} = E_{j,j}$ and $E_{i,j}E^*_{i,j} = E_{i,i}$ we see that $\pi(E_{i,j}$ defines an isometry from $\mathcal{M}_j$ onto $\mathcal{M}_i$. This guarantees that $dim(\mathcal{M}_i) = dim(\mathcal{M}_j)$ and if that if we use the maps $\pi(E_{i,j})$ to identify these as all the same space $\mathcal{M}$, then

$$\mathcal{K} = \mathcal{M}^{(d)},$$

and the maps $\pi(E_{i,j})$ just act as permutations of the j-th copy of $\mathcal{M}$ to the i-th copy.

We also have that, $d \cdot dim(\mathcal{M}) = dim(\mathcal{K}) \leq d^2 r$, so that

$$m := dim(\mathcal{M}) \leq dr.$$

With these identifications, for $X = (x_{i,j}) = \sum_{i,j=1}^{d} x_{i,j}E_{i,j}$, we have that

$$\pi(X) = (x_{i,j}I_{\mathcal{M}}).$$

But up to a permutation, we may also regard

$$\mathcal{K} \sim (\mathbb{C}^d)^{(m)},$$

and now

$$\pi(X) = Diag(X),$$

the block diagonal matrix of m copies of X, and now $V : \mathbb{C}^r \to \mathcal{K} = (\mathbb{C}^d)^{(m)}$ has the form

$$Vh = (V_1 h, \ldots, V_m h)^t,$$

for maps $V_i : \mathbb{C}^r \to \mathbb{C}^d$, i.e., $d \times r$ matrices.

With these identifications,

$$\Phi(X) = V^* Diag(X) V = \sum_{i=1}^{m} V_i^* X V_i.$$

This last form of Φ is often called a **Choi-Kraus** representation of Φ.

Note that our proof shows that the Choi-Kraus representation can always be taken to have fewer than dr terms.

A few things to note. If Φ is UCP, then

$$I_r = \Phi(I_d) = \sum_{i=1}^{m} V_i^* V_i.$$

On the other hand if Φ is CPTP, then

$$Tr(X) = Tr(\Phi(X)) = Tr(\sum_{i=1}^{m} V_i^* X V_i) = Tr((\sum_{i=1}^{m} V_i V_i^*)X), \forall X,$$

from which it follows that

$$\sum_{i=1}^{m} V_i V_i^* = I_d.$$

Thus, we see that every CPTP $\Phi : B(\mathbb{C}^d) = \mathcal{C}_1(\mathbb{C}^d) \to B(\mathbb{C}^r) = \mathcal{C}_1(\mathbb{C}^r)$ corresponds to the quantum channel induced by an m outcome measurement system,

$$\{V_1^*, ..., V_m^*\},$$

between the initial space $\mathbb{C}^d$ and the final space $\mathbb{C}^r$.

Perhaps the key takeaway of this subsection is the following.

Corollary 7.9. *Every CPTP map $\Phi : M_d \to M_r$ is the quantum channel induced by an m-outcome measurement system, $\{V_1^*, ..., V_m^* : \mathbb{C}^d \to \mathbb{C}^r$.*

Thus, in finite dimensions the set of CPTP maps and the set of quantum channels induced by measurement systems coincide.

7.7. **Choi's Theorem.** Let $E_{i,j}, 1 \leq i, j \leq d$ denote the matrix units in M_d and let

$$(E_{i,j}) = \sum_{i,j=1}^{d} E_{i,j} \otimes E_{i,j} \in M_d(M_d),$$

denote the matrix of matrix units. Given any linear map $L : M_d \to M_r$ it is uniquely determined by its values on the basis of matrix units. Consequently, the map $L \to L^{(d)}((E_{I,j})) = (L(E_{i,j})) \in M_d(M_r)$, is a vector space isomorphism from $\mathcal{L}(M_d, M_r)$ onto $M_d(M_r)$. The matrix $C_L := (L(E_{i,j}))$ is called the **Choi matrix** or **Choi-Jamliokowska matrix** of the map.

Note that $E_{i,j} = |e_i\rangle \langle e_j|$ and so

$$\sum_{i,j=1}^{d} E_{i,j} \otimes E_{i,j} = \sum_{i,j=1}^{d} |e_i \otimes e_i\rangle \langle e_j \otimes e_j| = |u\rangle \langle u| \geq 0,$$

where $u = \sum_{i=1}^{d} e_i \otimes e_i$. The normalized vector $\frac{u}{\sqrt{d}}$ is called the **maximally entangled state**. The key point is that this shows that the matrix of matrix units is positive.

Theorem 7.10 (Choi)**.** *Let $\Phi : M_d \to M_r$ The following are equivalent.*

1. *Φ is completely positive,*
2. *Φ is d-positive,*
3. *$C_\Phi := (\Phi(E_{i,j})) \geq 0$ in $M_d(M_r) = M_{dr}$,*
4. *there exist $V_i : \mathbb{C}^r \to \mathbb{C}^d$, $1 \leq i \leq m \leq dr$, such that $\Phi(X) = \sum_{i=1}^{m} V_i^* X V_i$.*

Clearly (1) implies (2), and (2) implies (3) since the matrix of matrix units is positive. It is easily checked that any map of the form given in (4) is completely positive. The beauty of Choi's proof is that he gives a concrete way, from the positive matrix C_Φ to construct the matrices V_i.

For the details of the proof see either [2] or [7].

7.8. **Banach Space Adjoints versus Hilbert Space Adjoints.** We know that given two Hilbert spaces, $\mathcal{H}, \mathcal{K}$ and $T \in B(\mathcal{H}, \mathcal{K})$ that it has an adjoint $T^* \in B(\mathcal{K}, \mathcal{H})$ satisfying the adjoint equation,

$$\langle k|Th\rangle_{\mathcal{K}} = \langle T^*k|h\rangle_{\mathcal{H}}.$$

Given two Banach spaces, X, Y, too avoid overuse of the star symbol, we denote their dual spaces by X^d, Y^d. Given $T \in B(X, Y)$ there is similarly an adjoint operator $T^d \in B(Y^d, X^d)$ defined as follows, for $f \in Y^d$,

$$T^d(f) = f \circ T : X \to \mathbb{C}.$$

Note that

$$|T^d(f)(x)| = |f(T(x))| \leq \|f\|\|T(x)\|_Y \leq \|f\|\|T\|\|x\|_X,$$

which shows that $\|T^d(f)\| \leq \|f\|\|T\|$. Thus, $T^d(f) \in X^d$ and $\|T^d\| \leq \|T\|$. Using the Hahn-Banach theorem one can show that in fact $\|T^d\| = \|T\|$.

