Quantum Compression and Fixed Points of Schwarz Maps

Lukas Rauber

A thesis submitted for the degree of
Master of Science

August 2018

Supervisor:
Prof. Dr. Michael M. Wolf
Zentrum Mathematik, M5
Technische Universität München

Contents

Introduction

There exist various schemes for compression of classical (i.e., non-quantum) information, which we use almost everyday, e.g. the `.zip` (lossless) and `.mp3` (with loss) file formats. In the present work we want to analyse the possibilities of compressing *quantum* information, i.e. mapping it into a smaller quantum system – thereby possibly allowing classical side information – and decompressing it while preserving the measurement statistics of a given set of quantum effects.

In Chapter 1 we establish the necessary mathematical foundations for the description of quantum information in terms of $\mathcal{C}^*$-algebras; in Chapter 2 we recall the basic principles of quantum information. In Chapter 3 we will investigate the structure of fixed point spaces of Schwarz maps between von Neumann algebras and formulate a normal form theorem (Theorem 3.8), which we will employ several times when investigating lossless quantum compression in Chapter 4. In the last section we finally give an outlook on the possibilities of quantum compression with losses.

The present work aims to be self-contained; nearly all mathematical statements will be proven. As prerequisites, we will rely on the well-known theory of (continuous linear) operators in Hilbert spaces, together with basic notions from the theory of Topological Vector Spaces, which are used in the context of the various important topologies the space of continuous linear operators on a Hilbert space can be equipped with.

Chapter 1.

$\mathcal{C}^*$-Algebras

In this chapter we recall the basic theory of $\mathcal{C}^*$-Algebras.

As we are mainly concerned with quantum operations, we will focus on *concrete* $\mathcal{C}^*$-Algebras, i.e. algebras of operators on a Hilbert space. In view of later applications in quantum information theory and dimensionality reduction, at several points we only consider finite dimensional Hilbert spaces, if it simplifies matters.

1.1. $*$-Algebras and Commutants

We recall the definition of an abstract $*$-algebra, and derive some basic properties.

Definition 1.1. A *$*$-algebra* $\mathscr{A}$ is an associative algebra (with or without unit) over the field $\mathbb{C}$ of complex numbers, together with an involution $* : \mathscr{A} \longrightarrow \mathscr{A}$, $a \mapsto a^*$, such that for all $x, y \in \mathscr{A}$ and $\lambda \in \mathbb{C}$ the following relations are satisfied:

i) $(x^*)^* = x$;

ii) $(x + y)^* = x^* + y^*$;

iii) $(\lambda x)^* = \overline{\lambda} x^*$; ($\overline{\lambda}$ denotes the complex conjugate of λ)

iv) $(xy)^* = y^* x^*$.

If, in addition, $\mathscr{A}$ carries a norm $\|\cdot\|$ that renders the normed space $(\mathscr{A}, \|\cdot\|)$ complete and which satisfies

v) $\|xy\| \leq \|x\| \|y\|$ for all $x, y \in \mathscr{A}$ (submultiplicativity) and

vi) $\|x^* x\| = \|x\|^2$ for all $x \in \mathscr{A}$ (the $\mathcal{C}^*$-property),

then $\mathscr{A}$ is called *(abstract) $\mathcal{C}^*$-algebra.*

If $\mathscr{A}$ contains a *unit*, i.e. an element $1_{\mathscr{A}}$ satisfying $1_{\mathscr{A}} x = x 1_{\mathscr{A}} = x$ for all $x \in \mathscr{A}$, then $\mathscr{A}$ is called *unital.*

A *$*$-subalgebra* $\mathscr{B}$ of a $*$-algebra $\mathscr{A}$ is a linear subspace with the property that, if x and y are in $\mathscr{B}$, then also xy and x^* lie in $\mathscr{B}$. A *$\mathcal{C}^*$-subalgebra* of a $\mathcal{C}^*$-algebra is a complete (equivalently, $\|\cdot\|$-closed) $*$-subalgebra.

Note that if $\mathscr{A}$ is unital, we do not require a $*$-subalgebra $\mathscr{B}$ of $\mathscr{A}$ to have the same unit as $\mathscr{A}$ (or have a unit at all).

As more or less trivial consequences of the definition, we note:

Lemma 1.2. *In a $*$-algebra $\mathscr{A}$ it holds that $0^* = 0$ and, if $\mathscr{A}$ is unital, $(1_{\mathscr{A}})^* = 1_{\mathscr{A}}$. Moreover, in a $\mathcal{C}^*$-algebra $\mathscr{A}$, we have $\|x\| = \|x^*\|$ for all $x \in \mathscr{A}$.*

Proof. From properties (i) and (ii) of Definition 1.1 it follows that $x = x^{**} = (x^* + 0)^* = x + 0^*$ for all $x \in \mathscr{A}$, so $0^* = 0$ by uniqueness of the neutral element in a group. The equality $(1_{\mathscr{A}})^* = 1_{\mathscr{A}}$ follows similarly with (i) and (iv) by $x = x^{**} = (x^* 1_{\mathscr{A}})^* = (1_{\mathscr{A}})^* x$, as well as $x = x^{**} == (1_{\mathscr{A}} x^*)^* = x\,(1_{\mathscr{A}})^*$.

Using properties v) and vi), we obtain the inequality $\|x\|^2 = \|x^* x\| \leq \|x^*\|\,\|x\|$ for all $x \in \mathscr{A}$, hence $\|x\| \leq \|x^*\|$ (the special case $x = 0$ is valid by the preceding argument). Since the adjoint map is an involution, we can replace x by x^* and use (i) to get the reverse inequality. $\square$

As an example, let $\mathcal{H}$ be a complex Hilbert space and let $\mathscr{L}(\mathcal{H})$ denote the algebra of all linear continuous[1] maps $T : \mathcal{H} \longrightarrow \mathcal{H}$. Equipped with the usual adjoint operation $* : \mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{H})$ and the operator norm, $\mathscr{L}(\mathcal{H})$ is a $\mathcal{C}^*$-algebra. Note that although $*$-subalgebras of $\mathcal{C}^*$-algebras fulfil properties v) and vi) in Definition 1.1, they need not be $\mathcal{C}^*$-algebras again – consider for instance a separable infinite-dimensional complex Hilbert space $\mathcal{H}$ with an orthonormal basis $(e_i)_{i\in\mathbb{N}}$ and the $*$-subalgebra

$$\mathscr{A} := \{T \in \mathscr{L}(\mathcal{H}) \mid \operatorname{rank} T \text{ and } \operatorname{rank} T^* \text{ are finite}\} \subset \mathscr{L}(\mathcal{H}).$$

One easily checks that $\mathscr{A}$ is a $*$-algebra, but it is not complete; indeed the Cauchy sequence $T_n := \sum_{i=1}^n \frac{1}{i} |e_i\rangle\langle e_i|$ does not converge in $\mathscr{A}$. However, this phenomenon does not occur in finite dimensional Hilbert spaces, because in this case all linear subspaces are complete.

We will mainly be concerned with $*$-algebras consisting of operators on some Hilbert space, which justifies an autonomous definition:

Definition 1.3. A sub-$*$-algebra of $\mathscr{L}(\mathcal{H})$ for some complex Hilbert space $\mathcal{H}$ is called a *concrete $*$-algebra*, or a *$*$-algebra of operators (in $\mathcal{H}$)*.

The apparently greater generality of *abstract* $\mathcal{C}^*$-algebras over concrete ones is in fact deceptive: According to the *Gelfand-Naimark* theorem (see for example [Tak, Theorem 9.18 in Ch. I] or [Arv3, Theorem 1.7.3]), every abstract $\mathcal{C}^*$-algebra is isometrically isomorphic (cf. section 1.4) to a concrete one. We will not prove this theorem, but we will restrict our statements to concrete $\mathcal{C}^*$-algebras at several points.

Finally, we consider a special class of concrete $\mathcal{C}^*$-algebras, namely von Neumann algebras. We define:

Definition 1.4. Let $\mathcal{H}$ be a complex Hilbert space. For a subset $S \subseteq \mathscr{L}(\mathcal{H})$, we call

$$S' := \{t \in \mathscr{L}(\mathcal{H}) \mid ts = st \;\forall s \in S\}$$

[1]Note that in the case $\dim \mathcal{H} < \infty$, all linear operators $T : \mathcal{H} \longrightarrow \mathcal{H}$ are continuous.

the *commutant* of S. The *double* and *triple commutant* are defined as $S'' := (S')'$ and $S''' := (S'')'$, respectively. The *centre* of a concrete $*$-algebra $\mathscr{A} \subseteq \mathscr{L}(\mathcal{H})$ is by definition $\mathfrak{Z}(\mathscr{A}) := \mathscr{A} \cap \mathscr{A}'$.

Finally, a subset $\mathscr{A} \subseteq \mathscr{L}(\mathcal{H})$ is called *von Neumann algebra (in $\mathcal{H}$)*, if $\mathscr{A} = \mathscr{A}'' = \mathscr{A}^*$.

As the name already suggests, a von Neumann algebras are associative algebras; actually they are special cases of unital concrete $\mathcal{C}^*$-algebras, which is made clear in part (f) of the next Proposition, which also summarises some properties of commutants and von Neumann algebras.

Proposition 1.5 ([Dix, Section I.1.1]). *Let $\mathcal{H}$ be a complex Hilbert space.*

a) *The operations of taking the adjoint and taking the commutant of a set, commute, i.e. $(S^*)' = (S')^*$ for all $S \subseteq \mathscr{L}(\mathcal{H})$.*

b) *For two sets $S, T \subseteq \mathscr{L}(\mathcal{H})$, the implication $S \subseteq T \implies T' \subseteq S'$ holds.*

c) *For every set $S \subseteq \mathscr{L}(\mathcal{H})$ it holds that $S \subseteq S''$.*

d) *The commutant S' of a set $S \subseteq \mathscr{L}(\mathcal{H})$ is a strongly closed[2] algebra containing $\mathrm{id}_{\mathcal{H}}$. In particular, if $S = S^*$, then S' is a unital $\mathcal{C}^*$-algebra in $\mathcal{H}$.*

e) *We have $S''' = S'$ for every subset $S \subseteq \mathscr{L}(\mathcal{H})$. In particular, if $S = S^*$, then S' is a von Neumann algebra.*

f) *Every von Neumann algebra $\mathscr{A}$ in $\mathcal{H}$ is a strongly closed $\mathcal{C}^*$-algebra of operators in $\mathcal{H}$ that contains $\mathrm{id}_{\mathcal{H}}$ as a unit.*

g) *For $S \subseteq \mathscr{L}(\mathcal{H})$, the set $(S \cup S^*)''$ is the smallest von Neumann algebra containing S, i.e.*

$$(S \cup S^*)'' = \bigcap \left\{ T \subseteq \mathscr{L}(\mathcal{H}) \,\middle|\, T \supseteq S \ \wedge\ T'' = T = T^* \right\}.$$

Proof. a) Calculate:

$$\begin{aligned}(S^*)' &= \{t \in \mathscr{L}(\mathcal{H}) \mid ts^* = s^*t \ \forall s \in S\} \\ &= \{t \in \mathscr{L}(\mathcal{H}) \mid st^* = t^*s \ \forall s \in S\} \\ &= \{t \in \mathscr{L}(\mathcal{H}) \mid st = ts \ \forall s \in S\}^* = \left(S'\right)^*.\end{aligned}$$

b) Assume $S \subseteq T \subseteq \mathscr{L}(\mathcal{H})$ and let $u \in T'$. Since u commutes with every element of T, it certainly commutes with every element of S (as $T \supseteq S$); hence $u \in S'$.

c) Let $s \in S$. In order to prove $s \in S''$, we have to show $st = ts$ for any given $t \in S'$. But this is exactly the definition of S', so this statement is reasonably trivial.

d) It is fairly evident that S' is an algebra: Obviously it is a linear subspace of $\mathscr{L}(\mathcal{H})$, and we have for $x, y \in S'$

$$\forall s \in S: \ xys = xsy = sxy \quad \text{(by definition of } S'\text{)},$$

[2] For a definition of the numerous topologies on $\mathscr{L}(\mathcal{H})$, see Appendix A.

hence $x, y \in S'$. To prove that S' is closed w.r.t. the strong operator topology, we take a net $(t_\delta) \subseteq S'$ converging strongly to a limit $t \in \mathscr{L}(\mathcal{H})$, i.e. $t_\delta \xi \to t\xi$ for all $\xi \in \mathcal{H}$, and show that t lies in S'. As $t_\delta \in S'$ for every δ, we have $t_\delta s \xi = s t_\delta \xi$ for all $s \in S$ and all δ. The left hand side converges to $ts\xi$, whereas the right hand side converges to $st\xi$, thus by uniqueness of limits $ts\xi = st\xi$ for all $\xi \in \mathcal{H}$; hence $t \in S'$.

e) By part (c) we have $S' \subseteq (S')'' = S'''$. The other inclusion follows by applying (b) to the inclusion $S \subseteq S''$, which yields $S''' = (S'')' \subseteq S'$. The auxiliary statement follows from (a), as $(S')^* = (S^*)' = S'$.

f) Let $\mathscr{A} \subseteq \mathscr{L}(\mathcal{H})$ be a von Neumann algebra. Since $\mathscr{A} = (\mathscr{A}')'$, part (d) tells us that $\mathscr{A}$ is a strongly closed algebra containing $\mathrm{id}_{\mathcal{H}}$. The second defining property $\mathscr{A} = \mathscr{A}^*$ implies that $\mathscr{A}$ is a $*$-algebra. Since the strong operator topology is weaker than the uniform topology, $\mathscr{A}$ is also $\|\cdot\|$-closed, hence complete.

g) "$\subseteq$". Let $T \subseteq \mathscr{L}(\mathcal{H})$ be such that $T'' = T = T^*$ and $S \subseteq T$. By taking adjoints, $S^* \subseteq T^* = T$, hence $(S \cup S^*) \subseteq T$. Now apply (b) twice to get $(S \cup S^*)'' \subseteq T'' = T$.

Conversely, we know from (e) and (c) that $(S \cup S^*)''$ is a von Neumann algebra containing S; so it actually occurs in the intersection on the right hand side, which shows "$\supseteq$". $\square$

Remark 1.6. The converse statement of part (f) also holds true, namely that a concrete $*$-algebra is a von Neumann algebra, iff it contains $\mathrm{id}_{\mathcal{H}}$ and is closed w.r.t. the strong (or, equivalently, weak) operator topology. This is a direct consequence of the famous *Double Commutant Theorem* of J. von Neumann (see Appendix A for a formal statement and proof of the double commutant theorem.). Thus, whereas in the general case von Neumann algebras are more special than concrete $\mathcal{C}^*$-Algebras, the situation is much simpler, if the underlying Hilbert space is finite-dimensional, for in finite dimensions all subspaces of $\mathscr{L}(\mathcal{H})$ are closed w.r.t. to any of the weak, strong or norm topology. More precisely, the following corollary of the double commutant theorem holds in finite dimensions:

Proposition 1.7 (Double Commutant Theorem, finite dimensional case, cf. [Dix, p. 45])**.** *Let $\mathscr{A}$ be a concrete $*$-algebra in the finite dimensional Hilbert space $\mathcal{H}$. Define the subspace*

$$\mathcal{X} := \operatorname{span}\{A\xi \mid A \in \mathscr{A},\ \xi \in \mathcal{H}\} \subseteq \mathcal{H}$$

and let $P \in \mathscr{L}(\mathcal{H})$ denote the orthogonal projection onto $\mathcal{X}$.

Then P is the unit of, and the greatest[3] projection in $\mathscr{A}$. Moreover, we have

$$\mathscr{A}'' = \mathscr{A} + \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}};$$

and the following statements are equivalent:

i) $\mathscr{A}$ *is a von Neumann algebra in* $\mathcal{H}$.

ii) $P = \mathrm{id}_{\mathcal{H}}$.

[3]meaning: All other projections $Q \in \mathscr{A}$ have a proper subspace of $\mathcal{X}$ as their image.

iii) $\mathrm{id}_{\mathcal{H}} \in \mathscr{A}$.

In other words: All sub-$*$-algebras of $\mathscr{L}(\mathcal{H})$ are actually unital $\mathcal{C}^*$-algebras for finite dimensional $\mathcal{H}$.

Operator Systems

In later applications, we will consider maps defined only on linear subspaces of $\mathscr{L}(\mathcal{H})$ that are not necessarily closed under multiplication. We define:

Definition 1.8. Let $\mathscr{A}$ be a unital $\mathcal{C}^*$-Algebra. A linear subspace $\mathcal{S} \subset \mathscr{A}$ is called an *operator system*, if it is self-adjoint (i.e. $\mathcal{S}^* := \{s^* \mid s \in \mathcal{S}\} = \mathcal{S}$) and contains the unit element of $\mathscr{A}$.

1.2. Hermiticity, Positivity and Order

Definition 1.9. An element x of a $*$-algebra $\mathscr{A}$ is called

- *hermitian* or *self-adjoint*, if $x^* = x$.
- *anti-hermitian*, if $x^* = -x$.
- *positive*, if $x = y^*y$ for a $y \in \mathscr{A}$. In this case we write $x \geq 0$. For $a, b \in \mathscr{A}$ we write $a \leq b$, if a and b are hermitian and $b - a \geq 0$. In this case we occasionally may say that b *majorises* a.
- *projection*, if $x^2 = x = x^*$.

It follows directly from the definition, that every projection is positive, that every positive element is hermitian, and that the set of hermitian elements of a $*$-algebra constitutes a vector space over $\mathbb{R}$. Although it is not obvious, the positivity of an element $x \in \mathscr{A}$ does not depend on whether we regard x as an element of $\mathscr{A}$ or as an element of some subalgebra $\mathscr{B} \subseteq \mathscr{A}$.

As is well-known, in the case of concrete $\mathcal{C}^*$-algebras one can characterise positivity of an operator $a \in \mathscr{L}(\mathcal{H})$ by several equivalent conditions:

i) For all vectors $\psi \in \mathcal{H}$, the number $\langle\psi|a\psi\rangle$ is real and non-negative.

ii) $a = h^2$ for some hermitian operator $h \in \mathscr{L}(\mathcal{H})$.

iii) a is hermitian and its spectrum is contained in $[0, +\infty)$.

Hence, in a concrete $\mathcal{C}^*$-algebra, the set of positive elements forms a convex cone (i.e., it is closed under addition and multiplication with non-negative real numbers). The same holds for abstract $\mathcal{C}^*$-algebras, though this is harder to show, if one does not use a representation on a concrete Hilbert space. For a reference, see [Tak, Chapter I.6].

The following proposition summarises properties and calculation rules of hermitian and positive elements, as well as connections between positivity and the $\mathcal{C}^*$-norm. The proofs are mostly taken from [Pau, Chapter 2].

Proposition 1.10. *Let $\mathscr{A}$ be a concrete unital $\mathcal{C}^*$-algebra on $\mathcal{H}$, and let $\mathcal{S} \subset \mathscr{A}$ be an operator system.*

i) *An element $x \in \mathscr{A}$ is anti-hermitian, iff $\mathrm{i}x$ is hermitian.*

ii) *For any $x \in \mathcal{S}$, there is a unique decomposition $x = h + a$, where $h \in \mathcal{S}$ is hermitian and $a \in \mathcal{S}$ is anti-hermitian. In this case we have that $\|h\| \leq \|x\|$ and $\|a\| \leq \|x\|$.*

iii) *If $h \in \mathscr{A}$ is hermitian, then we have $-\|h\| \cdot 1_{\mathscr{A}} \leq h \leq \|h\| \cdot 1_{\mathscr{A}}$.*

iv) *Every hermitian element $h \in \mathcal{S}$ can be expressed as the difference of two positive elements in $\mathcal{S}$, namely*

$$h = \frac{1}{2}(\|h\| \cdot 1_{\mathscr{A}} + h) - \frac{1}{2}(\|h\| \cdot 1_{\mathscr{A}} - h).$$

v) *For two positive elements p_1 and p_2 in $\mathscr{A}$ we have that*

$$\|p_1 - p_2\| \leq \max\{\|p_1\|, \|p_2\|\}.$$

vi) *If a and b are hermitian elements of $\mathscr{A}$ with $a \leq b$, then for all $c \in \mathscr{A}$ it holds that $c^*ac \leq c^*bc$.*

vii) *For any $a, c \in \mathscr{A}$ we have that $a^*c^*ca \leq \|c\|^2 a^*a$.*

Proof. (i) We have the following equivalence chain:

$$\mathrm{i}x \text{ is hermitian } \Leftrightarrow \mathrm{i}x = (\mathrm{i}x)^* = -\mathrm{i}x^* \Leftrightarrow x^* = -x \Leftrightarrow x \text{ is antihermitian.}$$

(ii) First we show uniqueness of the decomposition: If we have $x = h + a$ with h hermitian and a anti-hermitian, by taking adjoints we get $x^* = h - a$. Respectively adding or subtracting these two equations yields $h = (x + x^*)/2$ and $a = (x - x^*)/2$, so h and a are uniquely determined by x. Obviously, h and a add up to x. Since $\|x^*\| = \|x\|$ (Lemma 1.2), the triangle inequality applied to the definitions of h and a implies $\|h\|, \|a\| \leq \|x\|$.

(iii) For every vector $\xi \in \mathcal{H}$ we can use the Cauchy-Schwarz inequality to obtain

$$\langle \xi | h\xi \rangle \leq \|\xi\| \, \|h\xi\| \leq \|h\| \, \|\xi\|^2 = \left\langle \xi \middle| (\|h\| \, 1_{\mathscr{A}}) \, \xi \right\rangle,$$

hence $h \leq \|h\| \cdot 1_{\mathscr{A}}$. The other operator inequality then follows by multiplication with -1 and replacing h by $-h$.

(iv) follows from (iii).

(v) Because the operator $p_1 - p_2$ is hermitian, we can calculate its norm by

$$\begin{aligned}
\|p_1 - p_2\| &= \sup_{\|\xi\| \leq 1} |\langle \xi | (p_1 - p_2)\xi \rangle| = \sup_{\|\xi\| \leq 1} \Big| \underbrace{\langle \xi | p_1 \xi \rangle}_{\geq 0} - \underbrace{\langle \xi | p_2 \xi \rangle}_{\geq 0} \Big| \\
&\leq \sup_{\|\xi\| \leq 1} \max \Big\{ |\langle \xi | p_1 \xi \rangle|, \; |\langle \xi | p_2 \xi \rangle| \Big\} = \max_{p \in \{p_1, p_2\}} \sup_{\|\xi\| \leq 1} |\langle \xi | p \xi \rangle| \\
&= \max\{\|p_1\|, \|p_2\|\}.
\end{aligned}$$

(vi) Setting $d := b - a \geq 0$, we have $\langle \xi | c^* bc - c^* ac | \xi \rangle = \langle \xi | c^* dc | \xi \rangle = \langle c\xi | d | c\xi \rangle \geq 0$ for all $\xi \in \mathcal{H}$.

(vii) Again, for $\xi \in \mathcal{H}$ it holds that

$$\langle \xi | a^* c^* ca | \xi \rangle = \langle ca\xi | ca\xi \rangle = \|ca\xi\|^2 \leq (\|c\| \, \|a\xi\|)^2 = \left\langle \xi \middle| \|c\|^2 \, a^* a \middle| \xi \right\rangle .$$

□

Note. Of course, the calculation rules of proposition 1.10 also hold for abstract $\mathcal{C}^*$-algebras, which can be proved by representing the elements as operators on a Hilbert space.

When considering maps between $\mathcal{C}^*$-algebras (e.g. quantum operations), or – more generally – maps between operator systems, we will demand that the structures of hermitian or positive elements shall be preserved. This gives rise to the next definition.

Definition 1.11. Let $\mathscr{A}$ and $\mathscr{B}$ be two $\mathcal{C}^*$-Algebras and $\mathcal{S} \subset \mathscr{A}$ an operator system. A linear map $T : \mathcal{S} \longrightarrow \mathscr{B}$ is called

- *hermiticity-preserving*, if it maps hermitian elements to hermitian elements, i.e.

$$\forall x \in \mathcal{S} : \quad x^* = x \;\Rightarrow\; (T(x))^* = T(x)$$

- *positivity-preserving* (or just *positive*), if it maps positive elements to positive elements, i.e.

$$\forall x \in \mathcal{S} : \quad x \geq 0 \;\Rightarrow\; T(x) \geq 0.$$

Note. Every positivity-preserving map is hermiticity-preserving by proposition 1.10iv). Moreover, the set of hermiticity-preserving maps $T : \mathcal{S} \longrightarrow \mathscr{B}$ constitutes an $\mathbb{R}$-vector space.

Lemma 1.12. *A linear map $T : \mathcal{S} \longrightarrow \mathscr{B}$ between an operator system $\mathcal{S}$ and a $\mathcal{C}^*$-algebra $\mathscr{B}$ is hermiticity-preserving, if and only if for all $x \in \mathcal{S}$ we have $(T(x))^* = T(x^*)$.*

Proof. By parts (ii) and (i) of proposition 1.10, we can decompose a general element $x \in \mathcal{S}$ as $x = h + \mathrm{i}k$, where both h and k are hermitian elements of $\mathcal{S}$. We calculate

$$\begin{aligned}(T(x))^* &= (T(h) + \mathrm{i}T(k))^* = (T(h))^* - \mathrm{i}\,(T(k))^* \\ &= T(h) - \mathrm{i}T(k) = T((h + \mathrm{i}k)^*) = T(x^*).\end{aligned}$$

The converse implication is obvious. □

Lemma 1.13 ([Pau, Proposition 2.1])**.** *Let $\mathcal{S}$ be an operator system and let $\mathscr{B}$ be a $\mathcal{C}^*$-algebra. If $\phi : \mathcal{S} \longrightarrow \mathscr{B}$ is a positive map, then ϕ is bounded with operator norm $\|\phi\| \leq 2\,\|\phi(1)\|$.*

Proof. First, consider an hermitian element $h \in \mathcal{S}$, $h \neq 0$. Using the decomposition from proposition 1.10(iv) of h, by positivity of ϕ and part (v) of proposition 1.10 we have

$$\begin{aligned} \|\phi(h)\| &= \frac{1}{2} \left\| \phi\big((\|h\| 1 + h) - (\|h\| 1 - h)\big) \right\| \\ &\leq \frac{1}{2} \max \{ \|\phi(\|h\| 1 + h)\|, \|\phi(\|h\| 1 - h)\| \} \\ &= \frac{\|h\|}{2} \max \left\{ \left\| \phi\left(1 \pm \frac{h}{\|h\|}\right) \right\| \right\}, \end{aligned}$$

and since $0 \leq 1 \pm h/\|h\| \leq 2$, positivity of ϕ implies $\|\phi(h)\| \leq \|h\| \|\phi(1)\|$. Now, we can decompose a general element $x \in \mathcal{S}$ according to parts (ii) and (i) of proposition 1.10 into $x = a + \mathrm{i}b$ for hermitian elements $a, b \in \mathcal{S}$, and we get

$$\|\phi(x)\| \leq \|\phi(a)\| + \|\phi(b)\| \leq (\|a\| + \|b\|) \|\phi(1)\| \leq 2 \|x\| \|\phi(1)\|.$$

□

We close this section with some statements about positivity in $*$-algebras on a finite dimensional Hilbert space. Let $\mathcal{H}$ and $\mathcal{K}$ be finite dimensional Hilbert spaces, and $\mathscr{A} \subseteq \mathscr{L}(\mathcal{H})$ and $\mathscr{B} \subseteq \mathscr{L}(\mathcal{K})$ $*$-algebras of operators.

First we consider the spectral decomposition

$$a = \sum_{\lambda \in \sigma(a)} \lambda e_\lambda$$

of an hermitian element $a \in \mathscr{A}$, where $\sigma(a)$ denotes the spectrum (i.e., the set of eigenvalues) of a, and $e_\lambda \in \mathscr{L}(\mathcal{H})$ are the mutually orthogonal eigenprojections. Since we can express every e_λ as a polynomial of a, e.g.

$$e_\lambda = \left(\prod_{\mu \in \sigma(a) \setminus \{\lambda\}} \frac{(a - \mu \cdot 1_{\mathscr{A}})}{\lambda - \mu} \right),$$

all the e_λ do actually belong to $\mathscr{A}$.[4] As a consequence, we state another characterisation of positive elements and positivity preserving maps.

Lemma 1.14. *Let $\mathcal{H}$ and $\mathcal{K}$ be finite dimensional Hilbert spaces, and let $\mathscr{A} \subseteq \mathscr{L}(\mathcal{H})$ and $\mathscr{B} \subseteq \mathscr{L}(\mathcal{K})$ be $*$-algebras of operators. Then the following statements hold true:*

a) *An element $a \in \mathscr{A}$ is positive, iff for every projection $p \in \mathscr{A}$ it holds that* $\mathrm{tr}(pa) \geq 0$.

b) *A linear map $T : \mathscr{A} \longrightarrow \mathscr{B}$ is positive, iff for all projections $q \in \mathscr{A}$, $p \in \mathscr{B}$, it holds that* $\mathrm{tr}\,(pT(q)) \geq 0$.