If one thinks of the pairing between a functional $f \in X^d$ and a vector $x \in X$ as defining a bilinear map,

$$\langle f|x\rangle_X : X^d \times X \to \mathbb{C},$$

then we see that,

$$\langle f|T(x)\rangle_Y = \langle T^d(f)|x\rangle_X.$$

Thus, the map T^d satisfies this *adjoint equation*.

The key differences are that this pairing is bilinear, not sesquilinear as for Hilbert spaces, and that the pairing is generally between different spaces, since the dual of a Banach space is generally an entirely different space.

One can easily check that when ever the sums or products are defined that, $(T + R)^d = T^d + R^d$, $(T \circ R)^d = R^d \circ T^d$. But if $\lambda \in \mathbb{C}$, then $(\lambda T)^d = \lambda T^d$, unlike for the Hilbert space adjoint.

In the case that $X = \mathbb{C}^n$ with some norm, $X^d = \mathbb{C}^n$ but with a different norm and every functional $f : X \to \mathbb{C}$ is just given by the dot product, i.e., $f(x) = f_w(x) = \sum_{i=1}^n w_i x_i$. Note that if we view x as a column vector and w as a row vector, this is just the matrix product. If $Y = \mathbb{C}^m$ is another finite dimensional Banach space with $Y^d = \mathbb{C}^m$ via dot product and $A : X \to Y$ is represented by a matrix $A = (a_{i,j})$, then

$$A^d = A^t : \mathbb{C}^m \to \mathbb{C}^n.$$

This can be seen by the equation, $f = f_w \in \mathbb{C}^m$ then

$$A^d(f_w)(x) = f_w(Ax) = w \cdot (Ax) = w(Ax) = (wA)x = (A^t w^t)^t x,$$

Finally, one important property of the adjoint of a map, has to do with the **weak*-topology** which exists on dual spaces. Recall that we say that a **net** of functional $\{f_\lambda\}_{\lambda \in \Lambda} \subseteq X^d$ **converges in the weak*-topology** to $f \in X^d$ if for every $x \in X$ the net of numbers, $\{f_\lambda(x)\}_{\lambda \in \Lambda}$ converges to $f(x)$. This is the same as saying that the functionals f_λ converge **pointwise**

to f. One very important property of the weak*-topology is the **Banach-Alaoglu theorem** which says that the unit ball of a dual space is always compact in the weak*-topology.

The other key property that we shall use is that if $T \in B(X,Y)$ then not only is $T^d \in B(Y^d, X^d)$ but T^d is also **weak*-to-weak* continuous**, i.e., continuous between these two topological spaces.

See [3] for these facts.

7.9. **The Dagger of a Map versus its Adjoint.** Recall that $\mathcal{C}_1(\mathcal{H})^d = B(\mathcal{H})$. Formally, this means that if $f : \mathcal{C}_1(\mathcal{H}) \to \mathbb{C}$ is a bounded linear functional, then there exists a unique $W \in B(\mathcal{H})$ such that

$$f(X) = f_W(X) := Tr(WX),$$

and $\|f_W\| = \|W\|$. Now if $\Phi : \mathcal{C}_1(\mathcal{H}) \to \mathcal{C}_1(\mathcal{K})$ is bounded, then via these identifications,

$$\Phi^d : B(\mathcal{K}) \to B(\mathcal{H}).$$

Unraveling these, if $W \in B(\mathcal{K})$, it defines $f_W : \mathcal{C}_1(\mathcal{K}) \to \mathbb{C}$ and $\Phi^d(f_W) : \mathcal{C}_1(\mathcal{H}) \to \mathbb{C}$ is the map given by $\Phi^d(f_W)(X) = Tr(W\Phi(X))$. Since this is a bounded linear functional, there exists a unique $Z \in B(\mathcal{H})$ such that

$$Tr(W\Phi(X)) = f_Z(X) = Tr(ZX).$$

Thus, $\Phi^d(W) = Z$ is the unique operator satisfying the adjoint equation,

$$Tr(W\Phi(X)) = Tr(\Phi^d(W)X).$$

Physicists prefer to pretend that the pairing between $\mathcal{C}_1(\mathcal{H})$ and $B(\mathcal{H})$ is an inner product, even though in infinite dimensions the spaces are different. Given $W \in B(\mathcal{H})$ and $X \in \mathcal{C}_1(\mathcal{H})$ they set

$$\langle W|X\rangle = Tr(W^*X).$$

Given $\Phi : \mathcal{C}_1(\mathcal{H}) \to \mathcal{C}_1(\mathcal{K})$ they define $\Phi^\dagger(W) = Z$ where $Z \in B(\mathcal{H})$ is the unique operator satisfying the equation,

$$Tr(W^*\Phi(X)) = Tr(Z^*X).$$

To see the correspondence with the Banach space adjoint, note that

$$Tr(W^*\Phi(X)) = Tr(\Phi^d(W^*)X) = Tr(Z^*X),$$

so that

$$\Phi^\dagger(W) = Z = \Phi^d(W^*)^*.$$

Generally, $\Phi^\dagger \neq \Phi^d$. However, in the case that Φ^d is CP, which is the case that we will be interested in, by Stinespring $\Phi^d(W) = V^*\pi(W)V$ and hence,

$$\Phi^\dagger(W) = \Phi^d(W^*)^* = \left(V^*\pi(W^*)V\right)^* = V^*\pi(W^*)^*V^{**} = V^*\pi(W)^{**}V = \Phi^d(W),$$

using that π is a *-homomorphism.