[4] A generalisation of this is also true for infinite-dimensional $\mathcal{H}$: If the $*$-algebra $\mathscr{A}$ is strongly (or, equivalently, weakly) closed and $a \in \mathscr{A}$ is hermitian, then also $f(a) \in \mathscr{A}$ for every bounded measurable function f.

Proof. a) If $a \in \mathscr{A}$ is positive, we can write it as $a = b^*b$ for some $b \in \mathscr{A}$. Hence by cyclic invariance of the trace we get

$$\operatorname{tr}(pa) = \operatorname{tr}(p^2 b^* b) = \operatorname{tr}(pb^*bp) = \operatorname{tr}\left((bp)^* bp\right) \geq 0,$$

since the trace of a positive operator is non-negative. Conversely, assume that $\operatorname{tr}(pa) \geq 0$ holds for all projections $p \in \mathscr{A}$. We decompose a into hermitian and anti-hermitian part and invoke the spectral theorem for both parts to get

$$a = \frac{a + a^*}{2} + \mathrm{i}\frac{a - a^*}{2\mathrm{i}} = \sum_{\lambda \in X} \lambda e_\lambda + \mathrm{i} \sum_{\mu \in Y} \mu f_\mu$$

for some finite sets $X, Y \subset \mathbb{R}$ and projections $e_\lambda, f_\mu \in \mathscr{A}$. For every $\mu_0 \in Y$, the number

$$\operatorname{tr}\left(f_{\mu_0} a\right) = \sum_{\lambda \in X} \lambda \operatorname{tr}\left(f_{\mu_0} e_\lambda\right) + \mathrm{i}\mu_0 \operatorname{rank} f_{\mu_0}$$

is real by assumption. By the already proven part, the first sum is also real, hence $\mu \cdot \operatorname{rank} f_\mu = 0$ for all $\mu \in Y$, which shows that the anti-hermitian part of a vanishes. Now for $\lambda \in X$ we plug in $p = e_\lambda$ in our assumption and get

$$0 \leq \operatorname{tr}(e_\lambda a) = \lambda \operatorname{rank} e_\lambda.$$

So all eigenvalues of a are non-negative; hence $a \geq 0$.

b) "$\Rightarrow$" follows from (a) since $T(q)$ is positive. "$\Leftarrow$": Suppose that $a \in \mathscr{A}$ is positive; we show that $T(a)$ is positive, too. We have $\sigma(a) \subset [0, +\infty)$, and by spectral composition $a = \sum_{\lambda \in \sigma(a)} \lambda e_\lambda$ for some projections $e_\lambda \in \mathscr{A}$. We calculate

$$\operatorname{tr}\left(pT(a)\right) = \sum_{\lambda \in \sigma(a)} \lambda \underbrace{\operatorname{tr}\left(pT(e_\lambda)\right)}_{\geq 0} \geq 0,$$

and by part (a) we get $T(a) \geq 0$. $\square$

1.3. Ideals and Projections

Definition 1.15. Let $\mathscr{A}$ be a concrete $*$-algebra. A projection lying in the centre $\mathfrak{Z}(\mathscr{A})$ of $\mathscr{A}$ we may call a *central projection.* A family of projections $(p_i)_{i \in I} \subseteq \mathscr{L}(\mathcal{H})$ is called *mutually orthogonal*, if $p_i p_j = \delta_{ij} p_i$ for all $i, j \in I$.

From Hilbert space theory we know, that there is an order-preserving bijection between the set of projections in $\mathcal{H}$ and the set of closed subspaces of $\mathcal{H}$, given by $P \mapsto \operatorname{ran} P = P\mathcal{H}$, where the latter set is partially ordered by inclusion. Using this correspondence, it is easy to show that two projections are orthogonal, iff their ranges are orthogonal subspaces.

For strongly closed $*$-algebras, we will see that its structure is substantially determined by its projections. As a first result to be used later on, we show:

Lemma 1.16. *For a strongly closed $*$-algebra $(\mathfrak{B}, \mathcal{H})$ the following two statements are equivalent:*

i) $\mathfrak{B}$ contains no non-trivial (i.e. $\neq 0$ and $\neq 1_{\mathfrak{B}}$) projection.

ii) $\mathfrak{B} = \mathbb{C} \cdot 1_{\mathfrak{B}}$.

Proof. "(ii)⇒(i)" is trivial. We prove "$(i) \Rightarrow (ii)$" by contraposition. Assume that $\mathfrak{B}$ contains an element $A \notin \mathbb{C} \cdot 1_{\mathfrak{B}}$. By considering the hermitian or anti-hermitian part of A, we can safely assume that A is self-adjoint. By spectral calculus, there exists a subset S of the spectrum of A, such that $0 \neq \chi_S(A) \neq 1_{\mathfrak{B}}$, where χ_S denotes the characteristic function of S. Since $\mathfrak{B}$ is weakly closed, the projection $P := \chi_S(A)$ lies in $\mathfrak{B}$. □

We recall the definition of ideals from algebra:

Definition 1.17. Let $\mathscr{A}$ be a $*$-algebra. A subspace $\mathscr{I} \subset \mathscr{A}$ is called a

- *left-ideal in $\mathscr{A}$*, if $\mathscr{A}\mathscr{I} \subseteq \mathscr{I}$.
- *right-ideal in $\mathscr{A}$*, if $\mathscr{I}\mathscr{A} \subseteq \mathscr{I}$.
- *two-sided ideal in $\mathscr{A}$*, if $\mathscr{I}$ is a left-ideal and a right-ideal in $\mathscr{A}$.

Note. If $\mathscr{I}$ is a left-ideal (right-ideal) in $\mathscr{A}$, then $\mathscr{I}^*$ is a right-ideal (left-ideal) in $\mathscr{A}$, which can be easily seen by taking adjoints. In particular, a one-sided ideal is also two-sided, iff it is self-adjoint.

Obviously, if $\mathscr{A}$ is a $*$-algebra and $E \in \mathscr{A}$ is a projection[5], then the subset $\mathscr{A}E = \{AE \mid A \in \mathscr{A}\}$ is a left-ideal in $\mathscr{A}$. The natural question, whether all ideals arise in this way, is answered by the next proposition in the positive, at least when we consider only strongly closed ideals.

Proposition 1.18 (cf. [Dix, Corollary 3 in Sec. I.3.4])**.** *Let $\mathfrak{A}$ be a strongly closed $*$-algebra of operators on a Hilbert space $\mathcal{H}$. Then every strongly closed left ideal $\mathfrak{M}$ in $\mathfrak{A}$ is of the form*

$$\mathfrak{M} = \{T \in \mathfrak{A} \mid T = TE\} = \mathfrak{A}E$$

for a unique projection $E \in \mathfrak{A}$. $\mathfrak{M}$ is two-sided, iff E is central.

Proof. Let $\mathfrak{M} \subseteq \mathfrak{A}$ be a strongly closed left ideal. Then, the set $\mathfrak{N} := \mathfrak{M} \cap \mathfrak{M}^*$ is a strongly closed two-sided ideal in $\mathfrak{A}$, thus in particular a $*$-subalgebra of $\mathfrak{A}$. By the von Neumann double commutant theorem (Theorem A.7), $\mathfrak{N}$ has a unit element E. We set $\tilde{\mathfrak{M}} := \{T \in \mathfrak{A} \mid T = TE\}$ and show that $\mathfrak{M} = \tilde{\mathfrak{M}}$.

Let $T \in \tilde{\mathfrak{M}}$, i.e. $T \in \mathfrak{A}$ with $T = TE$. Since $\mathfrak{M}$ is a left-ideal and $E \in \mathfrak{N} \subseteq \mathfrak{M}$, we get $T = TE \in \mathfrak{M}$; so the inclusion $\tilde{\mathfrak{M}} \subseteq \mathfrak{M}$ holds. Conversely, if $T = U\,|T|$ is the polar

[5]Of course, $\mathscr{A}E$ is a left-ideal for any $E \in \mathscr{A}$. The points is, that the demand of E being a projection does not hurt (as we will show shortly after) and yields a 1-to-1 relation between (strongly closed) ideals and projections.

decomposition of an element $T \in \mathfrak{M}$, then $|T|^* = |T| = U^*T \in \mathfrak{M}$, hence $|T| \in \mathfrak{N}$. Since E is the unit element of $\mathfrak{N}$, it follows that $|T| = |T|\,E$, hence $T = U\,|T| = U\,|T|\,E = TE$, and thus $T \in \tilde{\mathfrak{M}}$.

In order to prove uniqueness, assume that $F \in \mathfrak{A}$ is another projection with the property $\mathfrak{M} = \{T \in \mathfrak{A} \mid T = TF\}$. Then obviously E and F lie in $\mathfrak{M}$, so we have that $E = EF$ and $F = FE$, hence $E = E^* = (EF)^* = F^*E^* = FE = F$.

Now, assume that $\mathfrak{M}$ is two-sided. Then we have $\mathfrak{M}^* = \mathfrak{M}$, hence $\mathfrak{N} = \mathfrak{M}$ and for all $A \in \mathfrak{A}$, both AE and EA lie in $\mathfrak{N}$, thus $AE = E(AE) = (EA)E = EA$, as E is the unit of $\mathfrak{N}$. □

Corollary 1.19. *Let $\mathfrak{A}$ be a strongly closed $*$-algebra of operators, and let $\mathfrak{I}$ be a strongly closed two-sided ideal in $\mathfrak{A}$. Then for every element $A \in \mathfrak{A}$ the implication $A^*A \in \mathfrak{I} \implies A \in \mathfrak{I}$ holds.*

Proof. Let E be the central projection from proposition 1.18, such that $\mathfrak{I} = E\mathfrak{A}$. We write $A = EA + B$ with $B := (1_{\mathfrak{A}} - E)A$ and use $E \in \mathfrak{A}'$ and $E(1_{\mathfrak{A}} - E) = 0$ to get $A^*A = EA^*A + B^*B$. Since $A^*A \in \mathfrak{I}$ holds by assumption, we have $A^*A = EA^*A$, and thus $B^*B = 0$. Hence $B = 0$ and finally $A = EA \in \mathfrak{I}$. □

Remark. As noted earlier, in finite-dimensional $\mathcal{C}^*$-algebras all subspaces (i.e. in particular all sub-algebras and ideals) are closed in any of the mentioned operator topologies.

We have seen that the left ideals are in 1-1 correspondence to the projections contained in $\mathfrak{A}$. We now tend to the projections contained in the commutant $\mathfrak{A}'$. As the next proposition states, they correspond to the set of invariant subspaces of $\mathfrak{A}$. First, we recall:

Definition 1.20. Let $\mathscr{A}$ be a $*$-algebra of operators in the Hilbert space $\mathcal{H}$. A closed subspace $V \subseteq \mathcal{H}$ is called *invariant under $\mathscr{A}$*, if $\mathscr{A}V \subseteq V$, i.e. Av lies in V for every $A \in \mathscr{A}$ and every $v \in V$.

Lemma 1.21. *Let $\mathscr{A}$ be a $*$-algebra of operators in the Hilbert space $\mathcal{H}$, let $P \in \mathscr{L}(\mathcal{H})$ be an orthogonal projection and $V := \operatorname{ran} P \subseteq \mathcal{H}$ its range. Then, V is invariant under $\mathscr{A}$ if and only if $P \in \mathscr{A}'$.*

Proof. We have the following chain of equivalences:

$$\begin{aligned}
V \text{ is invariant under } \mathscr{A} &\iff Av = PAv \quad \forall A \in \mathscr{A}\ \forall v \in V \\
&\iff AP\xi = PAP\xi \quad \forall A \in \mathscr{A}\ \forall \xi \in \mathcal{H} \\
&\iff AP = PAP \quad \forall A \in \mathscr{A} \\
&\iff AP = PAP = (PA^*P)^* = (A^*P)^* = PA \quad \forall A \in \mathscr{A} \\
&\iff P \in \mathscr{A}'.
\end{aligned}$$

□

In the remaining part of the section, we analyse the set of projections in a unital $\mathcal{C}^*$-algebra more closely. As subset of the hermitian elements, it is partially ordered, and it has a least element and a greatest element, namely 0 and $1_{\mathscr{A}}$. If we exclude 0 from the set, one can consider minimal elements, which we will do now. This, later on, leads to the decomposition of $\mathcal{C}^*$-algebras on finite-dimensional Hilbert spaces. First, we define:

Definition 1.22. A non-zero projection $P \in \mathscr{A}$ is called *minimal (in $\mathscr{A}$)*, if P majorises no other projection except 0 and P.

In other words, a minimal projection is a minimal element of the partially ordered set $\{P \in \mathscr{A} \mid P \text{ projection}, P \neq 0\}$. In the general case, minimal projections need not exist (if they exist, the algebra is called *discrete* or of *type I*, but there are also other types, see [Dix, Part I, Chapter 8]). At least in the finite-dimensional case, we are better off:

Proposition 1.23 ([Arv3, Lemma 1.4.1]). *Let $\mathscr{A}$ be a $*$-algebra of operators in a finite-dimensional Hilbert space $\mathcal{H}$. Then a non-zero projection $P \in \mathscr{A}$ is minimal, iff $P\mathscr{A}P = \mathbb{C} \cdot P$. Moreover, every projection P in $\mathscr{A}$ is a finite sum of mutually orthogonal minimal projections. In particular, there are minimal projections $(P_k)_{k=1}^d$ in $\mathscr{A}$, such that $1_{\mathscr{A}} = \sum_{k=1}^d P_k$ and $P_k P_l = \delta_{kl} P_k$.*

Proof. Let $P \in \mathscr{A}$ be a minimal projection. If $E \in P\mathscr{A}P$ is a projection, then $E = PEP$ implies $P \geq E$, so $E \in \{0, P\}$ by minimality of P. Hence the only projections in $P\mathscr{A}P$ are 0 and P. Note that $\mathscr{B} := P\mathscr{A}P$ is a sub-$*$-algebra of $\mathscr{A}$. Since $\mathscr{B}$ is spanned by its projections (which can be seen as invoking the spectral theorem for the hermitian and anti-hermitian part of a general element $B \in \mathscr{B}$), we conclude $\mathscr{B} = \mathbb{C} \cdot P$. Conversely, if P is not minimal, then there is another projection $Q \in \mathscr{A} \setminus \{0, P\}$ with $0 \leq Q \leq P$. Then $PQP = Q$ implies $Q \in P\mathscr{A}P$, and thus $P\mathscr{A}P \neq \mathbb{C} \cdot P$.

We prove the second statement by induction on $m := \operatorname{rank} P$. The cases $m = 0$ (take the empty sum – defined to be 0) and $m = 1$ (then P itself is minimal) are obvious. Assume that the statement holds true for all $m < m_0$, and let $P \in \mathscr{A}$ be a projection with $\operatorname{rank} P = m_0$, $m_0 \geq 2$. If P itself is minimal, there is nothing to show; otherwise there exists a projection $E \in \mathscr{A} \setminus \{0, P\}$ with $0 \leq E \leq P$, hence $EP = E$. We can decompose $P = EP + (1_{\mathscr{A}} - E)P = E + (P - E)$, where E and $(P - E)$ are orthogonal and both E and $(P - E)$ have ranks strictly between 0 and m_0. Using the induction hypothesis for E and for $(P - E)$ we can write $E = \sum_j E_j$ and $(P - E) = \sum_k F_k$ for two finite sets (E_j) and (F_k) of mutually orthogonal minimal projections. Since E and $(P - E)$ are orthogonal, each E_j is orthogonal to each F_k, as $E_j F_k = (E_j E)((P - E) F_k) = E_j \underbrace{E(P - E)}_{=0} F_k = 0$.

So $P = \sum_j E_j + \sum_k F_k$ is the desired decomposition. □

1.4. Homomorphisms

Definition 1.24. A map $\phi : \mathscr{A} \longrightarrow \mathscr{B}$ between two $\mathcal{C}^*$-algebras $\mathscr{A}$ and $\mathscr{B}$ is called a *$*$-homomorphism*, if it preserves the $*$-algebra structure, i.e. if it is linear, multiplicative and hermiticity-preserving. A bijective $*$-homomorphism is called *$*$-isomorphism.* $\mathscr{A}$ and

$\mathscr{B}$ are called *isomorphic* (which we may write as $\mathscr{A} \simeq \mathscr{B}$), if there exists a $*$-isomorphism between them.

Remark 1.25. Note that the inverse of a $*$-isomorphism is again a $*$-isomorphism. Actually, as the norm on a $\mathcal{C}^*$-algebra is already determined by the $*$-algebra structure[6], every $*$-isomorphism is isometric.

Note 1.26. Since a $*$-homomorphism ϕ maps positive elements a^*a to positive elements $\phi(a^*a) = \phi(a^*)\phi(a) = \phi(a)^*\phi(a)$, we see that $*$-homomorphisms are automatically positive. Moreover, the kernel of a $*$-homomorphism between $\mathcal{C}^*$-algebras is a norm-closed two-sided ideal.

The converse statement, that every norm-closed two-sided ideal is the kernel of a homomorphism, will become obvious in definition 1.37.

The following result shows, that the structure of the centre of a concrete $*$-algebra is preserved under $*$-isomorphisms.

Lemma 1.27. *Let $\mathscr{A}$ and $\mathscr{B}$ are strongly closed concrete $*$-algebras, and let $\phi : \mathscr{A} \longrightarrow \mathscr{B}$ be a $*$-isomorphism. Then we have $\mathfrak{Z}(\mathscr{B}) = \phi\left(\mathfrak{Z}(\mathscr{A})\right)$.*

Proof. We calculate:

$$\begin{aligned}
\mathfrak{Z}(\mathscr{B}) = \mathfrak{Z}(\phi(\mathscr{A})) = \phi(\mathscr{A}) \cap (\phi(\mathscr{A}))' &= \left\{\phi(A) \mid A \in \mathscr{A},\ \phi(A) \in (\phi(\mathscr{A}))'\right\} \\
&= \left\{\phi(A) \,\middle|\, A \in \mathscr{A},\ \forall \tilde{A} \in \mathscr{A} : \phi(A)\phi(\tilde{A}) = \phi(\tilde{A})\phi(A)\right\} \\
&= \left\{\phi(A) \,\middle|\, A \in \mathscr{A},\ \forall \tilde{A} \in \mathscr{A} : \phi(A\tilde{A}) = \phi(\tilde{A}A)\right\} \\
&= \left\{\phi(A) \,\middle|\, A \in \mathscr{A},\ \forall \tilde{A} \in \mathscr{A} : A\tilde{A} = \tilde{A}A\right\} \\
&= \left\{\phi(A) \mid A \in \mathscr{A},\ A \in \mathscr{A}'\right\} = \phi(\mathscr{A} \cap \mathscr{A}') = \phi(\mathfrak{Z}(\mathscr{A})).
\end{aligned}$$

□

In the following we want to distinguish two notions of concrete $\mathcal{C}^*$-algebras being equivalent: namely as $\mathcal{C}^*$-algebras (i.e., there exists a $*$-isomorphism between them), and the stronger notion of unitary equivalence, which we will define next.

Definition 1.28. Two concrete $\mathcal{C}^*$-algebras $\mathscr{A}$ and $\mathscr{B}$ on Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, respectively, are called *unitarily equivalent* (written as $\mathscr{A} \cong \mathscr{B}$), iff there is a unitary map $U : \mathcal{H} \longrightarrow \mathcal{K}$ such that $\mathscr{B} = U\mathscr{A}U^*$.

Note that a necessary condition for unitary equivalence is that the underlying Hilbert spaces are isomorphic. This need not be the case for only $*$-isomorphic algebras. Therefore, for the purpose of dimension reduction, unitary equivalence is the more important notion for us.

Two concrete $\mathcal{C}^*$-algebras that are unitarily equivalent, are also $*$-isomorphic, where the $*$-isomorphism can be *unitarily implemented*, i.e. be of the form $A \mapsto UAU^*$ for some unitary $U : \mathcal{H} \longrightarrow \mathcal{K}$. Moreover, it is easy to see, that if $\mathscr{A}$ is a von Neumann algebra and $\mathscr{B}$ is unitarily equivalent to $\mathscr{A}$, then $\mathscr{B}$ is also a von Neumann algebra.

[6] a fact that we have not proved

Notation. We denote by $\mathcal{M}_d$ ($d \in \mathbb{N}$) the set of $d \times d$ matrices with entries in $\mathbb{C}$. If $\mathcal{H}$ is a d-dimensional Hilbert space, then we know that $\mathscr{L}(\mathcal{H}) \cong \mathcal{M}_d$.

The following theorem is originally due to Wigner; for a mathematically rigorous and detailed proof see [Bar].

Theorem 1.29 (Wigner)**.** *Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be complex Hilbert spaces, let*

$$\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$$

denote the unit circle, and let $\mathcal{R}_i := \{\mathbb{T}\xi \mid \xi \in \mathcal{H}_i \setminus \{0\}\}$ be the set of rays[7] *in $\mathcal{H}_i$ ($i \in \{1,2\}$). Assume that a mapping $T : \mathcal{R}_1 \longrightarrow \mathcal{R}_2$ is given, such that*

$$\forall \xi, \eta \in \mathcal{H}_1 \setminus \{0\} : \quad |\langle T(\mathbb{T}\xi) | T(\mathbb{T}\eta)\rangle| = |\langle \mathbb{T}\xi | \mathbb{T}\eta\rangle| \,.$$

Then there exists a linear or an anti-linear[8] isometry $U : \mathcal{H}_1 \longrightarrow \mathcal{H}_2$ with $\forall \xi \in \mathcal{H} : U\xi \in T(\mathbb{T}\xi)$. If T is surjective, then so is U (so that is, in fact, unitary or anti-unitary).

1.5. Basic operations on $\mathcal{C}^*$-Algebras

In this chapter we recall methods for constructing new $\mathcal{C}^*$-algebras from given ones. As a tool to keep track, how the underlying Hilbert space (and especially its dimension) changes, we occasionally may denote a concrete $*$-algebra $\mathscr{A}$ of operators on a Hilbert space $\mathcal{H}$ by the pair $(\mathscr{A}, \mathcal{H})$. For the same reason, we will distinguish between inner and outer direct sums.

As we realised in chapter 1.1, every von Neumann algebra is a $\mathcal{C}^*$-algebra. Conversely, a concrete $\mathcal{C}^*$-algebra $(\mathscr{A}, \mathcal{H})$ can fail to be a von Neumann algebra of two potential reasons: $\mathscr{A}$ may not be weakly closed in $\mathscr{L}(\mathcal{H})$ – a topological constraint, that however plays no role in finite dimensions – or the unit element of $\mathscr{A}$ (which exists for finite dimensional $\mathcal{H}$ by proposition 1.7) may be not the identity operator on $\mathcal{H}$. In the latter case the situation can be remedied by shrinking the Hilbert space appropriately:

Proposition 1.30. *Let $(\mathscr{A}, \mathcal{H})$ be a weakly closed concrete $\mathcal{C}^*$-algebra. Let P denote the unit element of $\mathscr{A}$ (which evidently is an orthogonal projection in $\mathcal{H}$), and for $A \in \mathscr{A}$, let $A^\flat$ denote the operator*

$$A^\flat : P\mathcal{H} \longrightarrow P\mathcal{H}, \quad \xi \mapsto A\xi.$$

Then the set $\mathscr{A}^\flat := \left\{A^\flat \,\middle|\, A \in \mathscr{A}\right\}$ is a von Neumann algebra in the Hilbert space $P\mathcal{H}$, and we have $(\mathscr{A}, \mathcal{H}) \simeq \left(\mathscr{A}^\flat, P\mathcal{H}\right)$.

Note 1.31. In particular, the class of von Neumann algebras is not stable under $*$-isomorphisms. The algebra $A^\flat$ is sometimes called the *reduced von Neumann algebra* (cf. [Dix, Part I, Ch. 2]).

[7] Here, we define a ray in a Hilbert space to be a vector up to a phase, i.e. up to a complex factor of modulus one. Note that other authors define a ray as $\mathbb{C} \cdot \xi$ for $\xi \in \mathcal{H}$.

[8] An anti-linear isometry is a map f satisfying $f(x + \alpha y) = f(x) + \bar{\alpha} f(y)$ and $\langle f(x)|f(y)\rangle = \langle y|x\rangle$ for $x, y \in \mathcal{H}$, $\alpha \in \mathbb{C}$.

Proof. This is only a reformulation of Lemma A.6ii). □

Next, we define the product (or outer direct sum) of $\mathcal{C}^*$-algebras:

Definition 1.32. Let $(\mathscr{A}_k, \mathcal{H}_k)$ be concrete unital $\mathcal{C}^*$-algebras for $k \in \{1, \ldots, m\}$. Consider the Hilbert space direct sum[9] $\mathcal{H}$ of the $\mathcal{H}_k$ and the $\mathcal{C}^*$-algebra $\mathscr{A}$ on $\mathcal{H}$ consisting of tuples $(A_k)_{k=1}^m$ with $A_k \in \mathscr{A}_k$, mapping $(\xi_1, \cdots, \xi_m) \in \mathcal{H}$ to $(A_1\xi_1, \cdots, A_m\xi_m)$. Then $\mathscr{A}$ is called the *product* or the *outer direct sum* of the $\mathscr{A}_k$, which we denote by

$$\mathscr{A} = \mathscr{A}_1 \times \cdots \times \mathscr{A}_m, \quad \text{or} \quad \mathscr{A} = \bigtimes_{k=1}^m \mathscr{A}_k.$$

Proposition 1.33. *The outer direct sum is associative, and in the situation of Definition 1.32 the following statements hold true:*

i) *If $1_{\mathscr{A}_k} = \mathrm{id}_{\mathcal{H}_k}$ for all k, then the commutant and double commutant of $\mathscr{A}$ can be computed factor-wise, i.e.*

$$\mathscr{A}' = \left(\bigtimes_{k=1}^m \mathscr{A}_k\right)' = \bigtimes_{k=1}^m \mathscr{A}_k', \qquad \mathscr{A}'' = \bigtimes_{k=1}^m \mathscr{A}_k''$$

In particular, $\mathscr{A}$ is a von Neumann algebra, if all the $\mathscr{A}_k$ are von Neumann algebras.

ii) *The natural inclusion maps*

$$\iota_k : \mathscr{A}_k \longrightarrow \mathscr{A}, \quad A \longmapsto (0, \cdots, 0, \underbrace{A}_{k\text{-th position}}, 0, \cdots, 0)$$

are injective $*$-homomorphisms, and the projections

$$p_k : \mathscr{A} \longrightarrow \mathscr{A}_k, \quad (A_1, \ldots, A_m) \longmapsto A_k$$

are surjective $*$-homomorphisms. Moreover, if all $\mathcal{H}_k$ are finite-dimensional and if we equip $\mathcal{H}$ and the $\mathcal{H}_k$ with the Hilbert-Schmidt scalar products, then p_k is the adjoint map of ι_k, and vice versa. In particular, an element $(A_1, \ldots, A_m)$ is positive or hermitian, iff all A_j are positive or hermitian, respectively; and the "embedded factors" $\iota_k(\mathscr{A}_k) = \ker p_k \subseteq \mathscr{A}$ are two-sided ideals in $\mathscr{A}$.