7.10. **The Finite Dimensional Case.** In the case that $\Phi : M_d \to M_r$ is CP we know that $\Phi(X) = \sum_{i=1}^m V_i^* X V_i$ and hence

$$Tr(\Phi^d(Y)X) = Tr(Y\Phi(X)) = \sum_{i=1}^m Tr(YV_i^* X V_i) = \sum_{i=1}^m Tr(V_i Y V_i^* X),$$

and it follows that

$$\Phi^d(Y) = \sum_{i=1}^m V_i Y V_i^*.$$

7.11. **The Infinite Dimensional Case.** We now prove a similar formula in the infinite dimensional case.

Theorem 7.11. *Let $\Phi : \mathcal{C}_1(\mathcal{H}) \to \mathcal{C}_1(\mathcal{K})$ be CP, then $\Phi^d : B(\mathcal{K}) \to B(\mathcal{H})$ is CP, weak*-to-weak* continuous and $\Phi^d = \Phi^\dagger$.*

Proof. To prove the theorem we only need to prove that Φ^d is CP. To this end, let $P_{i,j} \in B(\mathcal{K})$, $1 \leq i, j \leq n$ be chosen such that $P = (P_{i,j}) \geq 0$ as an operator on $\mathcal{K}^{(n)}$. Fix an arbitrary set of vectors $h_1, ..., h_n \in \mathcal{H}$, and let $h = (h_1, ..., h_n)^t \in \mathcal{H}^{(n)}$. We must prove that

$$(*) = \langle h | \big(\Phi^d(P_{i,j})\big) h \rangle_{\mathcal{H}^{(n)}} = \sum_{i,j=1}^n \langle h_i | \Phi^d(P_{i,j}) h_j \rangle_{\mathcal{H}} \geq 0.$$

Note that

$$\langle h_i | \Phi^d(P_{i,j}) h_j \rangle = Tr_{\mathcal{H}}(\Phi^d(P_{i,j}) \left|h_j\right\rangle \left\langle h_i\right|) = Tr_{\mathcal{K}}(P_{i,j}\Phi(\left|h_j\right\rangle \left\langle h_i\right|)).$$

Thus, $(*)$ becomes,

$$\sum_{i,j=1}^n Tr_{\mathcal{K}}\big(P_{i,j}\Phi(\left|h_j\right\rangle \left\langle h_i\right|)\big) = Tr_{\mathcal{K}^{(n)}}\big(\big(P_{i,j}\big)\big(\Phi(\left|h_i\right\rangle \left\langle h_j\right|)\big)\big) \geq 0,$$

since $(P_{i,j}) \geq 0$, $(\left|h_i\right\rangle \left\langle h_j\right|) \geq 0$ and Φ is CP. □

We are now able to sketch the proof of the main result.

Definition 7.12. Given operators $T_a \in B(\mathcal{H})$, $a \in A$ and $T \in B(\mathcal{H})$ we write

$$s - \sum_{a \in A} T_a = T,$$

and say that the **series converges in the strong operator topology to T** provided that for every vector $h \in \mathcal{H}$ we have that the series of vectors $\sum_{a \in A} T_a h$ converges in norm to Th.

Recall that this last equation means that for every $\epsilon > 0$ we can find a finite set $F_0 \subseteq A$ such that for every finite set F with $F_0 \subseteq F \subseteq A$, we have that $\| \sum_{a \in F} T_a h - Th \| < \epsilon$.

Theorem 7.13. *Let $\Phi : \mathcal{C}_1(\mathcal{H}) \to \mathcal{C}_1(\mathcal{K})$ be CPTP, then there exist operators $V_a : \mathcal{H} \to \mathcal{K}$, $a \in A$ such that $s - \sum_{a\in A} V_a^* V_a = I_{\mathcal{K}}$ and*

$$\Phi(X) = \sum_{a\in A} V_a X V_a^*,$$

where the convergence is in the norm topology.

The proof is very similar to the finite dimensional case, with a few extra bits to take care of the topology. First, we have that $\Phi^d : B(\mathcal{K}) \to B(\mathcal{H})$ is UCP and weak*-to-weak* continuous. Thus, by Stinespring, there exists a Hilbert space $\mathcal{L}$, a *-homomorphism, $\pi : B(\mathcal{K}) \to B(\mathcal{L})$ and a map $V : \mathcal{H} \to \mathcal{L}$ such that $\Phi^d(X) = V^*\pi(X)V$. The fact that Φ^d is unital tells us that $V^*V = I_{\mathcal{H}}$.

Pick an o.n.b. $\{e_i : i \in I\}$ for $\mathcal{K}$ and let $E_{i,j} = |e_i\rangle \langle e_j|$. It is easy to check that

$$s - \sum_{i\in I} E_{i,i} = I_{\mathcal{K}}.$$

From this it follows that for every $X \in \mathcal{C}_1(\mathcal{H})$ we have that

$$\sum_{i\in I} E_{i,i} X = X,$$

in $\mathcal{C}_1$ norm. To see this claim write $X = \sum_{n\in\mathbb{N}} s_n(X) |\phi_n\rangle \langle\psi_n|$ in its SVD, which is a norm convergent sum. Pick a large enough integer N so that $\sum_{n=N}^{\infty} s_n(X) < \epsilon$ and set $X_N = \sum_{n=1}^{N} s_n(X) |\phi_n\rangle \langle\psi_n|$. Then we will have that $\|X - X_N\|_1 < \epsilon$.

Now pick a finite set F_0 so that for every finite set $F_0 \subseteq F \subseteq I$ we have that $\| \sum_{i\in F} E_{i,i} |\phi_n\rangle - |\phi_n\rangle \| < \epsilon/N$, for $1 \leq n \leq N$. From this it follows that

$$\| \sum_{i\in F} E_{i,i} X_N - X_N\|_1 < \epsilon.$$

Then we have that

$$\| \sum_{i\in F} E_{i,i} X - X\|_1 = \|(\sum_{i\in F} E_{i,i})(X - X_N) + \big((\sum_{a\in A} E_{i,i} X_N - X_N) + \big(X_N - X\big)\|_1 < 3\epsilon$$

and the claim follows.