[9] I.e. $\mathcal{H} = \mathcal{H}_1 \times \cdots \times \mathcal{H}_m$ as a set, and the inner product is given by

$$\langle (\phi_1, \ldots, \phi_m) | (\psi_1, \ldots, \psi_m) \rangle = \sum_{k=1}^m \langle \phi_k | \psi_k \rangle \ \text{ for } \phi_k, \psi_k \in \mathcal{H}_k,\ k \in \{1, \ldots, m\}.$$

Proof. i) We only consider the case $m = 2$ (i.e., two summands); the general case follows by induction on m. We represent elements of $\mathscr{L}(\mathcal{H}_1 \times \mathcal{H}_2)$ as matrices and get

$$\begin{aligned}
&\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in (\mathscr{A}_1 \times \mathscr{A}_2)' \\
&\qquad \Longleftrightarrow \forall X \in \mathscr{A}_1\ \forall Y \in \mathscr{A}_2 : \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} \\
&\qquad \Longleftrightarrow \forall X \in \mathscr{A}_1\ \forall Y \in \mathscr{A}_2 : \begin{pmatrix} XA & XB \\ YC & YD \end{pmatrix} = \begin{pmatrix} AX & BY \\ CX & DY \end{pmatrix}.
\end{aligned}$$

The equations in the diagonal entries are equivalent to $A \in \mathscr{A}_1' \ \wedge\ D \in \mathscr{A}_2'$. Setting $X = \mathrm{id}_{\mathcal{H}}$ and $Y = 0$ yields $B = 0 = C$ in the non-diagonal entries. This shows (i).

ii) The statements about the ι_k and p_k are immediately apparent from the calculation rules of the product of algebras, and the statement about positivity follows from that since $*$-homomorphisms are positive (cf. Note 1.26). In order to prove that p_k and ι_k are mutually adjoint, let $A \in \mathscr{A}_k$, $B = (B_1, \dots, B_m) \in \mathscr{A}$, and calculate

$$\begin{aligned}
\mathrm{tr}_{\mathcal{H}}\left(\iota_k(A)^*(B_1, \dots, B_m)\right) &= \mathrm{tr}_{\mathcal{H}}\left(0, \dots, 0, A^*B_k, 0, \dots, 0\right) \\
&= \mathrm{tr}_{\mathcal{H}_k}\left(A^*B_k\right) = \mathrm{tr}_{\mathcal{H}_k}\left(A^*p_k(B)\right).
\end{aligned}$$

□

The fact, that the product of $\mathcal{C}^*$-algebras consists of "block algebras" which are two-sided ideals, motivates the following Definition:

Definition 1.34. Let $(\mathscr{A}, \mathcal{H})$ be a concrete $\mathcal{C}^*$-algebra, and suppose that $\mathscr{I}_k$, $k \in \{1, \dots, m\}$, are two-sided ideals of $\mathscr{A}$, so that $\mathscr{I}_k \cap \mathscr{I}_\ell = \{0\}$ for $k \neq \ell$. We say that $\mathscr{A}$ is the (inner) direct sum of the $\mathscr{I}_k$, denoted

$$\mathscr{A} = \bigoplus_{k=1}^{m} \mathscr{I}_k,$$

if every $A \in \mathscr{A}$ admits a unique decomposition $A = \sum_{k=1}^m B_k$ into elements $B_k \in \mathscr{I}_k$.

Proposition 1.35. *In the situation of an inner direct sum $\mathscr{A} = \bigoplus_{k=1}^m \mathscr{I}_k$ of concrete $\mathcal{C}^*$-algebras on a finite-dimensional Hilbert space $\mathcal{H}$, the projections onto the direct summands are given by the Hilbert-Schmidt-adjoint of the inclusion maps $\mathscr{I}_k \hookrightarrow \mathscr{A}$.*

Moreover, even for infinite dimensional $\mathcal{H}$, if the ideals are strongly (or, equivalently, weakly) closed, then the projections π_k onto the direct summands are given by $A \mapsto P_k A$, where P_k is the unit of the $*$-algebra $\mathscr{I}_k$ (cf. Theorem A.7), and equal to the orthogonal projection onto $\overline{\mathrm{span}\, \mathscr{I}_k \mathcal{H}}$. In particular, the π_k are $*$-homomorphisms, and $\sum_{k=1}^m \pi_k = \mathrm{id}_{\mathscr{A}}$.

Proof. We prove the second assertion first. By Proposition 1.18, for each k there exists a central projection $P_k \in \mathfrak{Z}(\mathscr{A}) \cap \mathscr{I}_k$, such that $\mathscr{I}_k = P_k\mathscr{A} = \mathscr{A}P_k$. Since P_k is the unit of $\mathscr{I}_k$, it follows by Theorem A.7 that P_k is the projection onto $\overline{\mathrm{span}\, \mathscr{I}_k \mathcal{H}}$.

For $A_1, A_2 \in \mathscr{A}$ we have $A_j = \sum_{k=1}^m \pi_k(A_j)$, thus

$$A_1 A_2 = \sum_{k=1}^m \pi_k(A_1 A_2) = \sum_{k=1}^m \sum_{\ell=1}^m \underbrace{\pi_k(A_1)\pi_\ell(A_2)}_{\in \mathscr{I}_k \cap \mathscr{I}_\ell} = \sum_{k=1}^m \pi_k(A_1)\pi_k(A_2).$$

By uniqueness of the decomposition we infer $\pi_k(A_1 A_2) = \pi_k(A_1)\pi_k(A_2)$, and by similar reasoning it holds that $\pi_k(A_1^*) = \pi_k(A_1)^*$. So the π_k are $*$-homomorphisms. Moreover, π_k must act as the identity on $\mathscr{I}_k$, which follows by decomposing elements from $\mathscr{I}_k$ and using that $\mathscr{I}_k \cap \mathscr{I}_\ell = \{0\}$ for $\ell \neq k$. Hence for $A \in \mathscr{A}$ we get

$$\begin{aligned} A &= \sum_{k=1}^m \underbrace{\pi_k(A)}_{\in \mathscr{I}_k} = \sum_{k=1}^m P_k \pi_k(A) = \sum_{k=1}^m \pi_k(P_k)\pi_k(A) \\ &= \sum_{k=1}^m \pi_k(\underbrace{P_k A}_{\in \mathscr{I}_k}) = \sum_{k=1}^m P_k A, \end{aligned}$$

hence (again by uniqueness of decomposition) $\pi_k(A) = P_k A = A P_k$.

Now to the first part. Assume that $\mathcal{H}$ is finite dimensional, and let $\iota_k : \mathscr{I}_k \hookrightarrow \mathscr{A}$ denote the inclusion maps. Then for $A \in \mathscr{A}$, $B \in \mathscr{I}_k$ we can calculate

$$\operatorname{tr}_{\mathcal{H}}\left((\pi_k(A))^* B\right) = \operatorname{tr}_{\mathcal{H}}\left((P_k A)^* B\right) = \operatorname{tr}_{\mathcal{H}}\left(A^* P_k B\right) = \operatorname{tr}_{\mathcal{H}}\left(A^* B\right) = \operatorname{tr}_{\mathcal{H}}\left(A^* \iota_k(B)\right).$$

□

The next Proposition shows, that outer and inner direct sums are closely related; up to reducing the individual summands, we have unitary equivalence.

Corollary 1.36. *Let $(\mathscr{A}, \mathcal{H})$ be a concrete strongly closed $\mathcal{C}^*$-algebra composed of a direct sum $\mathscr{A} = \bigoplus_{k=1}^m \mathscr{A}_k$. Then*

$$(\mathscr{A}, \mathcal{H}) = \bigoplus_{k=1}^m (\mathscr{A}_k, \mathcal{H}) \simeq \bigtimes_{k=1}^m \left(\mathscr{A}_k^\flat, 1_{\mathscr{A}_k}\mathcal{H}\right),$$

where the last expression is a von Neumann algebra.

Proof. The map

$$\phi : \bigoplus_{k=1}^m (\mathscr{A}_k, \mathcal{H}) \longrightarrow \bigtimes_{k=1}^m \left(\mathscr{A}_k^\flat, 1_{\mathscr{A}_k}\mathcal{H}\right), \quad \sum_{k=1}^m A_k \longmapsto \left(A_k^\flat\right)_{k=1}^m,$$

implements the $*$-isomorphism in question, as one can easily see from Propositions 1.30 and 1.35. That $\bigtimes_{k=1}^m \left(\mathscr{A}_k^\flat, 1_{\mathscr{A}_k}\mathcal{H}\right)$ is a von Neumann algebra, follows from Proposition 1.33i). □

Next, we define quotients of von Neumann algebras.

Definition 1.37. Let $\mathfrak{A}$ be a von Neumann algebra on $\mathcal{H}$ and $\mathfrak{I} \subseteq \mathfrak{A}$ a strongly closed two-sided ideal in $\mathfrak{A}$ (so in particular, a $*$-subalgebra). Let E denote the greatest projection in $\mathfrak{I}$ (cf. the double commutant theorem) and $\mathcal{E} := \operatorname{ran} E$. We define the *quotient von Neumann algebra* $\mathfrak{A}/\mathfrak{I}$ as a von Neumann algebra on the Hilbert space $\mathcal{H}/\mathcal{E}$, acting by

$$(A + \mathfrak{I})(h + \mathcal{E}) := Ah + \mathcal{E}.$$

Proof of well-definedness. For two elements $A, \tilde{A} \in \mathfrak{A}$ with $A - \tilde{A} \in \mathfrak{I}$ and two vectors $h, \tilde{h} \in \mathcal{H}$ with $h - \tilde{h} \in \mathcal{E}$ we have that

$$Ah - \tilde{A}\tilde{h} = Ah - \tilde{A}h + \tilde{A}h - \tilde{A}\tilde{h} = \underbrace{(A - \tilde{A})}_{\in \mathfrak{I}} h + \tilde{A} \underbrace{(h - \tilde{h})}_{\in \mathcal{E}} = \underbrace{E(A - \tilde{A})h}_{\in \mathcal{E}} + \tilde{A}E(h - \tilde{h}).$$

Since $\mathfrak{I}$ is an ideal and $E \in \mathfrak{I}$, we have that $\tilde{A}E \in \mathfrak{I}$, thus $\tilde{A}E(h-\tilde{h}) = E\tilde{A}(h-\tilde{h}) \in \mathcal{E}$. $\square$

In order to define m-positivity between $\mathcal{C}^*$-algebras, we need one more notion, namely the tensor product of von Neumann algebras.

Definition 1.38. Let $\mathscr{A}$ and $\mathscr{B}$ be $\mathcal{C}^*$-algebras on Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, respectively. We consider the tensor product $\mathscr{A} \otimes \mathscr{B}$ as a $\mathcal{C}^*$-algebra on the tensor product of Hilbert spaces $\mathcal{H} \otimes \mathcal{K}$.[10]

The $*$-algebra-operations are, of course, given by $(A_1 \otimes B_1) \cdot (A_2 \otimes B_2) = (A_1 A_2) \otimes (B_1 B_2)$ and $(A \otimes B)^* = A^* \otimes B^*$. Note that for simple tensors we have $\|A \otimes B\| = \|A\| \cdot \|B\|$

In the special case $\mathscr{B} = \mathcal{M}_m = \mathscr{L}(\mathbb{C}^m)$, clearly $\mathcal{H} \otimes \mathbb{C}^m$ is isomorphic as a Hilbert space to the m-fold direct product $\mathcal{H}^m = \bigtimes_{j=1}^m \mathcal{H}$, where a natural unitary map is given by (the linear extension of)

$$\sum_{j=1}^m h_j \otimes e_j \mapsto (h_j)_{j=1}^m ,$$

where $e_j \in \mathbb{C}^m$ is the j-th canonical unit vector.

Definition 1.39. Let $\mathcal{M}_d$ denote the von Neumann algebra of all $d \times d$ matrices with entries in $\mathbb{C}$. Let $\mathcal{S}$ be an operator system on the Hilbert space $\mathcal{H}$. For any number $n \in \mathbb{N}$, let us agree to regard $\mathscr{A} \otimes \mathcal{M}_n$ as a $\mathcal{C}^*$-algebra in the Hilbert direct sum $\mathcal{H}^n$ by means of the canonical isomorphism

$$\begin{aligned} \mathcal{S} \otimes \mathcal{M}_n \quad &\longrightarrow \quad \mathrm{Mat}_n(\mathcal{S}), \\ \sum_{k=1}^N S_k \otimes \left(m_{ij}^{(k)}\right)_{ij} \quad &\longmapsto \quad \sum_k \left(m_{ij}^{(k)} \cdot S_k\right)_{ij} , \end{aligned}$$

[10] If $\mathcal{H}$ or $\mathcal{K}$ (or both) are infinite-dimensional, then by $\mathcal{H} \otimes \mathcal{K}$ we mean the closure of the algebraic tensor product of $\mathcal{H}$ and $\mathcal{K}$, which is again a Hilbert space with scalar product uniquely determined by its values on simple tensors as

$$\langle \xi_1 \otimes \eta_1 | \xi_2 \otimes \eta_2 \rangle = \langle \xi_1 | \xi_2 \rangle \cdot \langle \eta_1 | \eta_2 \rangle \text{ for } \xi_1, \xi_2 \in \mathcal{H},\ \eta_1, \eta_2 \in \mathcal{K}.$$

In this case, $\mathscr{A} \otimes \mathscr{B}$ means the closure of the algebraic tensor product of $\mathscr{A}$ and $\mathscr{B}$ with respect to the uniform topology in $\mathscr{L}(\mathcal{H} \otimes \mathcal{K}) \cong \mathscr{L}(\mathcal{H}) \otimes \mathscr{L}(\mathcal{K})$.

where $N \in \mathbb{N}$, and for $k \in \{1, \dots, N\}$ $S_k \in \mathcal{S}$ and $m^{(k)} = (m_{ij}^{(k)})_{ij} \in \mathcal{M}_n$.

1.6. Basic Structure theory of $\mathcal{C}^*$- and von Neumann algebras

There are several possible accesses to the structure theory of finite-dimensional $\mathcal{C}^*$-algebras. First, for finite-dimensional algebras we have the classical algebraic approach leading to the Wedderburn theorem, see e.g. [Lan, §3]. Note that this approach does not use the $*$-structure, so it will be only of limited use to us. Second, in [Arv3, Section 1.4], the subalgebras of $\mathscr{L}\mathscr{C}(\mathcal{H})$, the set of compact operators on the Hilbert space $\mathcal{H}$, which also form a $\mathcal{C}^*$-algebra are classified by quite elementary methods. We will follow this path, but restrict to the case there $\dim \mathcal{H} < +\infty$. Third, one can use the spectral theory of abelian $\mathcal{C}^*$-algebras to classify finite-dimensional $\mathcal{C}^*$-algebras up to $*$-isomorphisms, see e.g. [Tak, Chapter I.11].

1.6.1. Strongly closed concrete $*$-algebras

In the first place we find that the "building blocks" of $\mathcal{C}^*$-algebras are two-sided ideals; more precisely that every concrete $*$-algebra – given that it is strongly closed – is the direct sum of its minimal ideals[11].

Definition 1.40. A concrete $*$-algebra $(\mathscr{A}, \mathcal{H})$ is called

- *non-degenerate* if $\overline{\mathrm{span}\mathscr{A}\mathcal{H}} = \mathcal{H}$.[12]
- *simple*, if it contains no non-trivial strongly closed ideals.[13]
- a *factor*, if $\mathfrak{Z}(\mathscr{A}) = \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}$.
- *irreducible*, if $\mathscr{A} \neq \{0\}$ and there are no closed non-trivial subspaces $V \subset \mathcal{H}$ that are invariant under $\mathscr{A}$.[14]

The next proposition summarises the relations between the various properties:

Proposition 1.41. *Let $(\mathscr{A}, \mathcal{H})$ be a strongly closed concrete $*$-algebra.*

a) $\quad$ *$\mathscr{A}$ is non-degenerate* $\iff$ $1_{\mathscr{A}} = \mathrm{id}_{\mathcal{H}}$.

---

[11] An ideal is minimal, iff the corresponding central projection is a minimal projection.

[12] Note that by $\mathrm{span}X$ we mean the set of *finite* linear combinations of elements from X, i.e.

$$\mathrm{span}X = \left\{ \sum_{j=1}^{n} c_j x_j \;\middle|\; n \in \mathbb{N},\, c_j \in \mathbb{C}, x_j \in X \right\}$$

[13] The definition of simplicity varies from author to author by means of in which topology the ideals shall be closed. Our choice is used throughout books about von Neumann algebras.

[14] The demand $\mathscr{A} \neq \{0\}$ might seem superfluous (at least for $\mathcal{H} \neq \{0\}$), but it is not, as the example $\mathscr{A} = \{0\}$ on $\mathcal{H} = \mathbb{C}^1$ shows.

b) *A strongly closed ideal $\mathcal{I}$ in $\mathscr{A}$ is simple, iff the corresponding central projection $1_{\mathcal{I}}$ (cf. Prop. 1.18) is minimal in $\mathfrak{Z}(\mathscr{A})$.*

c) *$\mathscr{A}$ is simple $\iff$ $\mathfrak{Z}(\mathscr{A}) = \mathbb{C} \cdot 1_{\mathscr{A}}$*

d) *$\mathscr{A}$ is a factor $\iff$ $\mathscr{A}$ is non-degenerate and simple.*

e) *$\mathscr{A}$ is irreducible $\implies$ $\mathscr{A}$ is a factor. Moreover, for $\mathcal{H} \neq \{0\}$, the following statements are equivalent:*

  i) *$\mathscr{A}$ is irreducible.*

  ii) *The only projections lying in $\mathscr{A}'$ are 0 and $\mathrm{id}_{\mathcal{H}}$.*

  iii) *$\mathscr{A}' = \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}$.*

  iv) *Every vector is cyclic for $\mathscr{A}$, i.e. $\overline{\mathscr{A}\xi} = \mathcal{H}$ for all $\xi \in \mathcal{H} \setminus \{0\}$.*

  v) *$\mathscr{A} = \mathscr{L}(\mathcal{H})$.*

Proof. a) is a consequence of the von Neumann bicommutant theorem (Theorem A.7): The "$\Leftarrow$"-direction is obvious, whereas the "$\Rightarrow$" follows from the fact that the unit $1_{\mathscr{A}}$ is given by the orthogonal projection onto the subspace $\overline{\mathrm{span}\mathscr{A}\mathcal{H}}$, which is equal to $\mathcal{H}$ if $\mathscr{A}$ is non-degenerate.

b) Recall that by Proposition 1.18 every strongly closed ideal $\mathcal{J}$ in $\mathscr{A}$ can be written as

$$\mathcal{J} = 1_{\mathcal{J}}\mathscr{A} = \{A \in \mathscr{A} \mid 1_{\mathcal{J}}A = A\}.$$

Let $\mathcal{I}$ be a strongly closed ideal in $\mathscr{A}$. If $1_{\mathcal{I}}$ is not minimal in $\mathfrak{Z}(\mathscr{A})$, there exists a projection $P \in \mathfrak{Z}(\mathscr{A})$ strictly between 0 and $1_{\mathcal{I}}$ which we can use to define another strongly closed ideal $\mathcal{J} := P\mathscr{A}$, so that $P = 1_{\mathcal{J}}$. Since $1_{\mathcal{I}}P = P = P1_{\mathcal{I}}$, we have

$$\mathcal{J} = P\mathscr{A} = (P1_{\mathcal{I}})\mathscr{A} = P(1_{\mathcal{I}}\mathscr{A}) = P\mathcal{I} \subseteq \mathscr{I};$$

but $1_{\mathcal{I}} \notin \mathcal{J}$ as $1_{\mathcal{J}}1_{\mathcal{I}} = P1_{\mathcal{I}} = P \neq 1_{\mathcal{I}}$. Hence $\mathcal{I}$ is not simple.

Conversely, if $\mathcal{I}$ is not simple, then there exists a strongly closed ideal $\mathcal{J}$ satisfying $\{0\} \subsetneq \mathcal{J} \subsetneq \mathcal{I}$, hence $1_{\mathcal{J}}$ is a central projection with $0 \lneq 1_{\mathcal{J}} \lneq 1_{\mathcal{I}}$, hence $1_{\mathcal{I}}$ is not minimal.

c) follows from (b) by setting $\mathcal{I} = \mathscr{A}$.

d) By parts (a) and (c), $\mathscr{A}$ is non-degenerate and simple, iff $1_{\mathscr{A}} = \mathrm{id}_{\mathcal{H}}$ and $\mathfrak{Z}(\mathscr{A}) = \mathbb{C} \cdot 1_{\mathscr{A}}$, which means that $\mathscr{A}$ is a factor.

e) We show first, that if $\mathscr{A}$ is irreducible, then it is non-degenerate. To this aim, consider the subspace $V := \ker 1_{\mathscr{A}}$. V is invariant under $\mathscr{A}$, since for $\xi \in V$ and $A \in \mathscr{A}$ we have $A\xi = A1_{\mathscr{A}}\xi = 0 \in V$. By irreducibility, either $V = \{0\}$ – in which case $1_{\mathscr{A}} = \mathrm{id}_{\mathcal{H}}$, so that $\mathscr{A}$ is non-degenerate by part (a) – or $V = \mathcal{H}$. In the latter case we have $1_{\mathscr{A}} = 0$, hence $\mathscr{A} = \{0\}$, which contradicts the irreducibility of $\mathscr{A}$.

We come to the proof of the stated equivalences. "$(i) \Leftrightarrow (ii)$" follows from Lemma 1.21, and "$(ii) \Leftrightarrow (iii)$" is Lemma 1.16.

"$(iii) \wedge (i) \Rightarrow (v)$": Since $\mathscr{A}' = \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}$, we have that $\mathscr{A}'' = (\mathbb{C} \cdot \mathrm{id}_{\mathcal{H}})' = \mathscr{L}(\mathcal{H})$. On the other hand, by the double commutant theorem A.7 in Appendix A, $\mathscr{A}''$ is equal to

$\mathscr{A} + \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}$. By assumption $\mathscr{A}$ is irreducible, hence a factor, hence non-degenerate by part d), hence we have $1_{\mathscr{A}} = \mathrm{id}_{\mathcal{H}}$ by part a). Thus $\mathscr{L}(\mathcal{H}) = \mathscr{A}'' = \mathscr{A} + \underbrace{\mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}}_{\subseteq \mathscr{A}} = \mathscr{A}$.

"$(v) \Rightarrow (iv)$": Fix $\xi \in \mathcal{H} \setminus \{0\}$. Then for $\eta \in \mathcal{H}$ there exist maps $M \in \mathscr{L}(\mathcal{H})$ such that $M\xi = \eta$, for example $M = \|\xi\|^{-2} \cdot |\eta\rangle\langle\xi|$. Thus $\mathscr{L}(\mathcal{H})\xi = \mathcal{H}$.

"$(iv) \Rightarrow (i)$": Let $V \subseteq \mathcal{H}$ be a closed subspace invariant under $\mathscr{A}$, and assume $V \neq \{0\}$. Then there exists $\xi \in V \setminus \{0\}$ and by assumption we have $\mathcal{H} = \overline{\mathscr{A}\xi} \subseteq \overline{\mathscr{A}V} \subseteq \overline{V} = V$, hence $V = \mathcal{H}$. □

The properties of a concrete $\mathcal{C}^*$-algebra of being non-degenerate, being irreducible and being a factor are *not* stable under $*$-isomorphisms – for example, one could simply enlarge the underlying Hilbert space to destroy these properties, hence basically destroying non-degeneracy. A notable example is simplicity:

Corollary 1.42. *Let $\mathscr{A}$ and $\mathscr{B}$ are strongly closed concrete $*$-algebras, that are $*$-isomorphic. Then $\mathscr{A}$ is simple iff $\mathscr{B}$ is.*

Proof. By Lemma 1.27, $\mathfrak{Z}(\mathscr{B}) = \phi(\mathfrak{Z}(\mathscr{A}))$, and as unit elements are unique in an algebra, we have necessarily $\phi(1_{\mathscr{A}}) = 1_{\mathscr{B}}$. The claim then follows by part c) of Proposition 1.41. □

1.6.2. Structure of $*$-algebras on finite dimensional Hilbert spaces

In this section, we want to give a complete characterisation of concrete $\mathcal{C}^*$-algebras on finite-dimensional Hilbert spaces. With the tools developed so far, we can as a first step reduce the problem to *simple* algebras, as the next Proposition shows.

Proposition 1.43. *Let $\mathscr{A}$ be a concrete $\mathcal{C}^*$-algebra on a finite-dimensional Hilbert space $\mathcal{H}$. Then, $\mathscr{A}$ is the direct sum of finitely many simple ideals $\mathscr{A}_k$ of $\mathscr{A}$, i.e.*

$$\mathscr{A} = \bigoplus_{k=1}^{n} \mathscr{A}_k$$

Proof. Consider the $\mathcal{C}^*$-algebra $\mathscr{Z} := \mathfrak{Z}(\mathscr{A}) = \mathscr{A} \cap \mathscr{A}'$, which contains $1_{\mathscr{A}}$, so that $1_{\mathscr{Z}} = 1_{\mathscr{A}}$. By proposition 1.23 there are mutually orthogonal minimal projections $P_1, \ldots, P_n \in \mathscr{Z}$, such that $1_{\mathscr{A}} = \sum_{k=1}^{n} P_k$. Let $\mathscr{A}_k := P_k\mathscr{A}$ denote the corresponding simple ideals in $\mathscr{A}$. Then we have obviously $\mathscr{A}_k \cap \mathscr{A}_l = \{0\}$ for $k \neq l$, and a general $A \in \mathscr{A}$ can be decomposed as

$$A = 1_{\mathscr{A}} A = \sum_{k=1}^{n} (P_k A),$$

hence $\mathscr{A} = \bigoplus_{k=1}^{n} \mathscr{A}_k$. □

Now, in order to move forward towards a complete characterisation of concrete $\mathcal{C}^*$-algebras on finite-dimensional Hilbert spaces, we need to analyse the structure of simple algebras further. We will show that, up to $*$-isomorphism, they are full matrix algebras $\mathcal{M}_d$ for some $d \in \mathbb{N}$. As a technical aid, we define:

Definition 1.44. Let $\mathscr{A}$ be a $*$-algebra. A doubly indexed collection $w_{ij} \in \mathscr{A} \setminus \{0\}$ with i and j running over $\{1, \ldots, d\}$ satisfying

$$\forall i,j,k,l \in \{1,\ldots,d\}: \quad w_{ij}^* = w_{ji} \ \wedge \ w_{ij}w_{kl} = \delta_{jk}w_{il}$$

and $\sum_{i=1}^d w_{ii} = 1_{\mathscr{A}}$, is called a *system of matrix units for $\mathscr{A}$.*

Note that from the defining equations for matrix units it follows that the w_{ii} are mutually orthogonal self-adjoint projections, with $w_{ii} \neq w_{jj}$ for $i \neq j$.

Proposition 1.45. *[Tak, Theorem 11.2]Let $\mathscr{A}$ be a $*$-algebra of operators on the finite-dimensional Hilbert space $\mathcal{H}$. Then the following statements are equivalent:*

i) *$\mathscr{A}$ is simple.*

ii) *There exist a number $d \in \mathbb{N}_0$ and a system of matrix units $(w_{ij})_{i,j=1}^d$ for $\mathscr{A}$, with w_{ii} being minimal (in particular non-zero) projections.*

iii) *$\mathscr{A}$ is $*$-isomorphic to $\mathcal{M}_d$ for some $d \in \mathbb{N}_0$.*

In this case, the numbers d in parts ii) and iii) coincide, and the system of matrix units (w_{ij}) from ii) forms an algebraic basis for $\mathscr{A}$.

Proof. First, let us deal with the trivial case $\mathscr{A} = \{0\}$. Then $\mathscr{A}$ is simple by definition (there are no non-trivial ideals contained in $\mathscr{A}$), and (ii) and (iii) are fulfilled with $d = 0$. So henceforth we assume that $\mathscr{A} \neq \{0\}$, in particular $1_{\mathscr{A}} \neq 0$.

"*(i)* $\Rightarrow$ *(ii)*". By Proposition 1.23 we can write $1_{\mathscr{A}} = \sum_{j=1}^d p_j$ for some minimal, mutually orthogonal projections $p_j \in \mathscr{A}$.

Note that for $i \in \{1, \ldots, d\}$ the subsets $\mathscr{B}_i := \operatorname{span}(\mathscr{A} p_i \mathscr{A})$ are manifestly two-sided ideals in $\mathscr{A}$, and $0 \neq p_i \in \mathscr{B}_i$. Since $\mathscr{A}$ is simple, we conclude $\mathscr{B}_i = \mathscr{A}$ for all i. We define the subspaces $\mathscr{B}_{ij} := p_i \mathscr{A} p_j \subseteq \mathscr{A}$ for $i, j \in \{1, \ldots, d\}$ and observe that

$$\operatorname{span}\left(\mathscr{B}_{ij}\mathscr{B}_{ij}^*\right) = \operatorname{span}\left((p_i\mathscr{A}p_j)\,(p_i\mathscr{A}p_j)^*\right) = p_i \underbrace{\operatorname{span}\left(\mathscr{A}p_j\mathscr{A}\right)}_{=\mathscr{A}} p_i = p_i\mathscr{A}p_i = \mathbb{C}\cdot p_i,$$

where the last equation follows from minimality of p_i (cf. Proposition 1.23). Thus, every $\mathscr{B}_{ij}$ contains non-zero elements. For every $i \in \{1, \ldots, d\}$, fix a normalised element $v_i \in \mathscr{B}_{1i}$. Note that by definition of $\mathscr{B}_{1i}$, $v_i = p_1 v_i = v_i p_i = p_1 v_i p_i$. Since $v_i^* v_i$ is manifestly positive and lies in $\mathscr{B}_{1i}^*\mathscr{B}_{1i} = \mathscr{B}_{i1}\mathscr{B}_{i1}^* \subseteq \mathbb{C}\cdot p_i$, we have $v_i^* v_i = \lambda_i p_i$ for some number $\lambda_i > 0$. The $\mathcal{C}^*$-property gives $\lambda_i = |\lambda_i| = \|\lambda_i p_i\| = \|v_i^* v_i\| = \|v_i\|^2 = 1$, hence $v_i^* v_i = p_i$. Taking adjoints, we see $v_i^* \in \mathscr{B}_{i1}$, hence it follows analogously that $v_i v_i^* = p_1$ for all i.

Now we define for $i, j \in \{1, \ldots, d\}$ the elements $w_{ij} := v_i^* v_j$ and verify their property of being matrix units: for $i, j, k, l \in \{1, \ldots, d\}$ we calculate

$$w_{ij}^* = \left(v_i^* v_j\right)^* = v_j^* v_i = w_{ji},$$

$$w_{ij}w_{kl} = v_i^* (v_jp_j) (v_kp_k)^* v_l = v_i^* v_j \underbrace{p_jp_k}_{=\delta_{jk}p_j} v_k^* v_l = \delta_{jk}\, \underbrace{v_i^* \underbrace{v_j v_j^*}_{=p_1}}_{=v_i} v_l = \delta_{jk} w_{il},$$

and finally

$$\sum_{i=1}^{d} w_{ii} = \sum_{i=1}^{d} v_i^* v_i = \sum_{i=1}^{d} p_i = 1_{\mathscr{A}}.$$

By construction, the $w_{ii} = v_i^* v_i = p_i$ are minimal projections.

"$(ii) \Rightarrow (iii)$". Set $p_i := w_{ii}$ and $\mathscr{B}_{ij} := p_i \mathscr{A} p_j$ as in the last part. Before we will construct the $*$-isomorphism, we show that all $\mathscr{B}_{ij}$ are one-dimensional. Indeed, $0 \neq w_{ij} \in \mathscr{B}_{ij}$, so $\dim \mathscr{B}_{ij} \geq 1$. Let $a, b \in \mathscr{B}_{ij}$ be such that $\|a\| = \|b\| = 1$. From the calculation

$$\mathscr{B}_{ij}\mathscr{B}_{ij}^* = (p_i \mathscr{A} p_j) (p_i \mathscr{A} p_j)^* = p_i \underbrace{\mathscr{A} p_j \mathscr{A}}_{\subseteq \mathscr{A}} p_i \subseteq p_i \mathscr{A} p_i = \mathbb{C} \cdot p_i,$$

where again the last equality is by minimality of $p_i = w_{ii}$ and Proposition 1.23, we can infer that $ab^* = \lambda p_i$ and $b^*b = \mu p_j$ for some $\lambda, \mu \in \mathbb{C}$. Since bb^* is inherently positive, we even know $\mu \geq 0$, and by the $\mathcal{C}^*$-property we have $1 = \|b\|^2 = \|b^*b\| = \mu^2 \|p_j\| = \mu^2$, hence $\mu = 1$, hence $b^*b = p_j$. Thus, the equation

$$\lambda b = \lambda(p_i b) = (\lambda p_i) b = (ab^*) b = a(b^*b) = ap_j = a$$

shows that a and b are linearly dependent. As a and b were arbitrary, $\mathscr{B}_{ij}$ is indeed one-dimensional, and we may write it as $\mathscr{B}_{ij} = \mathbb{C} \cdot w_{ij}$. Moreover, we can decompose

$$\mathscr{A} = 1_{\mathscr{A}} \mathscr{A} 1_{\mathscr{A}} = \left(\sum_{i=1}^{d} p_i \right) \mathscr{A} \left(\sum_{j=1}^{d} p_j \right) = \sum_{i,j=1}^{d} p_i \mathscr{A} p_j = \sum_{i,j=1}^{d} \mathscr{B}_{ij},$$

where the last sum is a direct sum in the sense of vector subspaces[15]. Therefore, the w_{ij} constitute a basis of $\mathscr{A}$, and we may define a $*$-isomorphism $\mathscr{A} \longrightarrow \mathcal{M}_d$ by (the unique linear extension of) $w_{ij} \longmapsto E_{ij}$, where $E_{ij} := |e_i \rangle\langle e_j| \in \mathcal{M}_d$ are the standard matrix units in $\mathcal{M}_d$.

"$(iii) \Rightarrow (i)$". It suffices to show that $\mathcal{M}_d$ is simple, since $*$-isomorphisms preserve ideals. But this follows directly from Prop. 1.41: By part e), $\mathcal{M}_d = \mathscr{L}(\mathbb{C}^d)$ is irreducible, thus in particular simple. $\square$

[15] To see that the sum is indeed direct (i.e. $\mathscr{B}_{ij} \cap \mathscr{B}_{kl} = \{0\}$ for $(i,j) \neq (k,l)$), one assumes $w_{ij} = \lambda w_{kl}$ for some $\lambda \in \mathbb{C}$ and fixed i,j,k,l, and uses the matrix units properties:

$$w_{ii} = w_{ij}w_{ji} = w_{ij}w_{ij}^* = |\lambda|^2 w_{kl}w_{kl}^* = |\lambda|^2 w_{kl}w_{lk} = |\lambda|^2 w_{kk} \implies i = k$$
$$w_{jj} = w_{ji}w_{ij} = w_{ij}^*w_{ij} = |\lambda|^2 w_{kl}^*w_{kl} = |\lambda|^2 w_{lk}w_{kl} = |\lambda|^2 w_{ll} \implies k = l$$

Remark. In the first part of the proof, instead of constructing the v_j and using them to define the w_{ij}, one could have the idea to construct the w_{ij} directly from the subsets $\mathscr{B}_{ij}$. However, if one does so, one would have to redefine the phases, because one might only find $w_{ij}w_{kl} = \delta_{jk}\alpha_{ijl}w_{il}$ for some phases $\alpha_{ijl} \in \{z \in \mathbb{C} \mid |z| = 1\}$.

With the two last results, we are ready to characterise finite dimensional $\mathcal{C}^*$-algebras up to $*$-isomorphisms.

Corollary 1.46. *Every concrete $*$-algebra $\mathscr{A}$ of operators on a finite dimensional Hilbert space is $*$-isomorphic to a direct product of full matrix algebra, i.e.*

$$\mathscr{A} \simeq \bigtimes_{j=1}^{n} \mathcal{M}_{d_j} \text{ for some } n \in \mathbb{N},\, d_j \in \mathbb{N}.$$

Proof. First, decompose $\mathscr{A}$ into the direct sum of simple ideals according to Proposition 1.43 as $\mathscr{A} = \bigoplus_{j=1}^{n} \mathscr{A}_j$. Every $\mathscr{A}_j$ is a simple $*$-algebra, hence by Proposition 1.45 there exist $*$-isomorphisms $\phi_j : \mathscr{A}_j \longrightarrow \mathcal{M}_{d_j}$ for some numbers $d_j \in \mathbb{N}$. Then, by

$$\phi : \mathscr{A} = \bigoplus_{j=1}^{n} \mathscr{A}_j \longrightarrow \bigtimes_{j=1}^{n} \mathcal{M}_{d_j}, \quad a = \sum_{j=1}^{n} a_j \longmapsto (\phi_j(a_j))_{j=1}^{n}$$

a $*$-isomorphism is given as claimed. □

Now we want to classify $*$-algebras on finite-dimensional Hilbert spaces up to unitary equivalence; thus we need a refinement for Proposition 1.45, i.e. a classification of simple algebras up to unitary equivalence. For a first step, Proposition 1.41(c) tells us that simple algebras are factors, up to reduction of the Hilbert space, cf. 1.30. So the next step is to classify factors:

Proposition 1.47. *Let $\mathfrak{A}$ be a $*$-algebra of operators on the finite-dimensional Hilbert space $\mathcal{H}$. Assume that $\mathfrak{A}$ is a factor. Then $\mathfrak{A}$ is unitarily equivalent to the $*$-algebra $\mathcal{M}_d \otimes (\mathbb{C} \cdot \mathbb{I}_\nu)$ on the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^\nu$ for some $d, \nu \in \mathbb{N}$, where $\mathbb{I}_\nu$ denotes the $\nu \times \nu$ identity matrix. In other words,*

$$(\mathfrak{A},\, \mathcal{H}) \cong \Big(\mathcal{M}_d \otimes (\mathbb{C} \cdot \mathbb{I}_\nu),\, \mathbb{C}^d \otimes \mathbb{C}^\nu\Big).$$

In particular it holds that $\dim \mathcal{H} = d \cdot \nu$ *and* $\dim \mathfrak{A} = d^2$.

Proof. By Proposition 1.45 there exists a system of matrix units $(w_{ij})_{i,j=1}^{d} \subset \mathfrak{A}$, where the $p_i := w_{ii}$ are mutually orthogonal minimal projections. To convey the idea behind the construction of the unitary that implements the claimed equivalence, we fix an orthonormal basis $(f_j)_{j=1}^{\nu}$ of the subspace $\operatorname{ran} p_1 \subseteq \mathcal{H}$, and decompose an arbitrary vector $\xi \in \mathcal{H}$ as follows:

$$\xi = \sum_{i=1}^{d} w_{ii}\xi = \sum_{i=1}^{d} w_{i1} \underbrace{w_{1i}\xi}_{\in \operatorname{ran} p_1} = \sum_{i=1}^{d} w_{i1} \sum_{j=1}^{\nu} |f_j\rangle\!\langle f_j|\, w_{1i}\xi = \sum_{i=1}^{d}\sum_{j=1}^{\nu} \langle f_j | w_{1i}\xi\rangle \cdot w_{i1} f_j.$$

Hence, the set $\mathcal{B} := \{w_{i1}f_j \mid i \in \{1, \ldots, d\},\, j \in \{1, \ldots, \nu\}\}$ spans $\mathcal{H}$. Actually, $\mathcal{B}$ is an orthonormal base, as the calculation

$$\langle w_{i1}f_j | w_{k1}f_l\rangle = \langle f_j | w_{1i}w_{k1}f_l\rangle = \delta_{ik}\,\langle f_j | w_{11}f_l\rangle = \delta_{ik}\,\langle f_j | f_l\rangle = \delta_{ik}\delta_{jl}$$

shows. Thus, we can define a unitary

$$U : \mathcal{H} \longrightarrow \mathbb{C}^d \otimes \mathbb{C}^\nu, \quad \xi \longmapsto \sum_{i=1}^{d}\sum_{j=1}^{\nu} \langle w_{i1}f_j | \xi\rangle \cdot (e_i \otimes e_j)\,,$$

which maps $w_{i1}f_j$ to $e_i \otimes e_j \in \mathbb{C}^d \otimes \mathbb{C}^\nu$. As usual, e_i denotes the i-th standard basis vector of $\mathbb{C}^d$ or $\mathbb{C}^\nu$, resp., and $E_{ij} := |e_i\rangle\!\langle e_j| \in \mathcal{M}_d$ shall denote the canonical matrix unit. It remains to show that U implements the $*$-isomorphism $\mathfrak{A} \cong \mathcal{M}_d \otimes (\mathbb{C} \cdot \mathbb{I}_\nu)$, i.e. that $U\mathfrak{A}U^{-1} = \mathcal{M}_d \otimes (\mathbb{C} \cdot \mathbb{I}_\nu)$. For $i, j, k \in \{1, \ldots, d\}$ and $l \in \{1, \ldots, \nu\}$ we calculate

$$\begin{aligned} Uw_{ij}U^{-1}(e_k \otimes e_l) &= Uw_{ij}w_{k1}f_l = \delta_{jk}Uw_{i1}f_l = \delta_{jk} \cdot (e_i \otimes e_l) \\ &= (\delta_{jk}e_i \otimes e_l) = (E_{ij}e_k \otimes e_l) = (E_{ij} \otimes \mathbb{I}_\nu)(e_k \otimes e_l). \end{aligned}$$

Thus $Uw_{ij}U^{-1} = E_{ij} \otimes \mathbb{I}_\nu \in \mathcal{M}_d \otimes (\mathbb{C} \cdot \mathbb{I}_\nu)$; and since the w_{ij} form a basis for $\mathfrak{A}$, we have $U\mathfrak{A}U^{-1} = \mathcal{M}_d \otimes (\mathbb{C} \cdot \mathbb{I}_\nu)$, as claimed. □

The last result finally leads to a complete characterisation of von $*$-algebras of operators on finite dimensional Hilbert spaces up to unitary equivalence:

Corollary 1.48. *Every $*$-algebra of operators $\mathfrak{A}$ on a finite-dimensional Hilbert space $\mathcal{H}$ is unitarily equivalent to a direct product*

$$(\mathfrak{A}, \mathcal{H}) \cong \left(\mathop{\times}_{j=1}^{n} \left(\mathcal{M}_{d_j} \otimes (\mathbb{C} \cdot \mathbb{I}_{\nu_j})\right) \times \{0\},\; \mathop{\times}_{j=1}^{n} \left(\mathbb{C}^{d_j} \otimes \mathbb{C}^{\nu_j}\right) \times \mathbb{C}^\kappa \right),$$

where the trivial algebra $\{0\}$ acts on $\mathbb{C}^\kappa$, $\mathbb{I}_\nu$ is the $\nu \times \nu$ identity matrix, $n \in \mathbb{N}$ and $d_j, \nu_j \in \mathbb{N}$. The numbers n and κ are uniquely determined by $\mathfrak{A}$ and the pairs (d_j, ν_j) are unique up to permutations. In particular, we have

$$\dim \mathcal{H} = \kappa + \sum_{j=1}^{n} d_j\nu_j \quad \textit{and} \quad \dim \mathfrak{A} = \sum_{j=1}^{n} d_j^2.$$

$\mathfrak{A}$ is non-degenerate, iff $\kappa = 0$ (viz. the last factor can be omitted); and $\mathfrak{A}$ is simple, iff $n = 1$.

Proof. As the first step, we want to get rid of the so-called null space of $\mathfrak{A}$, so we consider the reduced von Neumann algebra $\left(\mathfrak{A}^\flat, Y\right)$ (cf. Proposition 1.30) on the Hilbert subspace $Y = \operatorname{span} \mathfrak{A}\mathcal{H}$. We set $X := Y^\perp$ and $\kappa := \dim X$, and fix an orthonormal basis $(g_l)_{l=1}^{\kappa}$ of X. Then the unitary

$$U_1 : \mathcal{H} \longrightarrow Y \times \mathbb{C}^\kappa, \quad \mathcal{H} \ni \xi \longmapsto \left(\operatorname{Proj}_Y \xi,\, \sum_{l=1}^{\kappa} \langle g_l | \operatorname{Proj}_X \xi\rangle \cdot e_l \right) \in Y \times \mathbb{C}^\kappa$$

implements the unitary equivalence $(\mathfrak{A},\, \mathcal{H}) \cong \big(\mathfrak{A}^\flat \times \{0\},\, Y \times \mathbb{C}^\kappa\big)$, where $(e_l)_{l=1}^k$ denotes the canonical ONB of $\mathbb{C}^\kappa$. By construction, $\big(\mathfrak{A}^\flat,\, Y\big)$ is non-degenerate.

Secondly, we use Proposition 1.43 to decompose $\mathfrak{A}^\flat$ into simple ideals $\mathscr{A}_j \subseteq \mathfrak{A}^\flat$, i.e. $\mathfrak{A}^\flat = \bigoplus_{j=1}^n \mathscr{A}_j$. This concurrently gives another decomposition of the Hilbert space Y: recall that $1_{\mathscr{A}_j} \in \mathfrak{A}^\flat \subseteq \mathscr{L}(Y)$ are mutually orthogonal minimal projections, so the subspaces $Y_j := 1_{\mathscr{A}_j} Y$ are mutually orthogonal, and since $\mathfrak{A}^\flat$ was non-degenerate, Y is the direct sum of the Y_k. In order to "convert" the inner direct sum to an outer direct sum, we use the unitary

$$U_2 : Y \longrightarrow \bigtimes_{j=1}^n Y_k, \quad Y \ni \eta = \sum_{j=1}^n \underbrace{1_{\mathscr{A}_k}\eta}_{\in Y_k} \longmapsto (1_{\mathscr{A}_k}\eta)_{k=1}^n\,,$$

which implements the unitary equivalence $\big(\mathfrak{A}^\flat,\, Y\big) \cong \Big(\bigtimes_{j=1}^n \mathscr{A}_j^\flat,\, \bigtimes_{j=1}^n Y_j\Big)$, cf. Corollary 1.36.

Thirdly, we note that the $\mathscr{A}_j^\flat$ are simple by Proposition 1.30 and Corollary 1.42, and non-degenerate by construction. Hence they are factors by part (d) of Proposition 1.41, and we can invoke Proposition 1.47 to get unitaries

$$U_3^{(j)} : Y_j \longrightarrow \mathbb{C}^{d_j} \otimes \mathbb{C}^{\nu_j}, \quad j \in \{1, \dots, n\}$$

implementing the unitary equivalences $\Big(\mathscr{A}_j^\flat,\, Y_j\Big) \cong \big(\mathcal{M}_{d_j} \otimes (\mathbb{C} \cdot \mathbb{I}_{\nu_j}),\ \mathbb{C}^{d_j} \otimes \mathbb{C}^{\nu_j}\big)$.

Putting all together, we define the unitary $U : \mathcal{H} \longrightarrow \bigtimes_{j=1}^n \big(\mathbb{C}^{d_j} \otimes \mathbb{C}^{\nu_j}\big) \times \mathbb{C}^\kappa$ by the following commutative diagram:

$$\begin{tikzcd}
\mathcal{H} \arrow[r, bend left, "U_1"] \arrow[rrr, bend right, "U"'] & Y \times \mathbb{C}^\kappa \arrow[r, bend left, "(U_2,\, \mathrm{id}_{\mathbb{C}^\kappa})"] & \bigtimes_{j=1}^n Y_j \times \mathbb{C}^\kappa \arrow[r, bend left, "\big((U_3^{(j)})_{j=1}^n,\, \mathrm{id}_{\mathbb{C}^\kappa}\big)"] & \bigtimes_{j=1}^n \big(\mathbb{C}^{d_j} \otimes \mathbb{C}^{\nu_j}\big) \times \mathbb{C}^\kappa
\end{tikzcd}$$

Thus the stated unitary equivalence is proven. It remains to show that the numbers κ, n and the d_j and ν_j are uniquely determined by $\mathfrak{A}$. But by construction we know $\kappa = \dim\big(\bigcap_{A\in\mathfrak{A}} \ker A\big)$, which is preserved under unitary equivalences, as for $\mathfrak{B} \cong \mathfrak{A}$, say $\mathfrak{B} = V\mathfrak{A}V^*$ for some unitary V, we have

$$\begin{aligned}
\tilde{\kappa} := \dim\left(\bigcap_{B\in\mathfrak{B}} \ker B\right) &= \dim\left(\bigcap_{A\in\mathfrak{A}} \ker\,(VAV^*)\right) \\
&= \dim\left(\bigcap_{A\in\mathfrak{A}} \ker\,(AV^*)\right) = \dim\left(\bigcap_{A\in\mathfrak{A}} V\,(\ker A)\right) \\
&= \dim\left(V\left(\bigcap_{A\in\mathfrak{A}} \ker A\right)\right) = \dim\left(\bigcap_{A\in\mathfrak{A}} \ker A\right) = \kappa.
\end{aligned}$$

Furthermore, n is the number of simple ideals $\mathcal{I}_j$ contained in $\mathfrak{A}$, which is preserved under $*$-isomorphisms, thus in particular by unitary equivalences. Finally, the d_j and ν_j are – up to permutation, of course – determined by (cf. Proposition 1.47)

$$d_j^2 = \dim \mathcal{I}_j \quad \text{and} \quad d_j \cdot \nu_j = \dim \operatorname{span}(\mathcal{I}_j \mathcal{H}),$$

which for similar reasons are stable under unitary equivalences. □

1.7. n-positivity and complete positivity

For linear maps between $\mathcal{C}^*$-algebras to be quantum operations, one does not only demand that they are positive; in order to ensure that compound (i.e., "tensor-ed") operations on compound quantum systems are positive as well, one must demand a stronger property, namely complete positivity.

Definition 1.49. Let $\mathscr{A}$ and $\mathscr{B}$ be $\mathcal{C}^*$-Algebras and $\mathcal{S} \subset \mathscr{A}$ an operator system. A linear map $T : \mathcal{S} \longrightarrow \mathscr{B}$ is called *n-positive* ($n \in \mathbb{N}$), if the induced map

$$\phi^{(n)} := \phi \otimes \mathrm{id}_{\mathcal{M}_n} : \mathcal{S} \otimes \mathcal{M}_n \longrightarrow \mathscr{B} \otimes \mathcal{M}_n \tag{1.7.1}$$

is positive. If T is n-positive for all $n \in \mathbb{N}$, then T is called *completely positive* (abbreviated as *c.p.*), which for the sake of standardisation in the notation we may also call *∞-positive.*

If $T : \mathscr{A} \longrightarrow \mathscr{B}$ is linear and satisfies the *Schwarz inequality*

$$\forall A \in \mathscr{A} : \quad T(a)^* T(a) \leq T(a^* a),$$

then T is called *Schwarz map*, or *$3/2$-positive.*

Obviously one can replace the space $\mathcal{M}_n$ in 1.7.1 by $\mathscr{L}(\mathcal{H})$ for any n-dimensional Hilbert space $\mathcal{H}$. Note that the three properties 1-positive, positivity-preserving and positive (in the sense of mappings from operators to operators) are identical.

Note 1.50 (cf. [Pau, Ch. 3]). As the naming already suggests, n-positivity implies m-positivity for $n \geq m$ ($n, m \in \mathbb{N}$). Schwarz maps are 1-positive, and unital (!) 2-positive maps, that are defined on a $\mathcal{C}^*$-algebra, are Schwarz maps.

Furthermore, the concatenation and convex combination of finitely many m-positive maps ($m \in \{1, 3/2, 2, 3, 4, \dots\}$) are again m-positive; and the tensor product of completely positive maps is completely positive, if the underlying Hilbert spaces are finite-dimensional. Finally, a linear map $T : \mathcal{S} \longrightarrow \bigoplus_{j=1}^n \mathscr{A}_j$, which maps into a direct sum of ideals $\mathscr{A}_j$, is m-positive ($m \in \{1, 3/2, 2, 3, 4, \dots\}$), iff all the "coordinate maps" $\pi_j \circ T : \mathcal{S} \longrightarrow \mathscr{A}_j$ are.

Proof. For $n, m \in \mathbb{N}$, the first assertion follows directly via the canonical embedding

$$\mathcal{M}_m \hookrightarrow \mathcal{M}_n, \quad a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

The Schwarz property implies positivity, since $T(a^*a) \geq T(a)^*T(a) \geq 0$ for all $a \in \mathscr{A}$.

Now, suppose that $T : \mathscr{A} \longrightarrow \mathscr{B}$ is unital and satisfies the Schwarz inequality. For $a \in \mathscr{A}$ we have that

$$\begin{pmatrix} a & 1_{\mathscr{A}} \\ 0 & 0 \end{pmatrix}^* \begin{pmatrix} a & 1_{\mathscr{A}} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a^* & 0 \\ 1_{\mathscr{A}} & 0 \end{pmatrix} \begin{pmatrix} a & 1_{\mathscr{A}} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a^*a & a^* \\ a & 1_{\mathscr{A}} \end{pmatrix}$$

is a positive element of $\mathscr{A} \otimes \mathcal{M}_2$. Since T is 2-positive, also

$$T^{(2)} \begin{pmatrix} a^*a & a^* \\ a & 1_{\mathscr{A}} \end{pmatrix} = \begin{pmatrix} T(a^*a) & T(a)^* \\ T(a) & 1_{\mathscr{B}} \end{pmatrix}$$

is positive. Hence, for all ξ and η in the underlying Hilbert space we have

$$\begin{aligned} 0 \quad &\leq \quad \left\langle \begin{pmatrix} \xi \\ \eta \end{pmatrix} \middle| \begin{pmatrix} T(a^*a) & T(a^*) \\ T(a) & 1_{\mathscr{B}} \end{pmatrix} \middle| \begin{pmatrix} \xi \\ \eta \end{pmatrix} \right\rangle \\ &= \quad \langle \xi | T(a^*a) | \xi \rangle + \langle \xi | T(a)^* | \eta \rangle + \langle \eta | T(a) | \xi \rangle + \underbrace{\langle \eta | 1_{\mathscr{B}} | \eta \rangle}_{\leq \|\eta\|^2} \\ &\leq \quad \langle \xi | T(a^*a) | \xi \rangle + 2 \operatorname{Re} \langle \xi | T(a)^* | \eta \rangle + \langle \eta | \eta \rangle , \end{aligned}$$

and by plugging in $\eta := -T(a)\xi$ it follows that

$$\begin{aligned} 0 \quad &\leq \quad \langle \xi | T(a^*a) | \xi \rangle - 2 \operatorname{Re} \underbrace{\langle \xi | T(a)^* T(a) | \xi \rangle}_{\in \mathbb{R}, \text{ since } T(a)^*T(a) \geq 0} + \langle \xi | T(a)^* T(a) | \xi \rangle \\ &= \quad \langle \xi | (T(a^*a) - T(a)^* T(a)) | \xi \rangle . \end{aligned}$$

Since ξ was arbitrary, $T(a^*a) \geq T(a)^*T(a)$.

Now, if T and S are two concatenable m-positive maps ($m \in \mathbb{N}$), then

$$(T \circ S)^{(m)} = (T \circ S) \otimes \mathrm{id}_{\mathcal{M}_m} = (T \otimes \mathrm{id}_{\mathcal{M}_m}) \circ (S \otimes \mathrm{id}_{\mathcal{M}_m}) = T^{(m)} \circ S^{(m)}$$

shows, that also $T \circ S$ is also m-positive. For convex combinations, m-positivity is also quite obvious:

$$(\lambda T + (1-\lambda)S)^{(m)} = (\lambda T + (1-\lambda)S) \otimes \mathrm{id}_{\mathcal{M}_m} = \lambda T^{(m)} + (1-\lambda)S^{(m)}.$$

If T and S are merely Schwarz maps, then we can use positivity of T to apply it to the Schwarz inequality for S, before utilising the Schwarz inequality for T:

$$(T \circ S)(a^*a) = T\left(S(a^*a)\right) \geq T(S(a)^*S(a)) \geq T(S(a))^*T(S(a)),$$

which is the Schwarz inequality for $T \circ S$. The Schwarz inequality for convex combinations of Schwarz maps can be shown as follows: Let $0 \leq \lambda \leq 1$ and consider $R := \lambda T + (1-\lambda)S$ for two Schwarz maps T and S. Then, denoting $t = T(a)$ and $s = S(a)$, we can estimate

$$R(a)^*R(a) = \lambda^2\, t^*t + (1-\lambda)^2\, s^*s + \lambda(1-\lambda)\left[t^*s + s^*t\right]$$

For the term in square brackets, we use $0 \leq (t-s)^* (t-s) = t^*t + s^*s - [t^*s + s^*t]$ and get

$$\begin{aligned} R(a)^*R(a) &\leq \left(\lambda^2 + \lambda(1-\lambda)\right) t^*t + \Big((1-\lambda)^2 + \lambda(1-\lambda)\Big) s^*s \\ &= \lambda\, t^*t + (1-\lambda)\, s^*s \;\leq\; \lambda\, T(a^*a) + (1-\lambda)\, S(a^*a) \\ &= R(a^*a). \end{aligned}$$

For complete positivity of tensor products of c.p. maps, assume that $\mathscr{A}_j \subseteq \mathcal{M}_{d_j}$, $\mathscr{B}_j \subseteq \mathcal{M}_{e_j}$ are concrete $*$-algebras, $\mathcal{S}_j \subseteq \mathscr{A}_j$ are operator system, and let $T_j : \mathcal{S}_j \longrightarrow \mathscr{B}_j$ be completely positive maps ($j \in \{1,2\}$). Fix $n \in \mathbb{N}$ and denote by V and W the maps – defined on the appropriate spaces[16] – which exchange the first two tensor factors in a threefold tensor product. Then

$$\begin{aligned} (T_1 \otimes T_2)^{(n)} &= T_1 \otimes T_2 \otimes \mathrm{id}_{\mathcal{M}_n} = (T_1 \otimes \mathrm{id}_{\mathscr{B}_2} \otimes \mathrm{id}_{\mathcal{M}_n}) \circ (\mathrm{id}_{\mathcal{S}_1} \otimes T_2 \otimes \mathrm{id}_{\mathcal{M}_n}) \\ &= (T_1 \otimes \mathrm{id}_{\mathscr{B}_2} \otimes \mathrm{id}_{\mathcal{M}_n}) \circ W \circ (T_2 \otimes \mathrm{id}_{\mathcal{S}_1} \otimes \mathrm{id}_{\mathcal{M}_n}) \circ V \\ &= (T_1 \otimes \mathrm{id}_{\mathcal{M}_{e_2}} \otimes \mathrm{id}_{\mathcal{M}_n}) \circ W \circ (T_2 \otimes \mathrm{id}_{\mathcal{M}_{d_1}} \otimes \mathrm{id}_{\mathcal{M}_n}) \circ V \\ &= (T_1 \otimes \mathrm{id}_{\mathcal{M}_{e_2+n}}) \circ W \circ (T_2 \otimes \mathrm{id}_{\mathcal{M}_{d_1+n}}) \circ V. \end{aligned}$$

The last line is a concatenation of positive maps, hence $(T_1 \otimes T_2)^{(n)}$ is positive.