Next note that

$$Tr\big(\Phi^d(\sum_{i\in F} E_{i,i})X\big) = Tr\big((\sum_{i\in F} E_{i,i})\Phi(X)\big) \to tr(\Phi(X)),$$

as F grows by our last estimate. Although we haven't covered this, this equation exactly shows that $\sum_{i\in I} \Phi^d(E_{i,i}) = I_{\mathcal{K}}$ in the weak*-topology, which is often written as

$$wk* - \sum_{i\in I} \Phi(E_{i,i}) = I_{\mathcal{K}}.$$

Now as in the finite dimensional case, we note that $\pi(E_{i,i})$ is an orthogonal projection onto a subspace $\mathcal{M}_i \subseteq \mathcal{L}$, with $\mathcal{M}_i \perp \mathcal{M}_j$, $\forall i \neq j$, and the

operators $\pi(E_{i,j})$ define partial isometries between these spaces, showing that they all have the same dimension.

In the case that $\mathcal{K}$ was finite dimensional, we had that the finite sum $\sum_{i\in I}\pi(E_{i,i}) = I_{\mathcal{L}}$ and so these spaces gave us all of $\mathcal{L}$.

The hard part of the infinite dimensional case is to show that the same holds, namely that,

$$\mathcal{L} = \sum_{i\in I} \mathcal{M}_i,$$

or equivalently, that if $v \in \mathcal{L}$ and $v \perp \mathcal{M}_i, \forall i$ implies that $v = 0$.

This follows by using the fact that in the Stinespring representation, vectors that are finite sums of vectors of the form $\pi(Y)Vk$, $Y \in B(\mathcal{K})$, $k \in \mathcal{K}$ are dense in $\mathcal{L}$. Using this one can then show that

$$s - \sum_{i\in I} \pi(E_{i,i}) = I_{\mathcal{L}}.$$

We leave the details to the interested reader.

Using these fact we can write

$$\mathcal{L} \sim \mathcal{K} \otimes \mathcal{M} \sim \mathcal{K}^{(d)},$$

where $d = dim(\mathcal{M})$ is possibly infinite, and $\pi(Y) \sim Y \otimes I_{\mathcal{M}} \sim diag(Y)$, as in the finite dimensional case.

With these identifications, $V; \mathcal{H} \to \mathcal{L}$ is identified with operators, $V_a : \mathcal{H} \to \mathcal{K}$, $a \in A$ where A is the index set for an o.n.b. for $\mathcal{M}$. The fact that $V^*V = I_{\mathcal{H}}$ implies that

$$s - \sum_{a\in A} v_a^* V_a = I_{\mathcal{H}}$$

and

$$\Phi^d(Y) = V^*\pi(Y)V = V^*diag(Y)V = s - \sum V_a^* Y V_a.$$

Finally, via the pairing we get that

$$Tr(Y\Phi(X)) = Tr(\Phi^d(Y)X) = Tr(s - \sum_{a\in A} V_a^* Y V_a X) = \sum_{a\in A} Tr(Y V_a X V_a^*),$$

and with a careful use of functional analysis, one can show that the series,

$$\sum_{a\in A} V_a X V_a^*$$

converges in the norm topology to $\Phi(X)$.

7.12. **Back to axioms for quantum channels.** We saw earlier that to satisfy the axioms a map needed to be CPTP. We now know that CPTP maps satisfy all of the axioms except possibly the axiom for bipartite systems. We now show that CPTP maps satisfy this axiom too.

So suppose that we have $\Phi_A : \mathcal{C}_1(\mathcal{H}_{A,i}) \to \mathcal{C}_1(\mathcal{H}_{A,o})$, $\Phi_B : \mathcal{C}_1(\mathcal{H}_{B,i}) \to \mathcal{C}_1(\mathcal{H}_{B,o})$ both CPTP maps. We then know that there exist operators, $V_i : \mathcal{H}_{A,i} \to \mathcal{H}_{A,o}$, $i \in I$, $W_j : \mathcal{H}_{B,i} \to \mathcal{H}_{B,o}$ such that $s - \sum_{i\in I} V_i^* V_i = I_{H_{A,i}}$, $s - \sum_{j\in J} W_j^* W_j = I_{H_{B,i}}$ with $\Phi_A(X) = \sum_{i\in I} V_i X V_i^*$, $\Phi_B(Y) = \sum_{j\in J} W_j Y W_j^*$.

It then follows that

$$s - \sum_{i\in I, j\in J} (V_i \otimes W_j)^*(V_i \otimes W_j) = I_{H_{A,i}\otimes H_{B,i}},$$

and that if we define a map

$$\Phi_{AB} : \mathcal{C}_1(\mathcal{H}_{A,i} \otimes \mathcal{H}_{B,i}) \to \mathcal{C}_1(\mathcal{H}_{A,o} \otimes \mathcal{H}_{B,o}),$$

via

$$\Phi_{AB}(Z) = \sum_{i\in I, j\in J} (V_i \otimes W_j)Z(V_i \otimes W_j)^*,$$

then this is a CPTP map and $\Phi_{AB}(X \otimes Y) = \Phi_A(X) \otimes \Phi_B(Y)$.

Thus, any family of maps that satisfy the axiom must all be CPTP and the CPTP maps satisfy the axioms. So henceforth, we shall consider the terms "quantum channel" to be synonymous with "CPTP maps defined on the trace class operators".

The duals, or daggers, of quantum channels are exactly the UCP maps defined on spaces of bounded operators, that are also weak*-to-weak*-continuous.