Finally, let $T : \mathcal{S} \longrightarrow \mathscr{B}$ be a linear map, where $\mathscr{A} = \bigoplus_{j=1}^m \mathscr{B}_j$, and let $\pi_j : \mathscr{B} \longrightarrow \mathscr{B}_j$ denote the projection onto the j-th factor. Recall that π_j is a $*$-homomorphism by Proposition 1.35, and that $\sum_{j=1}^m \pi_j = \mathrm{id}_{\mathscr{B}}$. Let $n \in \mathbb{N}$. Then the last assertion follows from

$$\begin{aligned} T \text{ is } n\text{-positive} &\iff T \otimes \mathrm{id}_{\mathcal{M}_n} \text{ is positive} \\ &\implies ((\pi_j \circ T) \otimes \mathrm{id}_{\mathcal{M}_n}) = (\pi_j \otimes \mathrm{id}_{\mathcal{M}_n}) \circ (T \otimes \mathrm{id}_{\mathcal{M}_n}) \text{ is positive } \forall j \\ &\iff (\pi_j \circ T) \text{ is } n\text{-positive } \forall j \\ &\implies \sum_{j=1}^m (\pi_j \circ T) = (\mathrm{id}_{\mathscr{B}} \circ T) = T \text{ is } n\text{-positive.} \end{aligned}$$

$\square$

We already saw (cf. note 1.26), that $*$-homomorphisms are automatically positive. In fact, they are an example of completely positive maps, as the next lemma shows.

Lemma 1.51. *Every $*$-homomorphism between $\mathcal{C}^*$-algebras is completely positive.*

[16] More precisely,

$$\begin{aligned} V: &\quad \mathcal{S}_1 \otimes \mathcal{S}_2 \otimes \mathcal{M}_n \longrightarrow \mathcal{S}_2 \otimes \mathcal{S}_1 \otimes \mathcal{M}_n, \quad s \otimes t \otimes m \longmapsto t \otimes s \otimes m \\ W: &\quad \mathscr{B}_2 \otimes \mathcal{S}_1 \otimes \mathcal{M}_n \longrightarrow \mathcal{S}_1 \otimes \mathscr{B}_2 \otimes \mathcal{M}_n, \quad b \otimes s \otimes m \longmapsto s \otimes b \otimes m. \end{aligned}$$

It can easily be seen that V and W are (restrictions of) unitarily implemented $*$-isomorphisms, thus in particular positivity-preserving by Note 1.26.

Proof. Let $\phi : \mathscr{A} \longrightarrow \mathscr{B}$ be a $*$-homomorphism between $\mathcal{C}^*$-algebras, and let $n \in \mathbb{N}$. We show, that the map

$$\phi^{(n)} := \phi \otimes \mathrm{id}_{\mathcal{M}_n} : \mathscr{A} \otimes \mathcal{M}_n \longrightarrow \mathscr{B} \otimes \mathcal{M}_n.$$

is again a $*$-homomorphism, hence positive by note 1.26. For $(X_{ij}), (Y_{ij}) \in \mathrm{Mat}_n(\mathscr{A})$ we have

$$\begin{aligned}
\phi^{(n)}(X \cdot Y) &= \phi^{(n)} \left(\sum_{k=1}^{n} X_{ik} Y_{kj} \right)_{ij} = \left(\sum_{k=1}^{n} \phi(X_{ik} Y_{kj}) \right)_{ij} \\
&= \left(\sum_{k=1}^{n} \phi(X_{ik}) \phi(Y_{kj}) \right)_{ij} (\phi(X_{ij}))_{ij} \cdot (\phi(Y_{ij}))_{ij} = \phi^{(n)}(X) \cdot \phi^{(n)}(Y);
\end{aligned}$$

hence $\phi^{(n)}$ is multiplicative. Involutivity follows by

$$\phi^{(n)} \left(X_{ij}\right)_{ij}^* = \left(\phi(X_{ij})\right)_{ij}^* = \left(\phi(X_{ji})^*\right)_{ij} = \left(\phi(X_{ji}^*)\right)_{ij} = \phi^{(n)} \left(X_{ji}^*\right)_{ji} = \phi^{(n)} \left(X_{ij}\right)_{ij}^* .$$

$\square$

For the case, where the domain is just $\mathbb{C}$, positivity and complete positivity are the same, as the next lemma shows. We will later generalise this statement for commutative domains and ranges (Corollary 2.9).

Lemma 1.52. *Let $\mathscr{A}$ be a concrete $\mathcal{C}^*$-algebra, $\mathcal{S} \subseteq \mathscr{A}$ an operator system. Then every positive linear functional $\phi : \mathcal{S} \longrightarrow \mathbb{C}$ is actually completely positive.*

Proof. We have to show that $\phi^{(n)} : \mathcal{S} \otimes \mathcal{M}_n \longrightarrow \mathbb{C} \otimes \mathcal{M}_n$ is positive, so let $A \in \mathcal{S} \otimes \mathcal{M}_n$ be a positive element, say $A = \sum_{k=1}^{m} a_k \otimes m_k$ with $a_k \in \mathcal{S}$ and $m_k \in \mathcal{M}_n$. We have to show that $\phi^{(n)}(A)$ is a positive semidefinite matrix[17], so we calculate for $x \in \mathbb{C}^n$ (where the index and bounds of summation are omitted for better readability):

$$\begin{aligned}
\left\langle x \middle| \phi^{(n)}(A) \middle| x \right\rangle &= \left\langle x \middle| (\phi \otimes \mathrm{id}_{\mathcal{M}_n}) \left(\sum a_k \otimes m_k \right) \middle| x \right\rangle = \left\langle x \middle| \left(\sum \phi(a_k) \cdot m_k \right) \middle| x \right\rangle \\
&= \sum \phi(a_k) \cdot \langle x | m_k | x \rangle = \phi \left(\sum a_k \otimes \langle x | m_k | x \rangle \right) \\
&= \phi \left(\sum \big(\mathrm{id}_{\mathcal{H}} \otimes \langle x|\big) \big(a_k \otimes m_k\big) \big(\mathrm{id}_{\mathcal{H}} \otimes |x\rangle\big) \right) \\
&= \phi\Big(\big(\mathrm{id}_{\mathcal{H}} \otimes \langle x|\big) \underbrace{\left(\sum a_k \otimes m_k \right)}_{=A} \underbrace{\big(\mathrm{id}_{\mathcal{H}} \otimes |x\rangle\big)}_{=:V_x} \Big) = \phi\big(\underbrace{V_x^* A V_x}_{\geq 0} \big) \geq 0.
\end{aligned}$$

In the last line we have introduced the linear operator[18] $V_x = \mathrm{id}_{\mathcal{H}} \otimes |x\rangle : \mathcal{H} \doteq \mathcal{H} \otimes \mathbb{C} \longrightarrow \mathcal{H} \otimes \mathbb{C}^n$ and used the positivity of ϕ. $\square$

[17]Note that for any $\mathbb{C}$-vector space W, $\mathbb{C} \otimes W$ is canonically isomorphic to W via $z \otimes w \mapsto z \cdot w$; we will use this identification in the proof, using the symbol "$\doteq$" as in $\mathbb{C} \otimes \mathcal{M}_n \doteq \mathcal{M}_n$.

[18]Speaking strictly, writing $V_x = \mathrm{id}_{\mathcal{H}} \otimes |x\rangle$ is a bit abuse of notation: here, "$|x\rangle$" stands actually for the linear map $|x\rangle : \mathbb{C} \longrightarrow \mathcal{H},\ z \mapsto z \cdot x$, just as $\langle x| = \big(|x\rangle\big)^*$ stands for the linear functional $\langle x| : \mathcal{H} \longrightarrow \mathbb{C},\ \xi \mapsto \langle x|\xi\rangle$.

In later applications, we want to extend completely positive maps, that are defined only on an operator system, to the whole $\mathcal{C}^*$-algebra. For this case, Arveson proved in [Arv1] the following extension theorem (see also [Pau]):

Theorem 1.53. *Let $\mathscr{A}$ be a $\mathcal{C}^*$-Algebra, $\mathcal{S} \subseteq \mathscr{A}$ an operator system, and $\mathcal{H}$ a Hilbert space. Then every completely positive map $\phi : \mathcal{S} \longrightarrow \mathscr{L}(\mathcal{H})$ can be extended to a completely positive map $\tilde{\phi} : \mathscr{A} \longrightarrow \mathscr{L}(\mathcal{H})$.*

Remark 1.54. In theorem 1.53, the $\mathcal{C}^*$-algebra $\mathscr{L}(\mathcal{H})$ that ϕ maps into can in general not be replaced by an arbitrary $\mathcal{C}^*$-algebra.

1.8. Support Projections

This section defines support projections and states their most important properties. The presentation is mostly taken from [Dix].

Proposition 1.55. *Let $\mathfrak{A}$ be a concrete $\mathcal{C}^*$-algebra on a finite-dimensional Hilbert space $\mathcal{H}$ and $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ a unital Schwarz map. Then there exists a projection $P \in \mathfrak{A}$ – called the* support projection *of ψ – satisfying the following conditions:*

a) For $X \in \mathfrak{A}$ we have $\psi(X) = \psi(PX) = \psi(XP) = \psi(PXP)$.

b) For positive $H \in \mathfrak{A}$, the equivalence $\psi(H) = 0 \Leftrightarrow PHP = 0$ holds.

Proof. We set $\mathfrak{M} := \{T \in \mathfrak{A} \mid \psi(T^*T) = 0\}$. We claim that $\mathfrak{M}$ can also be written as $\mathfrak{M} = \{T \in \mathfrak{A} \mid \forall S \in \mathfrak{A} : \ \psi(S^*T) = 0\}$. Indeed, „$\supseteq$“ follows by plugging in $S = T$, and „$\subseteq$“ follows via the Schwarz inequality, proposition 1.10vii), and positivity of ψ:

$$
\begin{aligned}
& 0 \leq \psi(S^*T)^*\psi(S^*T) \leq \psi(\underbrace{T^*SS^*T}_{\leq \|S\|^2 T^*T}) \leq \|S^*\|^2\,\psi(T^*T) = 0 \\
\Longrightarrow\quad & \psi(S^*T)^*\psi(S^*T) = 0 \\
\Longrightarrow\quad & \psi(S^*T) = 0.
\end{aligned}
$$

In particular, $\mathfrak{M}$ is a left ideal in $\mathfrak{A}$, and by proposition 1.18 there exists a projection $E \in \mathfrak{A}$, such that $\mathfrak{M} = \{T \in \mathfrak{A} \mid T = TE\}$. Obviously $E \in \mathfrak{M}$, hence $\psi(SE) = 0$ for all $S \in \mathfrak{A}$. Furthermore, if we replace S by S^*, we get $0 = 0^* = \psi(S^*E)^* = \psi(ES)$ for all $S \in \mathfrak{A}$, where the last equality is by lemma 1.12. The projection $P := 1_{\mathfrak{A}} - E$ then satisfies part (a).

As to part (b), we note that for a positive element $H = X^*X \in \mathfrak{A}$ we have the equivalence chain

$$
\psi(H) = 0 \Longleftrightarrow X \in \mathfrak{M} \Longleftrightarrow XE = X \Longleftrightarrow XP = 0 \Longleftrightarrow 0 = (XP)^*XP = PHP.
$$

□

The following proposition constitutes the crucial step, when we later classify the possible fixed points sets of Schwarz maps and, in particular, of quantum channels. Part (a) is [Arv2, Lemma 1 on p. 286].

Proposition 1.56. *Let $\mathfrak{A}$ be a concrete $\mathcal{C}^*$-algebra on the finite-dimensional Hilbert space $\mathcal{H}$, and let $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ be an idempotent Schwarz map and P the support projection of ψ. Then, if we denote the fixed point set of ψ by $\operatorname{fix}\psi$, we have:*

a) *P commutes with all fixed points of ψ, i.e. $P \in (\operatorname{fix}\psi)'$.*

b) *If $P = 1_{\mathfrak{A}}$, then $\operatorname{fix}\psi$ is a $*$-algebra.*

Note that $P = 1_{\mathfrak{A}}$ is automatically fulfilled, if ψ is faithful (i.e. $A \neq 0 \wedge A \geq 0 \implies \psi(A) \neq 0$), since $\psi(1_{\mathfrak{A}}) = \psi(P)$ by the properties of support projections.

Proof. a) Let $X \in \mathfrak{A}$ be a fixed point of ψ. Part (vi) of proposition 1.10 and the Schwarz inequality imply

$$X^*PX \leq X^*X = \psi(X)^*\psi(X) = \psi(PX)^*\psi(PX) \leq \psi(X^*PX),$$

hence sandwiching with P from both sides (using again Part (vi) of proposition 1.10) yields

$$PX^*PXP \leq PX^*XP \leq P\psi(X^*PX)P.$$

Thus, $H := P\psi(X^*PX)P - PX^*PXP = P\left(\psi(X^*PX) - X^*PX\right)P$ is positive with $\psi(H) = 0$ by idempotence of ψ. Since P is the support projection of ψ, by part (b) of proposition 1.55 it follows that $0 = PHP = H$. Thus, in the above inequality chain we have actually equality, and in particular $PX^*PXP = PX^*XP$. Putting all terms onto the r.h.s., we get $0 = PX^*(1-P)XP = PX^*(1-P)^2XP = K^*K$, where $K := (1-P)XP$. But $K^*K = 0$ implies $K = 0$, hence $XP = PXP$ holds for all fixed points X. Since the set of fixed points is self-adjoint by lemma 1.12, X^* is a fixed point too, which implies

$$XP = PXP = (PX^*P)^* = (X^*P)^* = PX,$$

i.e. P commutes with X.

b) Suppose that $P = 1_{\mathfrak{A}}$. Since $\operatorname{fix}\psi$ is an operator system, by the polarisation identity

$$A^*B = \frac{1}{4}\sum_{k=0}^{3} \mathrm{i}^{-k}(A + \mathrm{i}^k B)^*(A + \mathrm{i}^k B) \quad \text{for } A, B \in \mathfrak{A}$$

it suffices to show, that $X \in \operatorname{fix}\psi$ implies $X^*X \in \operatorname{fix}\psi$. For $X \in \operatorname{fix}\psi$, the Schwarz inequality implies $X^*X = \psi(X)^*\psi(X) \leq \psi(X^*X)$. Hence $H := \psi(X^*X) - X^*X$ is positive with $\psi(H) = 0$. Again, it follows that $0 = PHP = H$, hence $\psi(X^*X) = X^*X$. □

Chapter 2.

Quantum Information Theory

2.1. Basic notions

In this chapter, we review the basic notions from quantum information. We do not want to review the whole physical-philosophical theory of how actual quantum-physical systems may be described mathematically in general and the various interpretations of quantum theory. Instead, we restrict ourselves to stating the fundamental assumptions we make in the descriptions of physical systems in terms of *states, effects, observables,* and *operations* (also called *channels*). What follows, is basically the mathematical essence of §1 in [Kra]; readers interested in the motivations of the definitions and axioms, as well as the technical details may read further in [Lud, Kra].

2.1.1. States and Effects

The general structure the authors in [Lud, Kra] start with, when they want to describe physical systems, is that of a statistical model:

Definition 2.1. A *statistical model* for a physical system consists of the following:

i) The set of *states* $\mathscr{S}$, that the system can be prepared in.

ii) The set of *effects* $\mathscr{E}$, representing physical measurements on the system with exactly two possible outcomes – "yes" and "no", or equivalently 1 or 0.

   There are always two special effects: the effect $1 \in \mathscr{E}$, which results always in the outcome "yes", and the effect $0 \in \mathscr{E}$, which never occurs, regardless of the state of the system being measured on.

iii) A mapping $\mu : \mathscr{S} \times \mathscr{E} \longrightarrow [0, 1]$, which assigns to a pair $(S, E) \in \mathscr{S} \times \mathscr{E}$ the probability[1] of a "yes"-outcomes, if the effect E is measured on a system prepared in the state S. For the special effects 0 and 1 we have obviously

[1] Here we mean "probability" in the statistical sense, i.e. if we prepare a number N of systems in the state S, measure E on all N systems, getting N_1 times the outcome "yes", and N_0 times the outcome "no", then for large N we have $\mu(S, E) \approx N_1/N$. Note that the outcome of a single measurement may not be determined by specifying S and E, but may be inherently random.

$\mu(S,1) = 1$ and $\mu(S,0) = 0$ for all states S.

$$\mu(S,E) = \mu(\tilde{S},E)\ \forall E \in \mathscr{E} \implies S = \tilde{S},$$
$$\mu(S,E) = \mu(S,\tilde{E})\ \forall S \in \mathscr{S} \implies E = \tilde{E}.$$

Both $\mathscr{S}$ and $\mathscr{E}$ carry the structure of a convex set, where a convex combination $\lambda S_1 + (1-\lambda S_2)$ of to states S_1 and S_2 shall describe a system, which is prepared in S_1 or S_2 with probability λ or $(1-\lambda)$, respectively; the convex combination $\lambda E_1 + (1-\lambda)E_2$ of two effects E_1 and E_2 shall correspond of randomly measuring E_1 (with probability λ) or E_2 (with probability $(1-\lambda)$). This interpretation demands, that μ shall behave well under convex combinations, i.e.

$$\mu\left(\lambda S_1 + (1-\lambda)S_2,\, E\right) = \lambda\, \mu(S_1,E) + (1-\lambda)\, \mu(S_2,E)$$

and

$$\mu\left(S,\, \lambda E_1 + (1-\lambda)E_2\right) = \lambda\, \mu(S,E_1) + (1-\lambda)\, \mu(S,E_2)$$

for $S, S_1, S_2 \in \mathscr{S}$ and $E, E_1, E_2 \in \mathscr{E}$. This is equivalent to saying that μ is an *affine map*.

Remark 2.2. There is an alternative viewpoint in that we consider the states as directly operating on the effects; indeed the probability map μ furnishes an embedding $\mathscr{S} \hookrightarrow \mathscr{E}^*$, where $\mathscr{E}^*$ denotes the set of affine maps $E : \mathscr{S} \longrightarrow [0,\, 1]$, given by $E(S) := \mu(S,E)$ for $E \in \mathscr{E}$, $S \in \mathscr{S}$.

For the cases we want to consider, i.e. classical probability and quantum mechanical systems, it turns out, that we do not need the full generality of statistical models. Instead we will be content of the special case where $\mathscr{E}$ is a subset of the algebra $\mathscr{L}(\mathcal{H})$ of bounded linear operators in a complex Hilbert space $\mathcal{H}$. In such a representation, $\mathscr{S}$ and $\mathscr{E}$ are given as follows:

- $\mathscr{E}$ is given by a convex subset of self-adjoint operators in $\mathcal{H}$ between 0 and 1, i.e. $\mathscr{E} = \{E \in \mathscr{L}(\mathcal{H}) \mid 0 \leq E \leq \mathrm{id}_{\mathcal{H}}\}$, with $\mathrm{id}_{\mathcal{H}} \in \mathscr{E}$.
- In the spirit of 2.2, $\mathscr{S}$ is given by a subset of $\{S : \mathscr{E} \longrightarrow [0,\, 1] \mid S \text{ affine}\}$.

Each state $S \in \mathscr{S}$ can be uniquely extended to a complex-linear map $\hat{S} : \mathscr{A} \longrightarrow \mathbb{C}$, where $\mathscr{A} \subseteq \mathscr{L}(\mathcal{H})$ is the $\mathcal{C}^*$-algebra generated by $\mathscr{E}$.[2] Moreover, $\mathscr{E}$ can be reconstructed from $\mathscr{A}$ as $\mathscr{E} = \mathscr{E}(\mathscr{A}) := \{E \in \mathscr{A} \mid 0 \leq E \leq \mathrm{id}_{\mathcal{H}}\}$. Thus we can embed the set of states into the dual $\mathscr{A}^*$ of $\mathscr{A}$.

[2]This can also be seen as a consequence of Proposition 1.10, according to which the set of effects spans the whole algebra linearly: each $x \in \mathscr{A}$ can decomposed as linear combination of at most 4 positive elements

$$x = \sum_{k=0}^{3} \mathrm{i}^k x_k = \sum_{k=0}^{3} \mathrm{i}^k \left\|x_k\right\| \cdot y_k,$$

where $y_k = x_k / \left\|x_k\right\|$ if $x_k \neq 0$ and $y_k = 0$ otherwise, so in both cases $y_k \in \mathscr{E}(\mathscr{A})$.

Note that $\mathscr{S}$ may be only a *subset* of the affine maps from $\mathscr{E}$ into [0, 1], because usually one will demand some kind of continuity of the elements of $\mathscr{S}$, e.g. uniform or ultraweak continuity. We do not wish to dive into the topological restrictions which can be demanded of states; instead, we limit ourselves to the case of finite-dimensional Hilbert spaces $\mathcal{H}$. In this case we can equip $\mathscr{L}(\mathcal{H})$ with the Hilbert-Schmidt scalar product (i.e. $(A, B) \mapsto \operatorname{tr}(A^\dagger B)$), $\mathscr{A}$ becomes (as a closed linear subspace) a Hilbert space on its own; so by the Riesz representation theorem, each state s may be written as $s(A) = \operatorname{tr}(\rho A)$ for a unique $\rho \in \mathscr{A}$. The element ρ is called *density matrix*. The requirements of s for being a state translate to the demand that ρ is positive and has trace equal to 1.

Remark. One need not postulate the existence of an underlying Hilbert space as a fundamental entity describing a quantum system. Many authors instead regard the effects as more fundamental and postulate a representation on some Hilbert space, which is always possible by the GNS-construction.

2.1.2. Examples

We show that the $\mathcal{C}^*$-algebra model can describe classical probability as well as quantum mechanics.

Example 2.3 (Classical Probability)**.** Consider $\mathcal{H} = \mathbb{C}^N$ for a classical system with N possible states (think for example of tossing a coin ($N = 2$) or rolling a dice ($N = 6$)). We define

$$\mathscr{A} := \mathcal{D}_N := \{\operatorname{diag}(\lambda_1, \dots, \lambda_N) \mid \lambda_j \in \mathbb{C}\ \forall j \in \{1, \dots, N\}\} \subseteq \mathscr{L}(\mathcal{H})$$

as the abelian $*$-algebra consisting of diagonal $N \times N$-matrices. Note that for $A = \operatorname{diag}(a_1, \dots, a_N) \in \mathcal{D}_N$ and $B = \operatorname{diag}(b_1, \dots, b_N) \in \mathcal{D}_N$, it holds that

$$\begin{aligned} A \geq 0 \quad &\Longleftrightarrow \quad a_j \geq 0 \quad \forall j \in \{1, \dots, N\} \text{ and} \\ A \geq B \quad &\Longleftrightarrow \quad a_j, b_j \in \mathbb{R} \ \wedge \ a_j \geq b_j \quad \forall j \in \{1, \dots, N\}. \end{aligned}$$

Then, the effect space is $\mathscr{E} = \{E \in \mathcal{D}_N \mid 0 \leq E \leq \mathbb{I}_N\}$ and the state space is $\mathscr{S} = \{\operatorname{tr}(\sigma\,(\cdot)) \mid \sigma \in \mathcal{D}_N,\, \sigma \geq 0,\, \operatorname{tr}\sigma = 1\}$. For $(\operatorname{tr}(\sigma(\cdot)) \in \mathscr{S}$, $\sigma = \operatorname{diag}(\sigma_1, \dots, \sigma_N)$, the numbers σ_j are the probabilities for the respective *elementary outcome* j (i.e. $\sigma_1 = \sigma_2 = 1/2$ for throwing a fair coin, $\sigma_1 = \dots = \sigma_6 = 1/6$ for throwing a fair dice), whereas for $E = \operatorname{diag}(\epsilon_1, \dots, \epsilon_N) \in \mathscr{E}$, the numbers ϵ_j stand for the probability of triggering a "yes"-outcome given the elementary outcome j.

Remark. More generally, one can treat continuous probability distributions by considering a locally compact measure space (X, μ) and setting $\mathcal{H} := L^2(X, \mu)$ and $\mathscr{A} := \{M_f \mid f \in \mathcal{C}_\mathrm{b}(X)\}$, where $\mathcal{C}_\mathrm{b}(X)$ denotes the set of bounded continuous functions $X \longrightarrow \mathbb{C}$, and $M_f : L^2(X, \mu) \longrightarrow L^2(X, \mu)$ acts as multiplication by $f \in \mathcal{C}_\mathrm{b}(X)$. The case of finitely many elementary states is contained therein with the choice $X = \{1, \dots, N\}$ and choosing μ as the counting measure.

Example 2.4 (Quantum Mechanics)**.** A k-state quantum system (e.g. a spin-s-particle with $k = 2s + 1$ having no other degrees of freedom) can be modelled by the Hilbert space $\mathcal{H} = \mathbb{C}^k$, where the effects are $\mathscr{E} = \{E \in \mathscr{L}(\mathcal{H}) \mid 0 \leq E \leq \mathrm{id}_{\mathcal{H}}\}$ and the state space is $\mathscr{S} = \{\mathrm{tr}(\rho\,(\cdot)) \mid \rho \in \mathscr{L}(\mathcal{H}),\, \rho \geq 0,\, \mathrm{tr}\rho = 1\}$. The matrices ρ are called *density matrices*. We may sometimes identify the linear map $\mathrm{tr}(\rho\,(\cdot))$ with the density matrix ρ in situations where it causes no confusion. In the beginning of learning Quantum Mechanics, quantum states are typically described by normalised vectors of the Hilbert space – up to a phase factor of modulus 1. This view can be embedded in our definition, when we regard the state represented by the unit vector $\psi \in \mathcal{H}$ by the corresponding density matrix is $\rho = |\psi\rangle\langle\psi|$, as is well known. Those states are called *pure states*, and they can be characterised by an extremality condition:

Proposition 2.5. *Consider general form of a finite-dimensional von Neumann algebra* $\mathscr{A} := \bigtimes_{j=1}^{n} \left(\mathcal{M}_{d_j} \otimes \left(\mathbb{C}\mathbb{I}_{\nu_j}\right)\right)$ *(cf. Corollary 1.48), operating on the Hilbert space* $\mathcal{H} = \bigtimes_{j=1}^{n} \left(\mathbb{C}^{d_j} \otimes \mathbb{C}^{\nu_j}\right)$. *For a density matrix* $\rho = (\rho_1, \ldots, \rho_n) \in \mathscr{S}(\mathscr{A})$ *the following statements are equivalent:*

i) ρ *is extremal in the convex set* $\mathscr{S}(\mathscr{A})$*, i.e. it cannot be written as proper convex combination* $\rho = \lambda\,\sigma + (1-\lambda)\,\tau$ *for* $\sigma, \tau \in \mathscr{S}(\mathscr{A})$*,* $\sigma \neq \tau$ *with* $0 < \lambda < 1$.

ii) *There exists* $j_0 \in \{1, \ldots, n\}$ *and* $\xi \in \mathbb{C}^{d_{j_0}}$ *with* $\|\xi\| = 1$*, such that* $\rho_{j_o} = |\xi\rangle\langle\xi| \otimes \left(\mathbb{I}_{\nu_{j_0}}/\nu_{j_0}\right)$ *and* $\rho_j = 0$ *for* $j \neq j_0$.[3]

Proof. "*(i)* $\Rightarrow$ *(ii)*". If there were two indices i, j with $\rho_i \neq 0 \neq \rho_j$ (w.l.o.g. $i = 1$), we could write ρ as the convex decomposition

$$\rho = \mathrm{tr}\rho_1 \cdot \left(\frac{\rho_1}{\mathrm{tr}\rho_1}, 0, \ldots, 0\right) + (1 - \mathrm{tr}\rho_1) \cdot \frac{(0, \rho_2, \rho_3, \ldots, \rho_n)}{1 - \mathrm{tr}\rho_1},$$

which is a valid decomposition in terms of density matrices since $1 = \mathrm{tr}\rho = \mathrm{tr}\rho_1 + \sum_{j=2}^{n} \mathrm{tr}\rho_j$, and $\rho \geq 0$ implies $\rho_j \geq 0$ for all j. Hence there exists $j_0 \in \{1, \ldots, n\}$ such that $\rho_j = 0$ for $j \neq j_0$.

Writing $\rho_{j_0} = r \otimes \left(\mathbb{I}_{\nu_{j_0}}/\nu_{j_0}\right)$ with $r \in \mathcal{M}_{d_{j_0}}$, where we divided by ν_{j_0} to assure that $\mathrm{tr}\rho_{j_0} = \mathrm{tr}r$, extremality of ρ in $\mathscr{S}(\mathscr{A})$ implies extremality of r in $\mathscr{S}(\mathcal{M}_{d_{j_0}})$. Consider the spectral decomposition

$$r = \sum_{k=1}^{\mathrm{rank}\, r} \lambda_k \cdot |e_k\rangle\langle e_k|$$

[3] Note that in the general case of a von Neumann algebra, there may exists no elements at all of the form $|\psi\rangle\langle\psi|$ in $\mathscr{A}$ (except 0, of course). For example, consider $\mathscr{A} = \mathcal{M}_d \otimes (\mathbb{C}\mathbb{I}_\nu)$ with $\nu \geq 2$. While $\mathrm{rank}\,(|\psi\rangle\langle\psi|) = 1$ for $\psi \in \mathcal{H} \setminus \{0\}$, the elements $a \otimes \mathbb{I}_\nu$ of $\mathscr{A}$ have a rank which is a multiple of ν, as $\mathrm{rank}\,(a \otimes \mathbb{I}_\nu) = \nu \cdot \mathrm{rank}\, a$. Thus the notion of pure states has to be slightly generalised to mean exactly the extremal elements of $\mathscr{S}(\mathscr{A})$; and this statement gives the exact structure of these elements in the general case.

of r, where $\lambda_k > 0$, $\sum_k \lambda_k = \mathrm{tr} r = 1$, and the (e_k) form an orthonormal system. If $\mathrm{rank}\, r$ was greater than 1, then we could again decompose convexly into density matrices as

$$r = \lambda_1 \cdot |e_1\rangle\langle e_1| + (1-\lambda_1) \cdot \frac{\sum_{k=2}^{\mathrm{rank}\, r} \lambda_k \cdot |e_k\rangle\langle e_k|}{1-\lambda_1},$$

in contradiction to extremality of r. Thus with $\xi := e_1$ we have $\rho_{j_o} = |\xi\rangle\langle\xi| \otimes \left(\mathbb{I}_{\nu_{j_0}}/\nu_{j_0}\right)$.

"$(ii) \Rightarrow (i)$". Let ρ have the supposed form as above. Assume that there exist density matrices $\sigma, \tau \in \mathscr{S}(\mathscr{A})$, $\sigma \neq \tau$ and $\lambda \in (0;1)$ such that $\rho = \lambda\sigma + (1-\lambda)\tau$. With respect to the structure of $\mathscr{A} = \bigtimes_{j=1}^n \left(\mathcal{M}_{d_j} \otimes \mathbb{I}_{\nu_j}\right)$ we can write $\rho = \left(r_j \otimes \mathbb{I}_{v_j}/\nu_j\right)_{j=1}^n$, $\sigma = \left(s_j \otimes \mathbb{I}_{v_j}/\nu_j\right)_{j=1}^n$ and $\tau = \left(t_j \otimes \mathbb{I}_{\nu_j}/\nu_j\right)_{j=1}^n$, with $0 \leq r_j, s_j, t_j \in \mathcal{M}_{d_j}$. The convex decomposition then reads as

$$r_j = \lambda \cdot s_j + (1-\lambda) \cdot t_j \quad \forall j \in \{1, \ldots, n\},$$

which for $j \neq j_0$ means $s_j = t_j = 0$ by positivity of the terms of the r.h.s.

Now, regarding $j = j_0$, we write $s = s_{j_0}$ and $t = t_{j_0}$. Observe that for any $\eta \in \mathbb{C}^{d_{j_0}}$ orthogonal to ξ, we have

$$0 = \langle\eta|\xi\rangle\langle\xi|\eta\rangle = \lambda \cdot \underbrace{\langle\eta|s|\eta\rangle}_{\geq 0} + (1-\lambda) \cdot \underbrace{\langle\eta|t|\eta\rangle}_{\geq 0},$$

hence $\langle\eta|s|\eta\rangle = 0 = \langle\eta|t|\eta\rangle$, which means that $\xi^\perp \subseteq \ker s \cap \ker t$. Taking orthogonal complements in $\mathbb{C}^{d_{j_0}}$, we get

$$\mathbb{C} \cdot \xi \supseteq (\ker s \cap \ker t)^\perp = \mathrm{ran}\, s^\dagger + \mathrm{ran}\, t^\dagger = \mathrm{ran}\, s + \mathrm{ran}\, t.$$

Thus, $\mathrm{ran}\, s = \mathbb{C} \cdot \xi = \mathrm{ran}\, t$, and $\mathrm{tr} s = 1 = \mathrm{tr} t$ implies $s = t = |\xi\rangle\langle\xi|$ and hence $\sigma = \tau$, a contradiction! $\square$

2.1.3. Observables

In quantum mechanics, one often does not use basic effects, but so-called *observables.* In our terms, an ***observable with finitely many values*** is a tuple of m effects $(E_j)_{j=1}^m$, where the E_j is the effect which occurs when outcome number j is measured. As the measurement of an observable should give exactly one outcome, the (E_j) have to sum up to 1. Such an observable is called a ***positive operator valued measure***, or *POVM.* In the special case that all the effects E_j are projections, it is called a ***projection-valued measure***, or *PVM.* This is the case that is treated in most textbooks in quantum mechanics. If we want, we can regard an effect E as a special observable, namely $(E, 1-E)$.

To a PVM (E_j) we may assign a hermitian element $O \in \mathscr{A}^{\mathrm{h}}$ via the spectral theorem, namely

$$O = \sum_{j=1}^m r_j E_j,$$

where the $r_j \in \mathbb{R}$ are the pairwise different real numbers used to indicate the measurement result. Conversely, each hermitian element $H \in \mathscr{A}^{\mathrm{h}}$ has a unique spectral decomposition

$$H = \sum_{\lambda \in \sigma(H)} \lambda E_\lambda,$$

where $\sigma(H) \subset \mathbb{R}$ denotes the spectrum of H, and the $(E_\lambda) \subset \mathscr{A}$ are the mutually orthogonal eigenprojections (which automatically sum up to $\mathrm{id}_{\mathcal{H}} = 1_{\mathscr{A}}$), so that the (E_λ) constitute a PVM.

There are two ways of constructing a one-to-one correspondence between self-adjoint operators in $\mathscr{L}(\mathcal{H})$ and PVMs, depending on whether we want to keep track of the numerical values that indicate the measurement results. Firstly, if we discard their importance, we may identify two self-adjoint operators in $\mathscr{L}(\mathcal{H})$ if they have the same eigenprojections (up to permutation, of course); then there obviously is a one-to-one correspondence between the equivalent classes $[O]$ of self-adjoint operators and PVMs, namely $O = \sum_{j=1}^m r_j E_j \;\longleftrightarrow\; (E_j)_{j=1}^m$.

Secondly, if we want to include the values indicating the measurement results, we can do that by denoting $\widehat{\mathbb{R}^m} := \{(r_1, \ldots, r_m) \in \mathbb{R}^m \mid r_1, \ldots, r_m \text{ pairwise different}\}$ the set of m-dimensional real vectors having pairwise different entries, and noting that

$$\{O \in \mathscr{L}(\mathcal{H}) \mid O^* = O\} \ni O \overset{\text{spectral theorem}}{=} \sum_{j=1}^m r_j E_j \;\longleftrightarrow\; ((r_j),\, (E_j)) \in \widehat{\mathbb{R}^m} \times \{\text{PVMs with } m \text{ values in } \mathscr{L}(\mathcal{H})\}$$

is a bijective map.

In practice, only PV measures are really implementable. However, of one performs a projective measurement on a compound system and subsequently discards one of the subsystems, the whole process can be described with a POVM on the other subsystem alone. We come back to this, as we we consider observables as channels in chapter 2.2.1.

2.1.4. Compound Systems

Consider two (distinguishable) systems, described by Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ and operator algebras $\mathscr{A} \subseteq \mathscr{L}(\mathcal{H})$ and $\mathscr{B} \subseteq \mathscr{L}(\mathcal{H})$.

As a preliminary consideration, take two distinguishable 6-sided dice (assume for example that they are painted white and black, respectively). Accordingly, we take $\mathcal{H} = \mathcal{K} = \mathbb{C}^6$ and $\mathscr{A} = \mathscr{B} = \mathcal{D}_6 = \{\mathrm{diag}(\lambda_1, \ldots, \lambda_6) \mid \lambda_j \in \mathbb{C}\}$ as $\mathcal{C}^*$-algebras describing the respective systems. The "elementary states" of the compound system are then obviously the states, where the first dice shows j and the second dice shows k ($j, k \in \{1, \ldots, 6\}$), so we can model the compound system Hilbert space as $\mathbb{C}^6 \otimes \mathbb{C}^6 = \mathcal{H} \otimes \mathcal{K}$, and the corresponding algebra as $\mathcal{D}_6 \otimes \mathcal{D}_6 = \mathscr{A} \otimes \mathscr{B}$. The effects of the compound system can then be given by (convex combinations) of "combinations" $E_1 \otimes E_2$, where $E_j \in \mathscr{E}_j$ ($j \in \{1, 2\}$),

This holds also true in the general case, where one or more systems may be quantum: For distinguishable systems $(\mathscr{A}_j, \mathcal{H}_j)$, the compound system is given by $\left(\bigotimes_j \mathscr{A}_j, \bigotimes_j \mathcal{H}_j\right)$

(c.f. the definition of tensor products of $*$-algebras in Definition 1.38). We remind that if we wanted to consider infinite-dimensional systems, we would have to take as compound Hilbert space the *Hilbert space tensor product,* which is given by the closure of the algebraic tensor product $\mathcal{H} \otimes \mathcal{K}$. Then also the tensor product of the respective algebras $\mathscr{A} \otimes \mathscr{B}$ needs to be closed in $\mathscr{L}(\mathcal{H} \otimes \mathcal{K})$ order to be a $\mathcal{C}^*$-algebra

There are also means for indistinguishable systems, where one must take the statistics of the particles into account; but we will only consider distinguishable systems.[4]

Remark. One might have wondered, why we consider proper sub-algebras $\mathscr{A} \subset \mathscr{L}(\mathcal{H})$ as representing physical systems. As an example, consider a bipartite system represented by $\mathscr{L}(\mathcal{H}) \otimes \mathscr{L}(\mathcal{K})$ of two spatially separated particles. If we want to emphasise that only the first particle is accessible by our measurements, we can emphasise this by restricting the algebra to $\mathscr{A} := \mathscr{L}(\mathcal{H}) \otimes (\mathbb{C} \cdot \mathrm{id}_{\mathcal{K}}) \subsetneq \mathscr{L}(\mathcal{H} \otimes \mathcal{K})$. Another example: We ignore the spin of a particle in a volume V: The full (i.e. dealing with spin and position) Hilbert space could be modelled as $L^2(V) \otimes \mathbb{C}^{2s+1}$, where $s \in \mathbb{N}_0/2$ denotes the total spin of the particle. If we lack the ability of (or just the interest in) measuring the direction of the spin of the particle, we may constrain our observable algebra to $\mathscr{L}(L^2(V)) \otimes (\mathbb{C} \cdot \mathrm{id}_{\mathbb{C}^{2s}})$.

2.2. Channels; Heisenberg and Schrödinger picture

Now we come to the modelling of how states can be manipulated. The presentation roughly follows [Key, 3.2.].

We want to consider measurements of observables and instruments on the same footing. This is possible if we define a channel (in the *Heisenberg picture*) as a unital completely positive map between two von Neumann algebras. The operational meaning is as follows: If E is an effect on $(\mathscr{A}, \mathcal{H})$ and $T : \mathscr{A} \longrightarrow \mathscr{B}$ is the channel, the $T(E)$ shall be the effect on $\mathscr{B}$ that corresponds to applying the channel T to the $\mathscr{A}$-system before measuring E.

It follows a justification why a channel shall have the above mentioned properties. First, as a mapping $\tilde{T} : \mathcal{E}(\mathscr{A}) \longrightarrow \mathcal{E}(\mathscr{B})$, it ought to respect mixtures, i.e. $\tilde{T}$ has to be affine. Thus, it has a unique linear extension to a $\mathbb{C}$-linear map $T : \mathscr{A} \longrightarrow \mathscr{B}$. Second, if we measure the effect 1 after applying our channel, then regardless of what the channel actually does[5], the event 1 occurs. Therefore T must be unital. Third, since a channel maps effects to effects, it has to be positive. We demand that it is possible in compound systems $\mathscr{A} \otimes \mathscr{C}$, where $\mathscr{C}$ is an arbitrary quantum system, to apply the channel only to the $\mathscr{A}$-system and do nothing on the $\mathscr{C}$-system. This operation is represented by the mapping $T \otimes \mathrm{id}_{\mathscr{C}}$, sending $\mathscr{A} \otimes \mathscr{C}$ systems to $\mathscr{B} \otimes \mathscr{C}$ systems. We want to think of $T \otimes \mathrm{id}_{\mathscr{C}}$ as special channel, thus in particular it has to be positive. Since $\mathscr{C}$ is arbitrary, this amounts to the fact that T is completely positive[6].

In many circumstances it seems more natural to think of channels as mapping states to

[4] Note that it is a good approximation, when we treat two identical quantum particles, that are isolated in disjoint volumes, as distinguishable.

[5] We tacitly assume that our channel cannot "destroy" the whole system.

[6] Although the definition of complete positivity only demands that $T \otimes \mathrm{id}_{\mathscr{C}}$ is positive for the special choices $\mathscr{C} \in \{\mathcal{M}_d \mid d \in \mathbb{N}\}$, the general case follows from that.

other states. Such a description is possible by dualisation, as we now show. Let $\mathscr{A}$ and $\mathscr{B}$ are concrete $\mathcal{C}^*$-algebras on finite dimensional Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, respectively, and let $\mathcal{S} \subseteq \mathscr{A}$ be an operator system. As (closed) subspaces of $\mathscr{L}(\mathcal{H})$ and $\mathscr{L}(\mathcal{K})$, $\mathscr{A}$, $\mathcal{S}$, and $\mathscr{B}$ inherit Hilbert-Schmidt scalar products

$$\mathscr{A} \times \mathscr{A} \ni (a,\, b) \longmapsto \mathrm{tr}(a^\dagger b) \in \mathbb{C},$$

which renders them Hilbert spaces in their own right. Here and henceforth we may denote the adjoint of an operator $a \in \mathscr{L}(\mathcal{H})$ by $a^\dagger$ instead of a^* (for $\mathscr{L}(\mathcal{K})$ accordingly). This helps us to distinguish between the adjoint of an element in a $*$-algebra and the adjoint of a map between two $*$-algebras, which we define now.

Definition 2.6. Let $T : \mathscr{A} \longrightarrow \mathscr{B}$ be a linear map. Its *adjoint* $T^* : \mathscr{B} \longrightarrow \mathscr{A}$ is defined using the Hilbert-Schmidt inner product via

$$\mathrm{tr}(b^\dagger T(a)) = \mathrm{tr}(T^*(b)^\dagger a) \;\forall a \in \mathscr{A}\, \forall b \in \mathscr{B}.$$

Note that the trace on the l.h.s. is taken over $\mathcal{K}$, whereas the trace on the r.h.s. is taken over $\mathcal{H}$. If T is a channel in the Heisenberg picture, thus mapping effects to effects, we call T^* a channel in the *Schrödinger picture,* mapping density matrices to density matrices. That verify this, we define:

Definition 2.7. A linear map $T : \mathscr{A} \longrightarrow \mathscr{B}$ is called *trace-preserving*, if it leaves the trace of an operator invariant, i.e.

$$\mathrm{tr}(T(a)) = \mathrm{tr} a \quad \forall a \in \mathscr{A}.$$

The adjoint map T^* enjoys many properties that T also has. In particular:

Proposition 2.8. *Let $T : \mathscr{A} \longrightarrow \mathscr{B}$ be a linear map. Its adjoint T^* is Hermiticity preserving, iff T is; and, for all $m \in \mathbb{N} \cup \{\infty\}$, T^* is m-positive, iff T is. Moreover, T^* is trace-preserving, iff T is unital.*

Proof. First, let T be hermitian and $b \in \mathscr{B}$. We must show that $T^*(b^\dagger) = T^*(b)^\dagger$. Indeed, by Hermiticity of T and cyclicity of the trace it holds for all $a \in \mathscr{A}$ that

$$\mathrm{tr}(T^*(b^\dagger)^\dagger a) = \mathrm{tr}(b^{\dagger\dagger} T(a)) = \mathrm{tr}(T(a)b) = \mathrm{tr}(T(a^\dagger)^\dagger b) = \mathrm{tr}(a^{\dagger\dagger} T^*(b)) = \mathrm{tr}(T^*(b)^{\dagger\dagger} a),$$

so that $T^*(b^\dagger) = T^*(b)^\dagger$.

The statement about positivity is proven as follows: for the case $m = 1$ (i.e. ordinary positivity) we have:

$$\begin{aligned} T \text{ positive} &\overset{1.14\text{b}}{\iff} \mathrm{tr}\,(pT(q)) \geq 0 \text{ for all projections } p \in \mathscr{B},\, q \in \mathscr{A} \\ &\iff \mathrm{tr}\,(T^*(p)q) = \mathrm{tr}\,(qT^*(p)) \geq 0 \text{ for all projections } p \in \mathscr{B},\, q \in \mathscr{A} \\ &\overset{1.14\text{b}}{\iff} T^* \text{ positive.} \end{aligned}$$

The case $m > 1$ follows from that, once we have shown that $(T^*)^{(n)} = \left(T^{(n)}\right)^*$. Per definition we have $(T^*)^{(n)} = T^* \otimes \mathrm{id}_{\mathcal{M}_n}$. We calculate for $a \in \mathscr{A}$, $b \in \mathscr{B}$, and $N, M \in \mathcal{M}_n$:

$$\begin{aligned}
\mathrm{tr}\left((a \otimes N)^\dagger \left(T^{(n)}\right)^* (b \otimes M)\right) &= \mathrm{tr}\left(\left(T^{(n)}(a \otimes N)\right)^\dagger (b \otimes M)\right) \\
&= \mathrm{tr}\left((T(a) \otimes N)^\dagger (b \otimes M)\right) \\
&= \mathrm{tr}\left((T(a)^\dagger b) \otimes (N^\dagger M)\right) = \mathrm{tr}\left(T(a)^\dagger b\right) \mathrm{tr}\left(N^\dagger M\right) \\
&= \mathrm{tr}\left(a^\dagger T^*(b)\right) \mathrm{tr}\left(N^\dagger M\right) = \mathrm{tr}\left((a^\dagger T^*(b)) \otimes (N^\dagger M)\right) \\
&= \mathrm{tr}\left((a^\dagger \otimes N^\dagger)(T^*(b) \otimes M)\right) \\
&= \mathrm{tr}\left((a \otimes N)^\dagger (T^*)^{(n)} (b \otimes M)\right),
\end{aligned}$$

hence $(T^*)^{(n)} = \left(T^{(n)}\right)^*$ by linearity.

For the last assertion we note the equivalence chain

$$\begin{aligned}
T^* \text{ trace-preserving} &\iff \mathrm{tr}\,(T^*(b)) = \mathrm{tr} b \quad \forall b \in \mathscr{B} \\
&\iff \forall b \in \mathscr{B}: \ \mathrm{tr}\,(b \cdot 1_{\mathscr{B}}) = \mathrm{tr}\,(T^*(b) \cdot 1_{\mathscr{A}}) = \mathrm{tr}\,(b \cdot T(1_{\mathscr{A}})) \\
&\iff 1_{\mathscr{B}} = T(1_{\mathscr{A}}) \iff T \text{ unital.}
\end{aligned}$$

□

As a mathematical consequence of the previous definitions and results, we show that complete positivity and mere positivity are actually the same, if at least one of the systems before and after applying the channel is classical.

Corollary 2.9. *Let $\mathscr{A}$ and $\mathscr{B}$ be $\mathcal{C}^*$-Algebras and $T : \mathscr{A} \longrightarrow \mathscr{B}$ a positive map. If $\mathscr{A}$ or $\mathscr{B}$ is abelian, then T is completely positive.*

Proof. It suffices to consider the case where $\mathscr{B}$ is abelian (otherwise consider first $T^* : \mathscr{B} \longrightarrow \mathscr{A}$ and apply Proposition 2.8). So assume that $\mathscr{B}$ is abelian. By Corollary 1.46 and Lemma 1.51 we can assume that

$$\mathscr{B} = \bigtimes_{j=1}^{n} \mathcal{M}_{d_j} \text{ for some } n \in \mathbb{N},\ d_j \in \mathbb{N},$$

which can only be commutative, if $d_j = 1$ for all j, hence $\mathscr{B} = \bigtimes_{j=1}^n \mathcal{M}_1 = \mathcal{D}_n$. Thus for all $j \in \{1, \dots, n\}$, the maps $T_j : \mathscr{A} \longrightarrow \mathbb{C}$, $T_j(A) = \langle e_j | T(A) | e_j \rangle$ are positive linear functionals, thus even completely positive by Lemma 1.52. The claim follows by Note 1.50. □

Remark 2.10. Although the property of m-positivity ($m \in \mathbb{N}$) is preserved when passing to the adjoint channel, the Schwarz property (according to our definition)[7] is not. As a

[7] A more general version of the Schwarz inequality for not necessarily unital maps is $T(A)^\dagger T(1)^{-1} T(A) \leq T(A^\dagger A)$, where the inverse is taken on the range.

counterexample, consider the linear map

$$E : \mathcal{M}_1 = \mathbb{C} \longrightarrow \mathcal{M}_d, \quad z \longmapsto z \cdot \mathbb{I}_d.$$

Clearly E is unital and positive; and as the domain is abelian, even completely positive by Corollary 2.9. The adjoint map $E^* : \mathcal{M}_d \longrightarrow \mathbb{C}$ can be calculated for $A \in \mathcal{M}_d$, $z \in \mathbb{C}$:

$$\operatorname{tr}\left(z^\dagger E^*(A)\right) = \operatorname{tr}\left(E(z)^\dagger A\right) = \operatorname{tr}(\overline{z}\mathbb{I}_d A) = \operatorname{tr}(z^\dagger A),$$

thus $E^* = \operatorname{tr}(\cdot)$. But for E^*, the Schwarz inequality does not hold if $d > 1$, since for example

$$E^*(\mathbb{I}_d)^\dagger E^*(\mathbb{I}_d) = d^2 \nleq d = E^*(\mathbb{I}_d^\dagger \mathbb{I}_d).$$

2.2.1. Examples

We give a few examples of what channels can describe operationally:

Example 2.11 (Classical probability)**.** Consider a classical-to-classical channel, i.e. two classical algebras $\mathscr{A} := \mathcal{D}_n$ and $\mathscr{B} := \mathcal{D}_m$ and a completely positive unital map $T : \mathscr{A} \longrightarrow \mathscr{B}$. T can be described by the numbers

$$t_{ij} := \langle e_j | T(|e_i\rangle\langle e_i|) | e_j \rangle \in [0;\, 1],$$

such that in terms of the "elementary effects" (propositions) $|e_k\rangle\langle e_k|$ we can write

$$T(|e_i\rangle\langle e_i|) = \sum_{j=1}^{m} t_{ij} \, |e_j\rangle\langle e_j| \, ,$$

which is nothing else than matrix algebra of stochastic matrices in disguise [8]. Indeed, complete positivity (which in this case reduces to positivity) implies $t_{ij} \geq 0$, and unitality of T implies that $\sum_{i=1}^{n} t_{ij} = 1$. In other words, the matrix (t_{ij}) is a stochastic matrix. Since we can write $t_{ij} = \operatorname{tr}(|e_j\rangle\langle e_j| \cdot T(|e_i\rangle\langle e_i|))$, the number t_{ij} is the probability of finding a system in the state $|e_i\rangle\langle e_i| \in \mathscr{B}$ after applying the channel, if it was before in the state $|e_j\rangle\langle e_j| \in \mathscr{A}$. The correspondent channel in the Schrödinger picture can be read off the same equation as $T^* : \mathcal{D}_m \longrightarrow \mathcal{D}_n$, $T^*(|e_j\rangle\langle e_j|) = \sum_{i=1}^{n} t_{ij} \, |e_i\rangle\langle e_i| \, .$

Example 2.12 (Observables and other mixed channels)**.** In chapter 2.1.3 we defined an observable as a collection $(E_1, \ldots, E_N) \subset \mathscr{A}$, i.e. a POVM, of effects on an algebra $\mathscr{A}$. We now show, that the measurement of observables can also be viewed as applying a channel: We define the mixed output algebra $\mathscr{B} := \mathscr{A} \otimes \mathcal{D}_N$ consisting of the quantum part $\mathscr{A}$, on which the effects are measured, and the classical channel $\mathcal{D}_N$ indicating the measurement result. Since the probability of triggering the effect E_j on a system

[8] For classical probability alone, the present framework may seem a bit too much bedevilled, but that is the price paid for a consistent way of treating classical, quantum mechanical and mixed systems on the same footing.

described by a density matrix $\rho \in \mathscr{A}$ is given by $p_j := \operatorname{tr}(\rho E_j)$, a model of the channel in the Schrödinger picture can be given by[9]

$$T^* : \mathscr{A} \longrightarrow \mathscr{A} \otimes \mathcal{D}_N, \quad \rho \longmapsto \sum_{j=1}^{N} \left(\sqrt{E_j} \rho \sqrt{E_j} \right) \otimes |e_j\rangle\langle e_j| \,.$$

If one is only interested in the measurement outcome, one can discard the quantum system after measurement, which in our model amounts to trace over the $\mathscr{A}$-part of the system:

$$\operatorname{tr}_1 \circ T^*(\rho) = \sum_{j=1}^{N} \operatorname{tr} \left(\sqrt{E_j} \rho \sqrt{E_j} \right) \cdot |e_j\rangle\langle e_j| = \sum_{j=1}^{N} p_j \, |e_j\rangle\langle e_j| \,.$$

So we get back the well-known formula for probabilities for quantum mechanical measurements.

For a detailed discussion and further examples of basic channels we refer to [Key, Chapter 3.2]

2.2.2. Structure theory of von Neumann algebras revisited

As a little interlude, with the techniques we have just introduced, we prove a corollary of Wigners theorem 1.29 on the level of von Neumann algebras. It shows, that bijective maps between $*$-algebras which are order-preserving in both directions are actually $*$-isomorphisms or $*$-anti-isomorphisms. First, we prove a result that can be found as a special case of [PWPR, Theorem II.4].

Lemma 2.13. *Let $\mathscr{A}$ and $\mathscr{B}$ be two $*$-algebras on finite-dimensional Hilbert spaces, and let $T : \mathscr{A} \longrightarrow \mathscr{B}$ be a positive, trace-preserving and unital map. If we equip $\mathscr{A}$ and $\mathscr{B}$ with the Hilbert-Schmidt scalar products $(x, y) \mapsto \operatorname{tr}(x^\dagger y)$ and the induced norm $\|x\|_2 = \sqrt{\operatorname{tr}(x^\dagger x)}$, then T is contractive w.r.t. these norms, i.e. $\|T(x)\|_2 \leq \|x\|_2$ for all $x \in \mathscr{A}$.*

Proof. We have to show $\|T\| \leq 1$, where $\|T\|$ denotes the operator norm w.r.t. to the Hilbert-Schmidt norms on $\mathscr{A}$ and $\mathscr{B}$. Since T is a mapping between Hilbert spaces, its norm equals the square root of its largest singular value, i.e. $\|T\|^2 = \max \sigma(T^* \circ T)$, where $\sigma(T^* \circ T)$ denotes the spectrum (= set of eigenvalues) of the positive (in the *usual* sense of linear algebra) operator $T^* \circ T$. By Proposition 2.8, T^* is positivity-preserving, unital, and trace-preserving, too. Hence in particular $(T^* \circ T)(1_{\mathscr{A}}) = 1_{\mathscr{A}}$.