We end with an example. Let $\Phi : \mathcal{C}_1(\ell^2_{\mathbb{N}}) \to \mathcal{C}_!(\ell^2_{\mathbb{N}})$ be defined by

$$\Phi((x_{i,j})) = Diag(x_{1,1}, x_{2,2}, \ldots).$$

We have that $s - \sum_{i\in\mathbb{N}} E_{i,i} = I$, but this sum is not norm convergent, and $\Phi(X) = \sum_{i\in\mathbb{N}} E_{i,i}XE_{i,i}$. This latter sum is seen to be norm convergent, since

$$\|\Phi(X) - \sum_{i=1}^{N} E_{i,i}XE_{i,i}\|_1 = \|Diag(0, ..., 0, x_{N+1,N+1}, ...)\|_1 = \sum_{i=N+1}^{\infty} |x_{i,i}| \to 0,$$

as $N \to +\infty$, since $Tr(X)$ is absolutely convergent.

8. Applications of other C*-algebras in QIT

An algebra is called **abelian** or **commutative** provided that $ab = ba$, $\forall a, b$ in the algebra.

Given a compact Hausdorrf space X, we let

$$C(X) = \{f : X \to \mathbb{C} | f \text{ is continuous } \},$$

given two functions $f, g \in C(X)$ we let $f + g$ and fg denote their pointwise sum and product, which makes $C(X)$ an abelian algebra. By setting f^* equal to the complex conjugate of f and

$$\|f\| = \|f\|_\infty := \sup\{|f(x)| : x \in X\},$$

we obtain a unital, abelian C*-algebra. By a theorem of Gelfand and Naimark, all unital abelian C*-algebras are of this form.

Theorem 8.1 (Gelfand-Naimark)**.** *Let $\mathcal{A}$ be a unital, abelian C*-algebra, then there exists a compact Hausdorff space X and a unital *-isomorphism, $\pi : \mathcal{A} \to C(X)$.*

Earlier we remarked that any time that we had a C*-algebra $\mathcal{A}$, then it had a unique C*-norm. We used this to argue that the C*-norm on $M_n(\mathcal{A})$ was unique. Ergo, $M_n(C(X))$ has a unique C*-norm, so it is interesting to see what it is. Note that if we let $C(X; M_n)$ denote the set of continuous functions from X into M_n, then this can be naturally made into a C*-algebra as follows:

- given $F, G \in C(X; M_n)$ define $F + G$ and $F \cdot G$ to be their pointwise sum and product,
- define F^* to be the function that is the pointwise conjugate transpose of F,
- define $\|F\| := \sup\{\|F(x)\|_{M_n} : x \in X\}$,

where the norm of a matrix $\|A\|_{M_n}$ is its norm as an operator on the Hilbert space $\mathbb{C}^n$. With this norm and operations, $C(X; M_n)$ is easily seen to be a unital C*-algebra.

Now if we identify $(f_{i,j}) \in M_n(C(X))$ with the function $F(x) = (f_{i,j}(x))$, then this is easily seen to define an algebraic *-isomorphism between these two algebras. Thus, the unique norm making $M_n(C(X))$ into a C*-algebra is

$$\|(f_{i,j})\| = \sup\{\|(f_{i,j}(x))\|_{M_n} : x \in X\}.$$

Another important theorem about abelian C*-algebras is due to Stinespring.

Theorem 8.2 (Stinespring)**.** *Let $\mathcal{A}, \mathcal{B}$ be unital C*-algebras and let $\Phi : \mathcal{A} \to \mathcal{B}$ be a positive map. If one of the two algebras is abelian, then Φ is completely positive.*

For a few examples of abelian C*-algebras, we note that if $H = H^* \in B(\mathcal{H})$, then the subalgebra $\mathcal{A}$ of $B(\mathcal{H})$ generated by $\{I, H\}$ is an abelian C*-algebra. By the spectral theory for a self-adjoint operator, $\mathcal{A}$ is *-isomorphic to $C(\sigma(H))$.

If we let $\mathcal{D}_n \subseteq M_n$ denote the C*-subalgebra of diagonal matrices, then this is *-isomorphic to the continuous functions on the finite set $\{1, 2, ..., n\}$, with the *-isomorphism defined by sending $D = Diag(d_1, ..., d_n) \in \mathcal{D}_n$ to the function $f \in C(\{1, ..., n\})$ defined by $f(i) = d_i$. This C*-algebra is often denoted ℓ_n^∞ and regarded as the set of n-tuples with pointwise sum and product. We shall let δ_i denote the function

$$\delta_i(j) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

Note that these functions span the C*-algebra ℓ_n^∞ and are orthogonal projections, i.e., $\delta_i = \delta_i^2 = \delta_i^*$ and $\delta_i \delta_j = 0, i \neq j$.

8.1. **K Outcome POVM's.** Recall that a K outcome measurement system on an input state space $\mathcal{H}_i$ is given by an output Hilbert space $\mathcal{H}_o$ and

operators $T_k : \mathcal{H}_i \to \mathcal{H}_o$ such that if we are in state ψ then the probability of observing outcome k is

$$p_k = \langle T_k\psi | T_k\psi\rangle = \langle \psi | T_k^* T_k \psi\rangle.$$

The operators $P_k = T_k^* T_k$ are positive, sum to one and

$$p_k = \langle \psi | P_k \psi\rangle.$$

Thus, if we are only interested in the probabilities of outcomes, all that matters are the positive operators P_k. Also note that $\sum_{k=1}^K P_k = I_{\mathcal{H}_i}$.

A set of operators $P_1, ..., P_K \in B(\mathcal{H})$ is called a **K outcome positive operator-valued measure** or **K-POVM** provided that they are positive and sum to the identity. A K-POVM is called a **K outcome projection-valued measure** or **K-PVM** when each P_k is a projection, i.e., $P_k = P_k^2 = P_k^*, \forall k$.

Given a K-POVM, define $\Phi : \ell_K^\infty \to B(\mathcal{H})$ by

$$\Phi(\sum_{k=1}^K a_k \delta_k) = \sum_{k=1}^K a_k P_k.$$

It is not hard to see that this map is unital and positive. Hence, by Stinespring's theorem it is UCP. Conversely, given any unital positive map $\Phi : \ell_K^\infty \to B(\mathcal{H})$ if we set $P_k = \Phi(\delta_k)$ then this defines a K-POVM.

Thus, studying K-POVM's is the same as studying UCP maps on ℓ_K^∞.

By Stinespring's dilation theorem, given a K-POVM on $\mathcal{H}$, there is another Hilbert space $\mathcal{K}$, an isometry $V : \mathcal{H} \to \mathcal{K}$ and a unital *-homomorphism, $\pi : \ell_K^\infty \to B(\mathcal{K})$ such that

$$P_k = V^* \pi(\delta_k) V, 1 \leq k \leq K.$$

Note that if we set $E_k = \pi(\delta_k)$ then $\{E_1, ..., E_K\}$ is a K-PVM on $\mathcal{K}$.

Thus, each K-POVM dilates to a K-PVM and this process is often called a **purification** of the K-POVM.

In this simple case it is possible to carry out this process directly. If we set $\mathcal{K} = \mathcal{H}^{(K)}$, let E_k denote the projection onto the k-th copy of $\mathcal{H}$, and define $V : \mathcal{H} \to \mathcal{H}^{(K)}$ by $Vh = (P_1^{1/2}h, ..., P_K^{1/2}h)$, then it is not hard to see that $P_k = V^* E_k V, 1 \leq k \leq K$. Thus, we have obtained a Stinespring-like dilation. However, this dilation will often not satisfy the minimality property needed to be equivalent to *the* Stinespring dilation.

8.2. **Quantum Marginals, Operator Systems, and Arveson's Extension Theorem.** Suppose that Alice and Bob are sharing a state space $\mathcal{H}$, Alice has outcomes, $1 \leq k \leq K$, and Bob has outcomes $1 \leq j \leq J$. Then we can discuss the probability that Alice observes outcome k and Bob observes outcome j. In this case we have a joint probability density given by a POVM $\{R_{k,j} : 1 \leq k \leq K, 1 \leq j \leq J\}$, i.e., $R_{k,j} \geq 0$ and $\sum_{k,j=1}^{K,J} R_{k,j} = I_{\mathcal{H}}$. such

that when the lab is in state ψ then the probability of the joint observation (k, j) is given by

$$p(k, j) = \langle \psi | R_{k,j} \psi \rangle.$$

If we set

$$P_k = \sum_{j=1}^{J} R_{k,j}, \text{ and } Q_j = \sum_{k=1}^{K} R_{k,j},$$

then these are two POVM's called the **quantum marginals** with the property that

$$p_A(k) := \langle \psi | P_k \psi \rangle, \; p_B(j) := \langle \psi | Q_j \psi \rangle,$$

gives the probability that Alice will observe outcome k and that Bob will observe outcome j.

Suppose that we are given two POVM's, $\{P_k : 1 \leq k \leq K\}$ and $\{Q_j : 1 \leq j \leq J\}$. The **quantum marginals problem** asks when does there exist a joint POVM, $\{R_{k,j} : 1 \leq k \leq K, 1 \leq j \leq J\}$ such that

$$P_k = \sum_{j=1}^{K} R_{k,j}, \; Q_j = \sum_{k=1}^{K} R_{k,j}?$$

Let $X = \{1, ..., K\} \times \{1, ..., J\}$ and let $C(X) := \ell_X^\infty$ denote the KJ dimensional space of continuous functions on X. We let $\delta_{k,j}$ be the Dirac delta function for the point (k, j), so that these KJ functions span $C(X)$. Set

$$f_k := \sum_{j=1}^{J} \delta_{k,j}, \; g_j := \sum_{k=1}^{K} \delta_{k,j}.$$

We see that the quantum marginals problem has a solution if and only if there is a POVM, $\{R_{k,j} : 1 \leq k \leq K, 1 \leq j \leq J\}$ satisfying the above conditions. But this is equivalent to having a UCP map,

$$\Phi : C(X) \to B(\mathcal{H}) \text{ such that } \Phi(f_k) = P_k, \; \Phi(g_j) = Q_j.$$

However, since we are only given the P_k's and Q_j's we only know the value of the desired map Φ on the f_k's and the g_j's.

Let

$$\mathcal{S} = span\{f_k, g_j : 1 \leq k \leq K, 1 \leq j \leq J\} \subseteq C(X).$$

Since the only linear relation among the functions is that $\sum_{k=1}^{K} f_k = \sum_{j=1}^{J} g_j = 1$, we can see that $dim(\mathcal{S}) = K + J - 1 < KJ$ as long as $K > 1$ and $J > 1$. Thus, $\mathcal{S} \neq C(X)$.

Because $\sum_{k=1}^{K} P_k = \sum_{j=1}^{J} = I$ we have that there is a well-defined unital, linear map

$$\Psi : \mathcal{S} \to B(\mathcal{H}), \; \Psi(f_k) + P_k, \; \Psi(g_j) = Q_j.$$

We arrive at the following conclusion:

Given POVM's $\{P_k : 1 \leq k \leq K\}$ and $\{Q_j : 1 \leq j \leq J\}$ in $B(\mathcal{H})$, the quantum marginals problem has a solution $\{R_{k,j} : 1 \leq k \leq K, 1 \leq j \leq J\}$

if and only if the map $\Psi : \mathcal{S} \to B(\mathcal{H})$ with $\Psi(f_k) = P_k, \Psi(g_j) = Q_j$ can be extended to a UCP map on all of $C(X)$.

It is not hard to see that $\mathcal{S}$ is a subspace, that $1 \in \mathcal{S}$ and that if $f \in \mathcal{S}$ then $f^* \in \mathcal{S}$. A subspace of a C*-algebra with these properties is called an **operator system**.

A theorem of W. B. Arveson gives us a nice criteria for deciding if the desired extension exists.