We want to show that all eigenvalues of $T^* \circ T$ are ≤ 1, so let λ be an eigenvalue with corresponding eigenvector $V : T^*(T(V)) = \lambda \cdot V$. Since both T and T^* are hermiticity-preserving, $V^\dagger$ is also an eigenvector to λ, hence also $\tilde{V} := (V + V^\dagger)/2$, which is hermitian. We define

$$\alpha := \max \left\{ r > 0 \,\middle|\, 1_{\mathscr{A}} + r\tilde{V} \geq 0 \right\} > 0,$$

[9] There are some caveats if this formula is used in the very general case of $(E_1, \ldots, E_N)$ being merely a POVM, since the state of the system after observing E_j may be changed arbitrarily by conjugating with some unitary U_j, as some authors suggest (e.g. [Pre, Ch. 3.1.2, esp. p. 11]). However, in the case where $(E_1, \ldots, E_N)$ is actually a PVM, such that $\sqrt{E_j} = E_j$, there is no such problem.

which is well-defined, since by Proposition 1.10iii) we have $\tilde{V} \geq -\left\|\tilde{V}\right\| 1_{\mathscr{A}}$, hence $1_{\mathscr{A}} - r\tilde{V} \geq 1_{\mathscr{A}} \cdot \left(1 - r\left\|\tilde{V}\right\|\right)$, where the last term is inherently positive at least for $r \in (0, \left\|\tilde{V}\right\|^{-1}]$. Thus we have

$$0 \leq (T^* \circ T)(1_{\mathscr{A}} + \alpha\tilde{V}) = 1_{\mathscr{A}} + \alpha\lambda\tilde{V},$$

hence by definition of α it follows that $\alpha\lambda \leq \alpha$, viz. $\lambda \leq 1$. □

Proposition 2.14. *Consider two von Neumann algebras* $\mathfrak{A}^{(i)} = \times_{k=1}^{n_i} \mathcal{M}_{d_k^{(i)}} \otimes \left(\mathbb{C}\mathbb{I}_{\nu_k^{(i)}}\right)$, $i \in \{1,2\}$. *Let* $\varphi : \mathfrak{A}^{(1)} \longrightarrow \mathfrak{A}^{(2)}$ *be a positive unital bijective linear map, such that its inverse* φ^{-1} *is positive, too.*[10] *Then we in fact have* $n_1 = n_2 =: n$, *and there exists a permutation* $\{1,\ldots,n\} \ni k \longmapsto \sigma(k) \in \{1,\ldots,n\}$, *such that:*

- *For all* $k \in \{1,\ldots,n\}$, *we have* $d_k^{(1)} = d_{\sigma(k)}^{(2)}$. *In particular,* $\mathfrak{A}^{(1)} \simeq \mathfrak{A}^{(2)}$.
- *For each* k *there exists a unitary* $U_k : \mathbb{C}^{d_k^{(1)}} \longrightarrow \mathbb{C}^{d_{\sigma(k)}^{(2)}}$ *such that the action of* φ *can be stated as*

$$\varphi\left(\left(A_k \otimes \mathbb{I}_{\nu_k^{(1)}}\right)_{k=1}^{n}\right) = \left((U_{\sigma(k)}^\dagger \chi_k(A_{\sigma(k)}) U_{\sigma(k)}) \otimes \mathbb{I}_{\nu_k^{(2)}}\right)_{k=1}^{n},$$

where each χ_k *is either the identity map or the transposition map* $A \mapsto A^t$. *In other words: Each block in* $\mathfrak{A}^{(1)}$ *gets mapped onto a correspondent block in* $\mathfrak{A}^{(2)}$, *either by unitary conjugation or by transposition and unitary conjugation.*

If, in addition, φ *is a Schwarz map, then all* χ_k *are identity maps, and* φ *is a* $*$-*homomorphism.*

Proof. We consider the state spaces $\mathscr{S}(\mathfrak{A}^{(i)})$ and the dual map $\varphi^* : \mathfrak{A}^{(2)} \longrightarrow \mathfrak{A}^{(1)}$, which is positive and trace-preserving and therefore maps $\mathscr{S}(\mathfrak{A}^{(2)})$ into $\mathscr{S}(\mathfrak{A}^{(1)})$. We note that φ^* is bijective with $(\varphi^*)^{-1} = \left(\varphi^{-1}\right)^*$, since for $X, Y \in \mathfrak{A}^{(1)}$ we have

$$\begin{aligned}\operatorname{tr}\left[X^\dagger \cdot \left(\varphi^*\left((\varphi^{-1})^*(Y)\right)\right)\right] &= \operatorname{tr}\left[(\varphi(X))^\dagger \cdot \left((\varphi^{-1})^*(Y)\right)\right] \\ &= \operatorname{tr}\left[\left(\varphi^{-1}(\varphi(X))\right)^\dagger \cdot Y\right] = \operatorname{tr}\left[X^\dagger Y\right],\end{aligned}$$

[10] Note that positivity of φ^{-1} does not follow automatically, as the example

$$\varphi(a,b) = ((2a+b)/3,\ (a+2b)/3)$$

on the commutative algebra $\mathbb{C}^2$ shows – its inverse is given by

$$\varphi^{-1}(x,y) = ((2x-y)/3,\ (2y-x)/3), \text{ so e.g. } \varphi(\underbrace{(0,3)}_{\geq 0}) = (-3,6) \ngeq 0$$

hence $\varphi^* \circ (\varphi^{-1})^* = \mathrm{id}_{\mathfrak{A}^{(1)}}$, and replacing φ with φ^{-1} shows $(\varphi^{-1})^* \circ \varphi^* = \mathrm{id}_{\mathfrak{A}^{(2)}}$. In particular, $(\varphi^*)^{-1}$ maps $\mathscr{S}(\mathfrak{A}^{(1)})$ into $\mathscr{S}(\mathfrak{A}^{(2)})$, thus φ^* furnishes an affine[11] bijection $\varphi^* : \mathscr{S}(\mathfrak{A}^{(2)}) \longrightarrow \mathscr{S}(\mathfrak{A}^{(1)})$ and therefore maps extreme points to extreme points.

Let us denote the extremal points of a set X by $\mathrm{ext}(X)$. Then, recalling the characterisation of extreme points of $\mathscr{S}(\mathfrak{A}^{(i)})$ from Proposition 2.5, we define for $k \in \{1, \dots, n_i\}$ the "blocks of extremal density matrices"

$$B_k^{(i)} := \left\{ (0, \dots, 0, \underbrace{|\xi\rangle\langle\xi| \otimes \mathbb{I}_{\nu_k^{(2)}}/\nu_k^{(2)}}_{k\text{-th position}}, 0, \dots, 0) \in \mathrm{ext}\,\mathscr{S}(\mathfrak{A}^{(i)}) \;\middle|\; \xi \in \mathbb{C}^{d_k^{(i)}},\ \|\xi\| = 1 \right\},$$

which comprise the connected components of $\mathrm{ext}\,\mathscr{S}(\mathfrak{A}^{(i)})$. As the image of a connected set under a continuous map is connected, for each $k \in \{1, \dots, n_2\}$ there has to be an index $\tilde{k} \in \{1, \dots, n_1\}$ such that $\varphi^*(B_k^{(2)}) \subseteq B_{\tilde{k}}^{(1)}$. Since the same holds, if we interchange (2) and (1) by considering $(\varphi^{-1})^*$ instead of φ^*, it must be that the mapping $k \mapsto \tilde{k}$ is bijective, and $\varphi^*(B_k^{(2)}) = B_{\tilde{k}}^{(1)}$. This also establishes $n_1 = n_2 =: n$, and – for dimensional reasons – $d_k^{(2)} = d_{\tilde{k}}^{(1)}$ for all k.

For the remainder of the proof, fix $k \in \{1, \dots, n\}$, and set $d := d_k^{(2)}$, $\nu := \nu_k^{(2)}$. Let $\phi : \mathcal{M}_d \longrightarrow \mathcal{M}_d$ denote the "k-th channel of φ" defined by the equation

$$\varphi^* \left(0, \dots, 0, \underbrace{A \otimes \mathbb{I}_\nu/\nu}_{k\text{-th position}}, 0, \dots, 0 \right) = \left(0, \dots, 0, \underbrace{\phi(A) \otimes \mathbb{I}_\nu/\nu}_{\tilde{k}\text{-th position}}, 0, \dots, 0 \right) \quad \forall A \in \mathcal{M}_d.$$

Note that ϕ bijective, and that ϕ and ϕ^{-1} are both positive and trace-preserving. Consider $E := \phi(\mathbb{I}_d)$, which is positive with $\mathrm{tr}E = d$. By spectral decomposition there exists an ONB $(u_\ell)_{\ell=1}^d$ of $\mathbb{C}^d$ so that $E = \sum_{\ell=1}^d \lambda_\ell \, |u_\ell\rangle\langle u_\ell|$. If we apply ϕ^{-1} to that again, we get

$$\mathbb{I}_d = \phi^{-1}(E) = \sum_{\ell=1}^d \lambda_\ell \, |v_\ell\rangle\langle v_\ell|$$

for some set of unit vectors $(v_\ell)_{\ell=1}^d \subset \mathbb{C}^d$ (not necessarily orthogonal), that satisfy $\phi\left(|v_\ell\rangle\langle v_\ell|\right) = |u_\ell\rangle\langle u_\ell|$. Since obviously $|v_\ell\rangle\langle v_\ell| \leq \mathbb{I}$, we get by positivity of ϕ that for all $\ell \in \{1, \dots, n\}$ it holds that

$$|u_\ell\rangle\langle u_\ell| = \phi\left(|v_\ell\rangle\langle v_\ell|\right) \leq \phi(\mathbb{I}_d) = E = \sum_{\ell=1}^d \lambda_\ell \, |u_\ell\rangle\langle u_\ell| \, .$$

[11] A map f between convex spaces is called *affine*, iff it preserves convex decompositions, i.e.

$$f(\lambda x + (1 - \lambda)y) = \lambda f(x) + (1 - \lambda) f(y).$$

Because (u_ℓ) is an ONB, we can infer $1 \leq \lambda_\ell$ for all ℓ. But then we have actually equality in $d = \mathrm{tr}E = \sum_{\ell=1}^d \lambda_\ell \geq \sum_{\ell=1}^d 1 = d$, so that in fact $\lambda_\ell = 1$ $\forall \ell$, and hence $E = \mathbb{I}_d$, which means that ϕ, and thus also ϕ^{-1}, are unital. Moreover, the v_ℓ are necessarily also orthonormal, so that ϕ maps orthogonal projectors to orthogonal projectors.

By Lemma 2.13, both ϕ and ϕ^{-1} are contractive w.r.t. the Hilbert-Schmidt norms on $\mathcal{M}_d$, hence they are isometric w.r.t. the Hilbert-Schmidt norm and (since this norm comes from a scalar product)

$$\mathrm{tr}\left(\phi(X)^\dagger \phi(Y)\right) = \mathrm{tr}\left(X^\dagger Y\right) \quad \forall X, Y \in \mathcal{M}_d.$$

Let $\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$ denote the unit circle. We want to define a projective automorphism $W : \mathcal{R} \longrightarrow \mathcal{R}$, where $\mathcal{R} := \left\{ \mathbb{T}\xi \,\middle|\, \xi \in \mathbb{C}^{d_k^{(2)}} \setminus \{0\} \right\}$, that we want to invoke Wigner's theorem on. So, let $\mathbb{T}\xi \in \mathcal{R}$ ($\xi \in \mathbb{C}^{d_k^{(2)}} \setminus \{0\}$). Consider $\phi(|\xi\rangle\langle\xi|)$, which is of the form $|\eta\rangle\langle\eta|$ for some $\eta \in \mathbb{C}^{d_k^{(i)}} \setminus \{0\}$, so that we can define $W(\mathbb{T}\xi) := \mathbb{T}\eta$. (This is well defined, because $|\eta\rangle\langle\eta| = |\tilde{\eta}\rangle\langle\tilde{\eta}|$ holds iff $\mathbb{T}\eta = \mathbb{T}\tilde{\eta}$). Now, observe that for $\xi, \eta \in \mathbb{C}^{d_k^{(2)}} \setminus \{0\}$ with $\|\xi\| = \|\eta\| = 1$ we have that

$$\begin{aligned}
|\langle W(\mathbb{T}\xi)|W(\mathbb{T}\eta)\rangle|^2 &= |\mathrm{tr}\left(|W(\mathbb{T}\xi)\rangle\langle W(\mathbb{T}\xi)| \cdot |W(\mathbb{T}\eta)\rangle\langle W(\mathbb{T}\eta)|\right)| \\
&= |\mathrm{tr}\left(\phi\left(|\xi\rangle\langle\xi|\right) \phi\left(|\eta\rangle\langle\eta|\right)\right)| \\
&= \left|\mathrm{tr}\left(\phi\left(|\xi\rangle\langle\xi|\right)^\dagger \phi\left(|\eta\rangle\langle\eta|\right)\right)\right| = |\mathrm{tr}\left(|\xi\rangle\langle\xi| \cdot |\eta\rangle\langle\eta|\right)| \\
&= |\langle\xi|\eta\rangle|^2 = |\langle\mathbb{T}\xi|\mathbb{T}\eta\rangle|,
\end{aligned}$$

so we can apply Wigners theorem 1.29, which shows that ϕ is either of the form $\phi(X) = UXU^\dagger$ or $\phi(X) = UX^tU^\dagger$ for some unitary $U \in \mathscr{L}(\mathbb{C}^d)$. If we argue in that way for each k, all claims but the last follow.

Finally, if φ is a Schwarz map, the second anti-unitary possibility is ruled out: either, the block dimension is $d = 1$, in which case $X^t = X$, or, in the case $d > 1$, the transpose map is not schwarz. Indeed, take for example $X = |e_1\rangle\langle e_2|$ ((e_i) the canonical basis in $\mathbb{C}^d$) and let $t : A \mapsto A^t$ denote the transpose map. We have $t(X) = |e_2\rangle\langle e_1| = X^\dagger$ and hence

$$t(X)^\dagger t(X) = XX^\dagger = |e_1\rangle\langle e_1| \not\leq |e_2\rangle\langle e_2| = X^\dagger X = t(X^\dagger X).$$

□

2.3. Maximally entangled states and special isomorphisms

Definition 2.15. If $(e_j)_{j=1}^n$ is an orthonormal basis in the finite-dimensional Hilbert space $\mathcal{H}$, we say that the unit vector $\Omega := (\dim \mathcal{H})^{-1/2} \sum_{j=1}^n e_j \otimes e_j \in \mathcal{H} \otimes \mathcal{H}$ is a *maximally entangled vector (for $\mathcal{H}$)*, and that $|\Omega\rangle\langle\Omega| \in \mathscr{L}(\mathcal{H} \otimes \mathcal{H})$ is a *maximally entangled state (for $\mathcal{H}$)*.

Indeed, Ω is a unit vector, as

$$\|\Omega\|^2 = \langle\Omega|\Omega\rangle = (\dim\mathcal{H})^{-1}\sum_{j=1}^{n}\sum_{k=1}^{n}\underbrace{\langle e_j\otimes e_j|e_k\otimes e_k\rangle}_{=\delta_{jk}} = \frac{n}{\dim\mathcal{H}} = 1,$$

hence $|\Omega\rangle\!\langle\Omega|$ is a pure density matrix in $\mathscr{L}(\mathcal{H}\otimes\mathcal{H})$. As an element of $\mathscr{L}(\mathcal{H})\otimes\mathscr{L}(\mathcal{H})$ it has also a interesting representation:

$$|\Omega\rangle\!\langle\Omega| = (\dim\mathcal{H})^{-1}\sum_{i,j=1}^{n}|e_i\otimes e_i\rangle\!\langle e_j\otimes e_j| = (\dim\mathscr{L}(\mathcal{H}))^{-1/2}\sum_{i,j=1}^{n}\left(|e_i\rangle\!\langle e_j|\right)\otimes\left(|e_i\rangle\!\langle e_j|\right).$$

Recalling that $(|e_i\rangle\!\langle e_j|)_{i,j=1}^n$ is an orthonormal base of the Hilbert space[12] $\mathscr{L}(\mathcal{H})$, we see that $|\Omega\rangle\!\langle\Omega|$ is also a maximally entangled vector for $\mathscr{L}(\mathcal{H})$.

The dimensions of $\mathscr{L}(\mathcal{H},\mathcal{K})$ and $\mathcal{H}\otimes\mathcal{K}$ are both equal to $\dim\mathcal{H}\cdot\dim\mathcal{K}$, so that they are isomorphic as Hilbert spaces. There is a special choice of isomorphism given by the so-called *Quantum Steering:*

Proposition 2.16 (Quantum Steering). *Let $\mathcal{H}$ and $\mathcal{K}$ be finite dimensional Hilbert spaces, and let $\Omega\in\mathcal{H}\otimes\mathcal{H}$ be a maximally entangled vector for $\mathcal{H}$. Then, the mapping*

$$\mathrm{QS}_{\mathcal{H},\mathcal{K}} : \left\{\begin{matrix}\mathscr{L}(\mathcal{H},\mathcal{K}) & \longrightarrow & \mathcal{K}\otimes\mathcal{H}\\ A & \longmapsto & \sqrt{\dim\mathcal{H}}\,(A\otimes\mathrm{id}_{\mathcal{H}})\,(\Omega)\end{matrix}\right\}$$

is an isomorphism of Hilbert spaces, where $\mathscr{L}(\mathcal{H},\mathcal{K})$ is equipped with the Hilbert Schmidt scalar product.

Proof. Clearly, $\mathrm{QS}_{\mathcal{H},\mathcal{K}}$ is linear. Let $(e_j)_{j=1}^n$ denote the ONB of $\mathcal{H}$ such that $\Omega = n^{-1/2}\sum_{j=1}^n e_j\otimes e_j$. Then we calculate for $A\in\mathscr{L}(\mathcal{H},\mathcal{K})$:

$$\begin{aligned}\left\|\mathrm{QS}_{\mathcal{H},\mathcal{K}}(A)\right\|^2 &= \left\|(A\otimes\mathrm{id}_{\mathcal{H}})\,(\sqrt{n}\Omega)\right\|^2 = \sum_{j,k=1}^{n}\langle(Ae_j)\otimes e_j|(Ae_k)\otimes e_k\rangle\\ &= \sum_{j,k=1}^{n}\langle Ae_j|Ae_k\rangle\underbrace{\langle e_j|e_k\rangle}_{=\delta_{jk}} = \mathrm{tr}(A^\dagger A) = \|A\|_2^2,\end{aligned}$$

where $\|A\|_2 = \sqrt{\mathrm{tr}(A^\dagger A)}$ denotes the Hilbert-Schmidt norm of A. The calculation shows that $\mathrm{QS}_{\mathcal{H},\mathcal{K}}$ is isometric, so by dimensional reasoning it is an isomorphism of Hilbert spaces. □

Because every maximally entangled state for $\mathcal{H}$ is a maximally entangled vector for $\mathscr{L}(\mathcal{H})$, we can “lift” Proposition 2.16 from $\mathcal{H}$ to $\mathscr{L}(\mathcal{H})$ and get an isomorphism, called *Choi-Jamiołkowski isomorphism*, which has also an important feature with regard to complete positivity:

[12] Remember that $\mathscr{L}(\mathcal{H},\mathcal{K})$ carries the scalar product $(A,B) = \mathrm{tr}(A^\dagger B)$

Proposition 2.17 (Choi-Jamiołkowski). *Let $\mathcal{H}$ and $\mathcal{K}$ be finite dimensional Hilbert spaces, and let $\Omega \in \mathcal{H} \otimes \mathcal{H}$ be a maximally entangled vector for $\mathcal{H}$. Then, the mapping*

$$\mathrm{CJ}_{\mathcal{H},\mathcal{K}} : \left\{ \begin{array}{ccll} \mathscr{L}\Big(\mathscr{L}(\mathcal{H}), \mathscr{L}(\mathcal{K})\Big) & \longrightarrow & \mathscr{L}(\mathcal{K}) \otimes \mathscr{L}(\mathcal{H}) & = \mathscr{L}(\mathcal{K} \otimes \mathcal{H}) \\ T & \longmapsto & (\dim \mathcal{H}) \left(T \otimes \mathrm{id}_{\mathscr{L}(\mathcal{H})}\right) (|\Omega\rangle\langle\Omega|) & =: T^\sharp \end{array} \right\}$$

is an isomorphism of Hilbert spaces that additionally satisfies the equivalence

$$T \textit{is completely positive} \iff T^\sharp \textit{is positive.}$$

In other words, $\mathrm{CJ}_{\mathcal{H},\mathcal{K}}$ *is order-preserving, if we equip* $\mathscr{L}(\mathscr{L}(\mathcal{H}), \mathscr{L}(\mathcal{K}))$ *with the partial order defined by complete positivity, i.e.*

$$T \succeq S \;:\iff\; S \textit{and } T \textit{are hermicity-preserving, and } T - S \textit{is c.p.}$$

Proof. By replacing $\mathcal{H}$ with $\mathscr{L}(\mathcal{H})$, $\mathcal{K}$ with $\mathscr{L}(\mathcal{K})$ and Ω with $|\Omega\rangle\langle\Omega|$, we have $\mathrm{CJ}_{\mathcal{H},\mathcal{K}} = \mathrm{QS}_{\mathscr{L}(\mathcal{H}),\mathscr{L}(\mathcal{K})}$; hence Proposition 2.16 implies that $\mathrm{CJ}_{\mathcal{H},\mathcal{K}}$ is bijective and isometric.

It remains to show that T is completely positive, iff $T^\sharp$ is positive. The "$\Rightarrow$"-direction is easy: if T is completely positive, then in particular $T \otimes \mathrm{id}_{\mathscr{L}(\mathcal{H})}$ is positivity-preserving by definition, and since $|\Omega\rangle\langle\Omega|$ is a positive element of $\mathscr{L}(\mathcal{H} \otimes \mathcal{H})$ as one-dimensional projector, obviously $T^\sharp = (\dim \mathcal{H}) \left(T \otimes \mathrm{id}_{\mathscr{L}(\mathcal{H})}\right) (|\Omega\rangle\langle\Omega|) \geq 0$.

"$\Leftarrow$". Let $n \in \mathbb{N}$. We assume that $T^\sharp$ is positive and we want to show that $T \otimes \mathrm{id}_{\mathcal{M}_n}$ is positivity-preserving, so let $B \in \mathscr{L}(\mathcal{H} \otimes \mathbb{C}^n)$, say (spectral theorem) $B = \sum_{k=1}^m \lambda_k |u_k\rangle\langle u_k|$ with $\lambda_k > 0$, $m = \operatorname{rank} B$, and $(u_k) \subset \mathcal{H} \otimes \mathbb{C}^n$ an orthonormal system. Let $\phi : \mathcal{H} \otimes \mathbb{C}^n \longrightarrow \mathbb{C}^n \otimes \mathcal{H}$ be the unitary map that interchanges the tensor factors, i.e. $\phi(a \otimes b) = b \otimes a$. By Proposition 2.16 we can write $\phi(u_k) \in \mathbb{C}^n \otimes \mathcal{H}$ as

$$\phi(u_k) = (\dim \mathcal{H})^{-1/2}\, \mathrm{QS}_{\mathcal{H},\mathbb{C}^n}(A_k) = (A_k \otimes \mathrm{id}_{\mathcal{H}})\,(\Omega)$$

for some (unique) $A_k \in \mathscr{L}(\mathcal{H}, \mathbb{C}^n)$. Hence

$$u_k = \phi(\phi(u_k)) = [\phi \circ (A_k \otimes \mathrm{id}_{\mathcal{H}})]\,(\Omega) = [(\mathrm{id}_{\mathcal{H}} \otimes A_k) \circ \phi]\,(\Omega) = [\mathrm{id}_{\mathcal{H}} \otimes A_k]\,(\Omega),$$

since $\phi(\Omega) = \Omega$. Inserting this into B and using some decomposition

$$|\Omega\rangle\langle\Omega| = \sum_{i \in I} X_i \otimes Y_i$$

with $X_i, Y_i \in \mathscr{L}(\mathcal{H})$ and some finite index I we get

$$\begin{aligned}
[T \otimes \mathrm{id}_{\mathcal{M}_n}] B &= [T \otimes \mathrm{id}_{\mathcal{M}_n}] \left(\sum_{k=1}^{m} \lambda_k \left(\mathrm{id}_{\mathcal{H}} \otimes A_k\right) |\Omega\rangle\langle\Omega| \left(\mathrm{id}_{\mathcal{H}} \otimes A_k^\dagger\right) \right) \\
&= \sum_{k=1}^{m} \lambda_k \sum_{i \in I} [T \otimes \mathrm{id}_{\mathcal{M}_n}] \left(\left(\mathrm{id}_{\mathcal{H}} \otimes A_k\right) \left(X_i \otimes Y_i\right) \left(\mathrm{id}_{\mathcal{H}} \otimes A_k^\dagger\right) \right) \\
&= \sum_{k=1}^{m} \lambda_k \sum_{i \in I} [T \otimes \mathrm{id}_{\mathcal{M}_n}] \left(X_i \otimes \left(A_k Y_i A_k^\dagger \right) \right) \\
&= \sum_{k=1}^{m} \lambda_k \sum_{i \in I} \left(T(X_i) \otimes \left(A_k Y_i A_k^\dagger \right) \right) \\
&= \sum_{k=1}^{m} \lambda_k \left(\mathrm{id}_{\mathcal{H}} \otimes A_k\right) \sum_{i \in I} \left(T(X_i) \otimes Y_i\right) \left(\mathrm{id}_{\mathcal{H}} \otimes A_k^\dagger\right) \\
&= \sum_{k=1}^{m} \lambda_k \underbrace{\left(\mathrm{id}_{\mathcal{H}} \otimes A_k\right) \underbrace{[T \otimes \mathrm{id}_{\mathcal{M}_n}] \left(|\Omega\rangle\langle\Omega|\right)}_{\geq 0 \text{ by assumption}} \left(\mathrm{id}_{\mathcal{H}} \otimes A_k\right)^\dagger}_{\geq 0 \text{ by Proposition 1.10(vi)}} \geq 0.
\end{aligned}$$

□

Remark. If $(e_j) \subset \mathcal{H}$ and $(f_j) \subset \mathcal{K}$ are orthonormal bases, and $e_{ij} := |e_i\rangle\langle e_j|$ and $f_{ij} := |f_i\rangle\langle f_j|$ the corresponding orthonormal bases of $\mathscr{L}(\mathcal{H})$ and $\mathscr{L}(\mathcal{K})$, then the Choi-Jamiołkowski-isomorphism acts quite simple on the canonical basis elements:

$$\begin{aligned}
\left(|f_{ij}\rangle\langle e_{kl}|\right)^\sharp &= \sum_{nm} \left(|f_{ij}\rangle\langle e_{kl}| \otimes \mathrm{id}_{\mathscr{L}(\mathcal{H})}\right) \left(e_{nm} \otimes e_{nm}\right) \\
&= \sum_{nm} \delta_{kn} \delta_{lm} \left(f_{ij} \otimes f_{nm}\right) = \left(f_{ij} \otimes e_{kl}\right).
\end{aligned}$$

2.4. Spectra of positive maps

Here we want to investigate the possible spectra of quantum channels $T : \mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{H})$. We assume, that the Hilbert space $\mathcal{H}$ is finite-dimensional; therefore, the spectrum $\sigma(T)$ of T consists exactly of the eigenvalues of the linear map T. The next proposition is [Wol, Proposition 6.1]:

Proposition 2.18. *Let $\mathcal{H}$ be a finite dimensional Hilbert space, and let $T : \mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{H})$ be a positive map. Then the spectrum of T is the same as the spectrum of T^*. If, in addition, T is unital, then the following holds:*

i) *The spectral radius of T is equal to one: $r(T) := \max_{\lambda \in \sigma(T)} |\lambda| = 1$.*

ii) *The Jordan blocks for eigenvalues λ with $|\lambda| = 1$ are of size one.*

Proof. T is in particular Hermiticity preserving, so using lemma 1.12 yields

$$\lambda \in \sigma(T) \iff \exists V \neq 0 : T(V) = \lambda V \iff \exists V \neq 0 : T(V)^* = T(V^*) = \overline{\lambda} V^* \iff \overline{\lambda} \in \sigma(T),$$

hence $\sigma(T) = \overline{\sigma(T)}$. But from linear algebra, $\sigma(T^*) = \overline{\sigma(T)}$ (regardless of the actual scalar product that is used to define the adjoint map T^*), so the first conclusion follows.

Before we prove i) and ii), we note that the set $\mathcal{C}$ of unital positive maps $T : \mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{H})$ is closed under multiplication. By lemma 1.13, it is also bounded.

Now, let $T \in \mathcal{C}$ be a unital positive map. Choose a basis B of $\mathscr{L}(\mathcal{H})$, such that T has Jordan normal form J with respect to B. Then, the representation matrix of T^n w.r.t. B is J^n. If an eigenvalue λ of T had absolute value greater than 1, the the set $\{J^n \mid n \in \mathbb{N}\} \subset \mathcal{S}$ would be unbounded, a contradiction. This shows „$\leq$“ in (i); equality holds because $\mathrm{id}_{\mathcal{H}}$ is an eigenvector to the eigenvalue 1.

Assume, towards a contradiction, that there is a non-trivial Jordan block $K = (k_{ij})$ for an eigenvalue λ with $|\lambda| = 1$, i.e. $k_{11} = \lambda$ and $k_{12} = 1$. In J^n, this block becomes $K^n =: \left(k_{ij}^{(n)}\right)$ and with $x_n := k_{12}^{(n)}$ it follows the recursion formula

$$x_{n+1} = (K \cdot K^n)_{12} = \sum_j k_{1j} k_{j2}^{(n)} = k_{11} k_{12}^{(n)} + k_{12} k_{22}^{(n)} = \lambda x_n + 1\lambda^n,$$

hence $x_n = n\lambda^n$, which again contradicts the boundedness of $\mathcal{C}$. □

The following proposition summarises the structure theory of completely positive maps on finite dimensional spaces.