Theorem 8.3 (Arveson's Extension Theorem)**.** *Let $\mathcal{A}$ be a unital C*-algebra, let $\mathcal{S} \subseteq \mathcal{A}$ be an operator subsystem, and let $\mathcal{H}$ be a Hilbert space. If $\Psi : \mathcal{S} \to B(\mathcal{H})$ is CP, then it can be extended to a CP map $\Phi : \mathcal{A} \to B(\mathcal{H})$.*

We would like to apply this theorem to the quantum marginals problem. Note that every element of $M_n(\mathcal{S}) \subseteq M_n(C(X))$ can be written in the form

$$F := \sum_{k=1}^{K} A_k \otimes f_k + \sum_{j=1}^{J} B_j \otimes g_j \text{ where } A_k, B_j \in M_n.$$

Since $M_n(C(X)) = C(X; M_n)$ the element F is positive if and only if the function F is a positive matrix at every point in X. Thus,

$$F \geq 0 \iff A_k + B_j \geq 0, \forall k, j.$$

The image of F undet the map $\Psi^{(n)}$ is $\sum_{k=1}^{K} A_k \otimes P_k + \sum_{j=1}^{J} B_j \otimes Q_j$. Thus we are lead to the following solution to the quantum marginals problem.

Theorem 8.4. *Let $\{P_1, ...P_K, Q_1, , , , Q_J\} \subseteq B(\mathcal{H})$ satisfy $P_k, Q_j \geq 0$ and $\sum_{k=1}^{K} P_k = \sum_{j=1}^{J} Q_j = I_{\mathcal{H}}$. Then there exist $\{R_{k,j} : 1 \leq k \leq K, 1 \leq j \leq J\} \subseteq B(\mathcal{H})$ with*

- $R_{k,j} \geq 0$,
- $\sum_{k,j=1}^{K,J} R_{i,j} = I_{\mathcal{H}}$,
- $P_k = \sum_{j=1}^{J} R_{k,j}$, $Q_j = \sum_{k=1}^{K} R_{k,j}$

if and only if $\forall n$ whenever $A_k, B_j \in M_n$ satisfy $A_k + B_j \geq 0, \forall k, j$ we have that $\sum_{k=1}^{K} A_k \otimes P_k + \sum_{j=1}^{J} B_j \otimes Q_j \geq 0$ in $B(\mathcal{H}^{(n)})$.

By Stinespring's theorem, every positive map on $C(X)$ is completely positive. Thus, one is lead to wonder if the same is true for operator systems $\mathcal{S} \subseteq C(X)$ and if the "completely" is really needed in Arveson's theorem. The following example answers both of these questions.

Example 8.5. Let $\mathbb{T}$ denote the unit circle in the complex plane, let $\mathcal{S} = span\{1, z, \bar{z}\} \subset C(\mathbb{T})$, let $X = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \in B(\mathbb{C}^2)$. Then the map $\Psi : \mathcal{S} \to B(\mathbb{C}^2)$ defined by

$$\Psi(a1 + bz + c\bar{z}) = aI_2 + bX + cX^*,$$

is a positive map that is not completely positive. Consequently, Ψ can not be extended to a positive map on $C(\mathbb{T})$.

First to see that Ψ is a positive map, we need to figure out when $f(z) = a1 + bz + c\bar{z}$ is a positive function on $\mathbb{T}$. If it is positive then it is real-valued, so

$$\bar{a} + \bar{b}\bar{z} + \bar{c}z = \overline{f(z)} = f(z) = a + bz + \bar{c}\bar{z} \implies a = \bar{a}, c = \bar{b}.$$

On the unit circle the minimum value of $a + bz + \overline{bz}$ is $a - 2|b|$. Thus, we see that f is a positive function if and only if $a = \bar{a}, c = \bar{b}$ and $a - 2|b| \geq 0$.

For such an f we have that

$$\Psi(f) = \begin{pmatrix} a & 2b \\ 2\bar{b} & a \end{pmatrix} := Y$$

and $Y \geq 0 \iff a \geq 0$ and $det(Y) \geq 0 \iff a - 2|b| \geq 0$. Thus, Ψ is a positive map.

Note that $F = \begin{pmatrix} 1 & z \\ \bar{z} & 1 \end{pmatrix} \geq 0$ in $M_2(\mathcal{S})$. But

$$\Psi^{(2)}(F) = \begin{pmatrix} I_2 & X \\ X^* & I_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix},$$

which is not a positive matrix.

Thus, Ψ is not even a 2-positive map.

Finally, if Ψ could be extended to a positive map Φ on $C(\mathbb{T})$, then by Stinespring's result Φ would be completely positive, and consequently, its restriction to $\mathcal{S}$, which is Ψ, would be completely positive.

Thus, we see that positive maps on operator systems need not have positive extensions.

8.3. **A Sketch of Arveson's Extension Theorem.** In the proof of his extension theorem, Arveson(1969) showed a correspondence between CP maps into matrix algebras and states on a tensor product. This is very similar to Choi's correspondence, which is often used in QIT, but is definitely different and so could be useful in QIT.

Recall that Choi identifies a CP map, $\Phi : M_d \to M_r$ with a positive matrix, $C_\Phi \in M_d(M_r)$. When the map is CPTP, this positive matrix can in turn be thought of as the density matrix for a state on M_{dr}.

Arveson, identifies a CP map on an operator system, $\Psi : \mathcal{S} \to M_r$ with a positive linear functional on $M_r(\mathcal{S})$. In the case that Ψ is UCP, this positive linear functional is a state. In the case that $\Phi : M_d \to M_r$ is CPTP, then $\Phi^\dagger : M_r \to M_d$ is UCP and Arveson's state for $\Phi^\dagger$ and Choi's state for Φ are essentially the same. But Arveson's construction is more general since it holds when the domain is an operator system and predates Choi's construction.

First we need to discuss what we mean by a **state** on an operator system.

Proposition 8.6 (Arveson)**.** *Let $\mathcal{S}$ be an operator system and let $f : \mathcal{S} \to \mathbb{C}$ be a linear functional with $f(I) = 1$. Then f is a positive linear functional if and only if $\|f\| = 1$.*

We call such a map a **state**.

We present Arveson's proof since it actually shows a bit more.

Lemma 8.7 (Arveson)**.** *Let $\mathcal{S}$ be an operator system and let $f : \mathcal{S} \to \mathbb{C}$ be a linear functional with $f(I) = 1$ and $\|f\| = 1$. If $H = H^* \in \mathcal{S}$ and we set $a = \min\{\lambda : \lambda \in \sigma(H)\}$, $b = \max\{\lambda : \lambda \in \sigma(H)\}$, then $a \leq f(H) \leq b$.*

Proof. Note that the closed interval $[a, b]$ is the intersection of all the closed disks that contain it.

Suppose that $f(H) \notin [a, b]$ then there is a closed disk D with center t and radius r such that $f(H) \notin D$. This implies that $|f(H) - t| > r$. But $f(H) - t = f(H - tI)$ and by the spectral theorem for self-adjoint operators,

$$\|H - tI\| = \sup\{|\lambda - t| : \lambda \in \sigma(H)\} \leq \sup\{|z - t| : a \leq z \leq b\} < r,$$

since $\sigma(H) \subseteq [a, b] \subseteq D$.

So $|f(H - tI)| > r > \|H - tI\|$ contradicting that $\|f\| = 1$. □

Now we prove the proposition. If $\|f\| = 1$, $f(I) = 1$ and $P \geq 0$, then by the Lemma, $f(P) \geq 0$ since $\min\{\lambda : \lambda \in \sigma(P)\} \geq 0$.

Conversely, let $f(I) = 1$ and let $f(P) \geq 0$, $\forall P \geq 0$. We must show that $\|f\| \leq 1$. Note that if $\|X\| = 1$ then for any *theta* we have that

$$\|e^{i\theta}X + e^{-i\theta}X^*\| \leq 2.$$

Hence,

$$-2 \cdot I \leq e^{i\theta}X + e^{-i\theta}X^* \leq 2 \cdot I,$$

and since positive linear functionals preserve order,

$$-2 = -2f(I) \leq ei\theta f(X) + e^{-i\theta}f(X^*) \leq +2f(I) = +2.$$

Since f is a positive functional we also have that $f(X^*) = \overline{f(X)}$.

Now choose θ so that $e^{i\theta}f(X) = |f(X)|$ and we have that

$$-2 \leq 2|f(X)| \leq +2,$$

from which it follows that $|f(X)| \leq 1$ for any $\|X\| = 1$. Hence, $\|f\| \leq 1$, and the proposition is proven.

Let $\mathcal{S}$ be an operator systems and let $L : \mathcal{S} \to M_n$ be a linear map. Then the **Arveson functional** $S_L : M_n(\mathcal{S}) \to \mathbb{C}$ is given by

$$s_\Phi\big((X_{i,j})\big) = 1/n \sum_{i,j=1}^{n} \langle e_i | L(X_{i,j}) e_j \rangle_{\mathbb{C}^n} = \langle v | \big(L(X_{i,j})v\big\rangle_{\mathbb{C}^n \otimes \mathbb{C}^n},$$

where

$$v = \frac{1}{\sqrt{n}} \sum_{j=1}^{n} e_j \otimes e_j.$$

Note that Arveson was using the maximally entangled state!

Conversely, given a functional $f : M_n(\mathcal{S}) \to \mathbb{C}$ define a linear map $L_f : \mathcal{S} \to M_n$ by

$$L_f(X) = \sum_{i,j=1}^{n} f(X \otimes E_{i,j})E_{i,j}.$$

The **Arveson correspondence** is that these operations are mutually inverses.

Theorem 8.8 (Arveson)**.** *Let $\mathcal{S}$ be an operator system and let $\Phi : \mathcal{S} \to M_n$. Then Φ is CP if and only if s_Φ is a positive linear functional. Also, if Φ, then s_Φ is a state.*

One direction is easy. If Φ is CP, then whenever $(P_{i,j}) \geq 0$ in $M_n(\mathcal{S})$ we have that, $\big(\Phi(P_{i,j})\big) \geq 0$ and hence,

$$s_\Phi\big((P_{i,j})\big) = \langle v|\big(\Phi(P_{i,j})\big)v\rangle \geq 0.$$

The converse direction is the hard one. One needs to show that if s_Φ is a positive functional and $X_{k,l} \in \mathcal{S},\ 1 \leq k, j \leq p$ with $\big(X_{k,l}\big) \in M_p(\mathcal{S})$ positive, then the matrix $\big(\Phi(X_{k,l})\big) \in M_p(M_n) = M_{pn}$ is positive. For the details see [1] or [7].

Once one has this correspondence the proof of Arveson's extension theorem in the finite dimensional and UCP case is straightforward.

Let $\mathcal{S} \subseteq \mathcal{A}$ and operator system and a unital C*-algebra. Given a UCP map, $\Phi : \mathcal{S} \to M_n$ the map $s_\Phi : M_n(\mathcal{S}) \to \mathbb{C}$ is a state. But this means that $\|s_\Phi\| = 1$. So by the Hahn-Banach theorem we may extend it to a linear functional, $f : M_n(\mathcal{A}) \to \mathbb{C}$. But by the Arveson correspondence this gives us a map $L_f : \mathcal{A} \to M_n$ which is CP by the theorem and which extends Φ.

References

[1] Arveson, William B.; Subalgebras of C^*-algebras. *Acta Math.* 123 (1969), 141?224.

[2] Choi, Man Duen; Completely positive linear maps on complex matrices. *Linear Algebra Appl.* 10 (1975), 285?290.

[3] Conway, John:; *A course in functional analysis*,

[4] Davidson, Kenneth R.; *C*-algebras by example*,

[5] Dunford, Nelson; Schwartz, Jacob T, *Linear operators. Part II: Spectral theory*, Reprint of the 1963 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1988.

[6] Goberg, I.C. and Krein, M.G.; *Introduction to the Theory of Linear Nonselfadjoint Operators*, Translations of Mathematical Monographs, American Mathematical Society, 1969

[**?**] S. J. Harris, S. K. Pandey, and V. I. Paulsen, *Entanglement and Non-locality.*

[7] Paulsen, Vern I.; *Completely bounded maps and operator algebras*, Cambridge University Press, 2002.

[8] Pedersen, G.; *C*-algebras and their automorphism groups*,

Institute for Quantum Computing and Department of Pure Mathematics, University of Waterloo, Waterloo, ON, Canada N2L 3G1

E-mail address: vpaulsen@uwaterloo.ca