Proposition 2.19. *Let $\mathcal{H}$ and $\mathcal{K}$ be finite dimensional Hilbert spaces, and let $T : \mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{K})$ be a linear map. Then the following statements are equivalent:*

i) *T is completely positive.*

ii) (Choi-Jamiołkowski) *The Choi matrix*

$$T^\sharp = \left(T \otimes \mathrm{id}_{\mathscr{L}(\mathcal{H})}\right)(|\Omega\rangle\langle\Omega|) \in \mathscr{L}(\mathcal{K} \otimes \mathcal{H})$$

is positive for one (and then all) maximally entangled states $\Omega \in \mathcal{H}$.

iii) (Kraus form) *There exist linear maps $K_j : \mathcal{K} \longrightarrow \mathcal{H}$, $j \in \{1, \dots, r\}$, such that T is of the form*

$$T(X) = \sum_{j=1}^{r} K_j^\dagger X K_j \quad \forall X \in \mathscr{L}(\mathcal{H}).$$

The K_j are called Kraus operators*. They can be chosen orthogonal w.r.t. the Hilbert-Schmidt inner product. The minimal r in the above representation is called the* Kraus rank *of T.*

iv) (Stinespring form) *There exist $e \in \mathbb{N}$ and a linear isometry $V : \mathcal{K} \longrightarrow \mathcal{H} \otimes \mathbb{C}^e$ such that T is of the form*

$$T(X) = V^\dagger (X \otimes \mathrm{id}_{\mathbb{C}^e}) V \quad \forall X \in \mathscr{L}(\mathcal{H}).$$

2.5. Compression of the identity channel is impossible

Proposition 2.20. *Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and let positive maps $T_j : \mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{H})$ ($j \in \{1, \dots, n\}$) be given such that $\sum_{j=1}^n T_j = \mathrm{id}_{\mathscr{L}(\mathcal{H})}$. Then every T_j is a multiple of the identity channel.*

Proof. We may assume that $\dim \mathcal{H} \geq 3$. Indeed, in the cases $\dim \mathcal{H} \in \{0, 1\}$ there is very little to show, and for $\dim \mathcal{H} = 2$ we can consider $\tilde{\mathcal{H}} := \mathcal{H} \otimes \mathbb{C}^2$ (hence $\mathscr{L}(\tilde{\mathcal{H}}) \cong \mathscr{L}(\mathcal{H}) \otimes \mathcal{M}_2$) and $\tilde{T}_j := T_j \otimes \mathrm{id}_{\mathcal{M}_2}$.

The key observation is that for two orthogonal vectors $\xi, \eta \in \mathcal{H}$ we have

$$\begin{aligned} 0 = |\langle \xi|\eta \rangle|^2 = \langle \eta|\xi \rangle \langle \xi|\eta \rangle &= \big\langle \eta \big| \mathrm{id}_{\mathscr{L}(\mathcal{H})} \left(|\xi\rangle\langle\xi|\right) \big| \eta \big\rangle \\ &= \left\langle \eta \middle| \left(\sum_{j=1}^n T_j \left(|\xi\rangle\langle\xi|\right) \right) \middle| \eta \right\rangle = \sum_{j=1}^n \langle \eta | T_j \left(|\xi\rangle\langle\xi|\right) | \eta \rangle, \end{aligned}$$

where each summand in the last expression is non-negative by positivity of the T_j. Since they sum up to 0, the summands vanish individually, so that we can note a partial result:

$$\forall j \in \{1, \dots, n\} \; \forall \xi, \eta \in \mathcal{H} : \quad \langle \xi|\eta \rangle = 0 \implies \langle \eta | T_j \left(|\xi\rangle\langle\xi|\right) | \eta \rangle = 0.$$

For the remainder of the proof let us fix an index $j \in \{1, \dots, n\}$. Since $T_j\left(|\xi\rangle\langle\xi|\right)$ is positive we get $\{\xi\}^\perp \subseteq \ker\left(T_j\left(|\xi\rangle\langle\xi|\right)\right) = \left(\mathrm{ran}\left(T_j\left(|\xi\rangle\langle\xi|\right)\right)\right)^\perp$, hence by taking orthogonal complements $\mathrm{ran}\left(T_j\left(|\xi\rangle\langle\xi|\right)\right) \subseteq \mathbb{C} \cdot \xi$, hence the spectral theorem and positivity of T_j imply $T_j\left(|\xi\rangle\langle\xi|\right) = f(\xi) \cdot |\xi\rangle\langle\xi|$ for some function $f : \mathcal{H} \setminus \{0\} \longrightarrow [0, +\infty)$. For non-zero ξ, taking traces gives

$$f(\xi) = \frac{\mathrm{tr}\left[T_j\left(|\xi\rangle\langle\xi|\right)\right]}{\|\xi\|^2}, \text{ in particular } f(z\xi) = f(\xi) \text{ for } z \in \mathbb{C} \setminus \{0\}. \tag{2.5.1}$$

Now we show that f is actually constant. Take two arbitrary non-zero normalised vectors $\xi, \eta \in \mathcal{H}$ and note that the map $p := |\xi\rangle\langle\xi| + |\eta\rangle\langle\eta|$ can equally be written as $p = \frac{1}{2}\Big[|\xi + \eta\rangle\langle\xi + \eta| + |\xi - \eta\rangle\langle\xi - \eta|\Big]$. When we apply T_j to both of these "versions" of p and use (2.5.1), we get

$$f(\xi)\, |\xi\rangle\langle\xi| + f(\eta)\, |\eta\rangle\langle\eta| = \frac{1}{2}\Big[f(\xi + \eta)\, |\xi + \eta\rangle\langle\xi + \eta| + f(\xi - \eta)\, |\xi - \eta\rangle\langle\xi - \eta|\Big].$$

Sandwiching the equation with $\langle \xi|\cdot|\xi \rangle$ and using $\|\xi\| = 1$ then yields

$$\begin{aligned} &f(\xi) + f(\eta)\, |\langle \xi|\eta \rangle|^2 \\ &\quad = \frac{1}{2}\Big[f(\xi + \eta)\left(1 + \langle \xi|\eta \rangle\right)\left(1 + \langle \eta|\xi \rangle\right) + f(\xi - \eta)\left(1 - \langle \xi|\eta \rangle\right)\left(1 - \langle \eta|\xi \rangle\right)\Big] \end{aligned}$$

which holds for all normalised elements $\xi, \eta \in \mathcal{H}$. Since the right hand side is invariant under the exchange $\xi \leftrightarrow \eta$, so must be the left hand side, which means that

$$f(\xi) + f(\eta)\, |\langle \xi|\eta \rangle|^2 = f(\xi)\, |\langle \xi|\eta \rangle|^2 + f(\eta),$$

or, rearranging the terms,

$$\left(1-|\langle\xi|\eta\rangle|^2\right) f(\xi)=\left(1-|\langle\xi|\eta\rangle|^2\right) f(\eta)$$

holds for all normalised $\xi,\eta\in\mathcal{H}$. If η is a multiple of ξ, then we know $f(\xi)=f(\eta)$ from (2.5.1); otherwise we have $|\langle\xi|\eta\rangle|^2\neq 1$, so we can divide by $\left(1-|\langle\xi|\eta\rangle|^2\right)$ and obtain $f(\xi)=f(\eta)$ as well. Thus f is constant, say $f\equiv c\geq 0$. By decomposing a general operator $a\in\mathscr{L}(\mathcal{H})$ into a linear combination of rank-1-projections[13] $a=\sum_k z_k\,|\xi_k\rangle\!\langle\xi_k|$ with $z_k\in\mathbb{C}$ we finally see that

$$T(a)=\sum_k z_k c\,|\xi_k\rangle\!\langle\xi_k|=ca,\ \text{ i.e. } T=c\cdot\mathrm{id}_{\mathscr{L}(\mathcal{H})}.$$

□

An important consequence of this seemingly technical result is the fact, that the identity channel on a quantum system cannot be compressed, even when using an arbitrarily large classical side channel.

Corollary 2.21. *Consider a quantum system represented by $\mathcal{M}_d$, $d\in\mathbb{N}$, and a mixed quantum-classical system $\mathcal{M}_e\otimes\mathcal{D}_f$ ($e,f\in\mathbb{N}$). Moreover, assume there exist positive maps $E:\mathcal{M}_d\longrightarrow\mathcal{M}_e\otimes\mathcal{D}_f$ and $D:\mathcal{M}_e\otimes\mathcal{D}_f\longrightarrow\mathcal{M}_d$ such that $D\circ E=\mathrm{id}_{\mathcal{M}_d}$. Then $e\geq d$.*

Proof. First, for the case $d=1$, the result is trivial, because $e=0$ would imply $\mathcal{M}_e\otimes\mathcal{D}_f=\{0\}\otimes\mathcal{D}_f=\{0\}$, hence $E=0$, in contradiction to $D\circ E=\mathrm{id}_{\mathcal{M}_d}$. So assume $d\geq 2$.

For $j\in\{1,\dots,f\}$, let $\Pi_j:\mathcal{C}_f\longrightarrow\mathcal{C}_f$ denote the canonical projection onto the j-th component – i.e. $\Pi_j\big(\mathrm{diag}(z_1,\dots,z_f)\big)=\mathrm{diag}(0,\cdots,0,z_j,0,\dots,0))$ – and define

$$T_j:=D\circ(\mathrm{id}_{\mathcal{M}_e}\otimes\Pi_j)\circ E.$$

As composition of positive maps, the T_j are positive, and

$$\sum_{j=1}^f T_j=D\circ\left(\mathrm{id}_{\mathcal{M}_e}\otimes\left(\sum_{j=1}^f\Pi_j\right)\right)\circ E=D\circ\left(\mathrm{id}_{\mathcal{M}_e}\otimes\mathrm{id}_{\mathcal{C}_f}\right)\circ E=D\circ E=\mathrm{id}_{\mathcal{M}_d}.$$

By Proposition 2.20, there are numbers $c_j\geq 0$ such that $T_j=c_j\cdot\mathrm{id}_{\mathcal{M}_d}$ for all j, and there is at least one index j_0 with $c_{j_0}>0$. Consequently,

$$d^2=\mathrm{rank}\,T_{j_0}=\mathrm{rank}\,(D\circ(\mathrm{id}_{\mathcal{M}_e}\otimes\Pi_{j_0})\circ E)\leq\mathrm{rank}\,(\mathrm{id}_{\mathcal{M}_e}\otimes\Pi_{j_0})=e^2.$$

□

[13] This is indeed possible: First decompose a general $a\in\mathscr{L}(\mathcal{H})$ into hermitian and anti-hermitian part, and then invoke the spectral theorem for both parts to get the desired representation.

Corollary 2.22. *Let $d, e, f \in \mathbb{N}$. Consider a system $\mathscr{A} = \mathcal{M}_d \times \mathscr{B}$ consisting of a d-dimensional quantum system $\mathcal{M}_d$ and another von Neumann algebra $\mathscr{B}$ as factors. Assume there are positive maps $E : \mathscr{A} \longrightarrow \mathcal{M}_e \otimes \mathcal{D}_f$ and $D : \mathcal{M}_e \otimes \mathcal{D}_f \longrightarrow \mathscr{A}$ satisfying $D \circ E = \mathrm{id}_{\mathscr{A}}$. Then $e \geq d$.*

Proof. Let $\pi : \mathscr{A} \longrightarrow \mathcal{M}_d$ be the projection onto the first factor, and $\iota := \pi^* : \mathcal{M}_d \longrightarrow \mathscr{A}$ the corresponding embedding. We define positive maps $\tilde{E} := E \circ \iota$ and $\tilde{D} := \pi \circ D$, and see that

$$\tilde{D} \circ \tilde{E} = \pi \circ \underbrace{D \circ E}_{=\mathrm{id}_{\mathscr{A}}} \circ \iota = \pi \circ \iota = \mathrm{id}_{\mathcal{M}_d}.$$

Thus, $e \geq d$ by Corollary 2.21. $\square$

Chapter 3.

Fixed points of Schwarz maps

In this chapter, we want to classify those subspaces $\mathcal{F} \subseteq \mathscr{L}(\mathcal{H})$ that arise as fixed point spaces of quantum channels – or, more general, Schwarz maps – on finite dimensional von Neumann algebras.

Notation 3.1. For a map f, we denote the set of fixed points of f by

$$\operatorname{fix} f := \{x \in X \mid f(x) = x\} .$$

3.1. Reduction of the problem

When we are interested in the fixed points of a given positive map, the Cesaro mean of the map turns out to be a useful tool, because it results in an idempotent map while retaining the fixed point space. The following proposition gives a summary of the properties of Cesaro means.

Proposition 3.2. *Let $\mathfrak{A}$ be a von Neumann algebra on a finite dimensional Hilbert space $\mathcal{H}$ and $T : \mathfrak{A} \longrightarrow \mathfrak{A}$ a positive unital map. Then the* Cesaro-mean

$$T^{\infty} := \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} T^n,$$

where T^n means the n-fold concatenation of T, i.e. $T^n = \overbrace{T \circ \cdots \circ T}^{n \text{ times}}$, is well-defined (i.e. the limit exists), unital, and idempotent; its spectrum is contained in $\{0, 1\}$, we have $TT^{\infty} = T^{\infty}T = T^{\infty}$, and $\operatorname{fix} T^{\infty} = \operatorname{fix} T$. Moreover, T^{∞} is m-positive ($m \in \mathbb{N} \cup \{3/2\}$), if T is; and the operations of taking adjoints taking the Cesaro mean commute, i.e. $(T^{\infty})^* = (T^*)^{\infty}$.

Proof. Since $\mathfrak{A}$ is finite-dimensional, for assuring the existence of the limit it suffices to prove pointwise convergence on a basis of $\mathfrak{A}$. We consider the Jordan normal form, i.e. there take a basis of $\mathfrak{A}$ consisting of (potentially generalised) eigenvectors of T.

First, let $A \in \mathfrak{A}$ be an eigenvector of T. If the corresponding eigenvector is 1 (viz. A is a fixed point of T), we obviously have $T_N(A) = A$ for all N, hence $T^{\infty}(A) = A$. If

$\lambda \neq 1$, then

$$\begin{aligned}\|T_N(A)\| &= \frac{1}{N}\left\|\sum_{n=1}^{N} T^n(A)\right\| = \frac{1}{N}\left\|\sum_{n=1}^{N} \lambda^n A\right\| = \frac{\|A\|}{N}\left|\frac{\lambda^{N+1}-\lambda}{1-\lambda}\right| \\ &\leq \frac{\|A\|}{N}\cdot\frac{|\lambda|^{N+1}+|\lambda|}{|1-\lambda|} \leq \frac{\|A\|}{N}\cdot\frac{2}{|1-\lambda|} \overset{N\to\infty}{\longrightarrow} 0,\end{aligned}$$

where in the last inequality we used $|\lambda| \leq 1$ by Prop. 2.18i). Thus $T^\infty(A) = 0$. We still have to check what happens to generalised eigenvectors, so let $A_0, \ldots, A_\nu$ be a Jordan chain of generalised eigenvectors, i.e. $T(A_0) = \lambda A_0$ and $T(A_k) = \lambda A_k + A_{k-1}$ for $k \in \{1, \ldots, \nu\}$. Using induction on n, it is straightforward to show that $T^n(A_k) = \sum_{j=0}^{k} \binom{n}{k-j} \lambda^{n+j-k} A_j$, so we can estimate

$$\begin{aligned}\|T_N(A_k)\| &= \frac{1}{N}\left\|\sum_{n=1}^{N}\sum_{j=0}^{k}\binom{n}{k-j}\lambda^{n+j-k}A_j\right\| \leq \frac{1}{N}\sum_{n=1}^{N}\sum_{j=0}^{k}\binom{n}{k-j}|\lambda|^{n+j-k}\|A_j\| \\ &= \frac{1}{N}\sum_{n=1}^{N}|\lambda|^n\sum_{j=0}^{k}\underbrace{\frac{n!}{(n-k+j)!}}_{\leq n^{k-j}\leq n^k}\cdot\frac{1}{(k-j)!}|\lambda|^{j-k}\|A_j\| \\ &\leq \frac{1}{N}\left(\sum_{n=1}^{N}|\lambda|^n n^k\right)\left(\sum_{j=0}^{k}\frac{|\lambda|^{j-k}}{(k-j)!}\|A_j\|\right).\end{aligned}$$

Note that by By Prop. 2.18ii) we have $|\lambda| < 1$ for generalised eigenvectors, so by the Root test, the sums $\sum_{n=1}^{N} |\lambda|^n n^k$ converge for $N \to \infty$, as $\sqrt[n]{|\lambda|^n n^k} = |\lambda| \sqrt[n]{n}^k \overset{N\to\infty}{\longrightarrow} |\lambda| < 1$. Thus also $T^\infty(A_k) = \lim_{N\to\infty} T_N(A_k) = 0$. Now, the assertions $TT^\infty = T^\infty T = T^\infty$ follow by plugging in the basis elements:

- For $T(A) = A$ (i.e. $\lambda = 1$), we have $T^\infty(A) = A = T(A)$, hence $T(T^\infty(A)) = T^\infty(T(A)) = T^\infty(A) = A$.
- For eigenvectors A that correspond to eigenvalues $\lambda \neq 1$ we have $T^\infty(A) = 0$, hence $T(T^\infty(A)) = T(0) = 0$, and $T^\infty(T(A)) = \lambda T^\infty(A) = 0$.
- For generalised eigenvectors A_k as above we have $T^\infty(A_k) = 0$, hence $T(T^\infty(A_k)) = 0$, and $T^\infty(T(A_k)) = T^\infty(\lambda A_k + A_{k-1}) = 0 + 0 = 0$.

The claim about positivity follows, as both positivity and the Schwarz property are stable under concatenations, convex combinations, and limits (cf. Note 1.50).

The equation $(T^\infty)^* = (T^*)^\infty$ is also evident, since $(T^n)^* = (T^*)^n$, and the mapping $T \mapsto T^*$ is real-linear, hence continuous. □

Remark. The mapping $T \mapsto T^\infty$ can be regarded as a projection onto the set of *idempotent* positive unital maps.

As a second step in simplifying the matter, we can restrict the domain of idempotent unital positive maps to the $*$-algebra generated by its fixed points.

Proposition 3.3. *Let $\mathfrak{A}$ be a von Neumann algebra on a finite dimensional Hilbert space $\mathcal{H}$ and let $T : \mathfrak{A} \longrightarrow \mathfrak{A}$ be an idempotent unital positive map. Let $\mathfrak{F}$ denote the $*$-algebra generated by $\operatorname{fix} T$. Then $\mathfrak{F}$ is a von Neumann algebra, and $\tilde{T} : \mathfrak{F} \longrightarrow \mathfrak{F}$, defined to be the restriction of T to $\mathfrak{F}$, is well-defined (i.e. $T(F)$ lies in $\mathfrak{F}$ for all $F \in \mathfrak{F}$), and it holds that $\operatorname{fix} \tilde{T} = \operatorname{fix} T = \operatorname{ran} T$.*

Proof. By unitality, $\mathrm{id}_{\mathcal{H}}$ is a fixed point of T, so $\mathfrak{F}$ contains $\mathrm{id}_{\mathcal{H}}$ and thus $\mathfrak{F}$ is a von Neumann algebra (cf. Prop. 1.7). Since for idempotent linear maps it holds that $\operatorname{ran} T = \operatorname{fix} T$, we have that $T(A) \in \operatorname{fix} T \subseteq \mathfrak{F}$ for every $A \in \mathfrak{A}$. □

Remark 3.4. Since $\tilde{T}$ has the same fixed point set as T, when constructing a channel that shall have a given set of operators as fixed points, it suffices to consider only channels that are defined on the $*$-algebra $\mathfrak{F}$ generated by the given operators. If one insists then on a map $\mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{H})$, one can extend it by zero on the Hilbert-Schmidt-orthogonal complement of $\mathfrak{F}$ in $\mathscr{L}(\mathcal{H})$.

It seems natural to ask, how much "information" on T is lost when restricting to $\mathfrak{F} := *\text{-Alg}(\operatorname{fix} T)$. Although in general, T cannot be reconstructed from $T_{\mathfrak{F}}$ (cf. example 3.12), but if T is in addition a Schwarz map and $\mathfrak{F}$ is unitarily equivalent to a direct sum of full matrix algebras, we will show – once we have proven the structure theorem 3.8 – that T must have been identically zero on the Hilbert-Schmidt-orthogonal complement of $\mathfrak{F}$.

3.2. The special case $*$-Alg$(\mathcal{F}) = \mathscr{L}(\mathcal{H})$

Armed with the results from section 1.8 we can now prove a key result, that can also be found (for completely positive maps, but for possibly infinite-dimensional Hilbert spaces) in [Arv2, p. 18]:

Proposition 3.5. *Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and let $T : \mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{H})$ be a unital Schwarz map. If $\operatorname{fix} T$ generates $\mathscr{L}(\mathcal{H})$ as a $*$-Algebra, then already $T = \mathrm{id}_{\mathscr{L}(\mathcal{H})}$.*

Proof. By proposition 3.2, we can safely assume that T is idempotent. Indeed, if it is not, we consider the Cesaro mean T^∞, which satisfies $\operatorname{fix} T^\infty = \operatorname{fix} T$, and use the obvious equivalence $T = \mathrm{id}_{\mathscr{L}(\mathcal{H})} \iff \operatorname{fix} T = \mathscr{L}(\mathcal{H})$.

Set $\mathcal{F} := \operatorname{fix} T$ and let P be the support projection of T (cf. proposition 1.55). By proposition 1.56a), $P \in \mathcal{F}' = (*\text{-Alg}(\mathcal{F}))' = \mathscr{L}(\mathcal{H})' = \mathbb{C}\cdot\mathrm{id}_{\mathcal{H}}$; and since P is a projection, either $P = 0$ or $P = \mathrm{id}_{\mathcal{H}}$. But $P = 0$ would imply $T(X) = T(PX) = 0$ for all $X \in \mathscr{L}(\mathcal{H})$, which would mean $\mathcal{F} = \{0\}$, a contradiction (unless $\mathcal{H} = \{0\}$, in which case the assertion is trivial)! Thus we conclude that $P = \mathrm{id}_{\mathcal{H}}$, and part (b) of proposition 1.56 yields the desired assertion. □

Proposition 3.5 implies, that for given set of fixed points, lossless compression of quantum information is impossible in the generic case (in a suitable sense):

Corollary 3.6. *Set $\mathcal{H} = \mathbb{C}^d$ and let $\mathcal{F} \subseteq \mathscr{L}(\mathcal{H}) = \mathcal{M}_d$ be a subset containing (at least) the following elements:*

- $\mathbb{I}_d \in \mathcal{F}$, *where* $\mathbb{I}_d \in \mathrm{Mat}_d(\mathbb{C})$ *is the* $d \times d$*-unit matrix,*
- *There exists a normal matrix $A \in \mathcal{F}$, that has d pairwise different (possibly complex) eigenvalues $\{\lambda_j\}$, say*
$$A = \sum_{j=1}^{d} \lambda_j \, |\psi_j\rangle\langle\psi_j| \,,$$
for some orthonormal basis $(\psi_j)_{j=1}^d \subset \mathbb{C}^d$.
- *There is another $B \in \mathcal{F}$, which, with respect to the eigenbasis of A, has non-vanishing matrix elements on the upper off-diagonal, i.e.*
$$\langle\psi_i|B|\psi_j\rangle \neq 0 \quad \textit{whenever} \quad j = i+1.$$

Then the only Schwarz map $T : \mathcal{M}_d \longrightarrow \mathcal{M}_d$, which satisfies $\mathcal{F} \subseteq \mathrm{fix}\, T$, is the identity channel $T = \mathrm{id}_{\mathcal{M}_d}$.

Proof. We consider the von Neumann algebra $\mathfrak{A} := *\text{-Alg}(\mathcal{F}) = \mathcal{F}''$ and show $\mathfrak{A} = \mathcal{M}_d$; then the conclusion follows by proposition 3.5. To this aim we will use the $*$-algebra structure of $\mathfrak{A}$, as well as functional calculus.

Firstly, for each $j \in \{1, \dots, d\}$, there exists a polynomial f_j that satisfies $f_j(\lambda_i) = \delta_{ij}$. For example, one can take
$$f_j(z) = \left(\prod_{i \neq j} (z - \lambda_i) \right) \Big/ \left(\prod_{i \neq j} (\lambda_j - \lambda_i) \right),$$
which is well defined, as the λ_j are pairwise different. By functional calculus[1] we get
$$\mathfrak{A} \ni P_j := f_j(A) = |\psi_j\rangle\langle\psi_j| \,;$$
and, by considering linear combinations, $\mathfrak{A}$ contains all matrices that are diagonal w.r.t. the ONB (ψ_j).

Secondly, for $j = i+1$ we get that
$$\mathfrak{A} \ni P_i B P_j = |\psi_i\rangle\langle\psi_i| \, B \, |\psi_j\rangle\langle\psi_j| = \underbrace{\langle\psi_i|B|\psi_j\rangle}_{\neq 0} |\psi_i\rangle\langle\psi_j| \,,$$
hence by linearity, $S_{ij} := |\psi_i\rangle\langle\psi_j| \in \mathfrak{A}$. For general $j > i$ we can write $S_{ij} = S_{i,i+1} \cdot \cdots \cdot S_{j-1,j}$, hence $S_{ij} \in \mathfrak{A}$; and for $j < i$ we get $S_{ij} = S_{ji}^* \in \mathfrak{A}$. Thus, $\mathfrak{A}$ entails all matrix units w.r.t. the ONB (ψ_j), and we conclude $\mathfrak{A} = \mathcal{M}_d$. $\square$

[1] Note that functional calculus defined for polynomials of a matrix is enough here. Since $\mathbb{I}_d \in \mathcal{F} \subset \mathfrak{A}$, the algebra $\mathfrak{A}$ is stable under this operation.

The next corollary gives two criteria to check, if an operator system generates whole $\mathscr{L}(\mathcal{H})$ as $*$-algebra.

Corollary 3.7. *Let $\mathcal{H}$ be a finite-dimensional Hilbert space and $\mathcal{F} \subseteq \mathscr{L}(\mathcal{H})$ self-adjoint with $\mathrm{id}_{\mathcal{H}} \in \mathcal{F}$. Then the following statements are equivalent:*

1. $*-\mathrm{Alg}(\mathcal{F}) = \mathscr{L}(\mathcal{H})$.
2. $\mathcal{F}' = \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}$.
3. *If $p \in \mathcal{F}'$ is a projection, then $p = 0$ or $p = \mathrm{id}_{\mathcal{H}}$.*

Proof. We have $\mathscr{A} := *-\mathrm{Alg}(\mathcal{F}) = \mathcal{F}''$ by finite dimension of $\mathcal{H}$ (since the generated von Neumann algebra equals the generated $*$-algebra) and Proposition 1.5(g). By part (e) of the same Proposition, $\mathscr{A}' = \mathcal{F}''' = \mathcal{F}'$, hence (1) $\Leftrightarrow$ (2).

(2) $\Rightarrow$ (3) is obvious, and $\neg$(2) $\Rightarrow$ $\neg$(3) follows by spectral calculus. □

3.3. The general case

Now we want to weaken the condition in proposition 3.5, that T lives on a full $\mathscr{L}(\mathcal{H})$-algebra. One finds the following classification theorem, which constitutes our main result in this chapter:

Theorem 3.8. *Let $\mathfrak{A}$ be a von Neumann algebra on a finite dimensional Hilbert space $\mathcal{H}$, and let $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ be an idempotent unital Schwarz map. Suppose that $\mathrm{fix}\,\psi$ generates whole $\mathfrak{A}$ as a $*$-algebra. Let P denote the support projection of ψ and set $\mathfrak{I} := (1-P)\mathfrak{A} \subseteq \mathfrak{A}$ and $\mathfrak{S} := P\mathfrak{A} \subseteq \mathfrak{A}$. Then the following holds:*

Both $\mathfrak{I}$ and $\mathfrak{S}$ are two-sided ideals in $\mathfrak{A}$, we have $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{I}$ in the sense of definition 1.34. There exists a uniquely determined unital Schwarz map $\Phi : \mathfrak{S} \longrightarrow \mathfrak{I}$ such that ψ can be written as

$$\psi(S + I) = S + \Phi(S) \quad \text{for } S \in \mathfrak{S},\ I \in \mathfrak{I},$$

or, equivalently, $\psi(A) = PA + \Phi(PA)$ for all $A \in \mathfrak{A}$. Moreover:

i) $\mathrm{fix}\,\psi$ *can be given in terms of Φ as* $\mathrm{fix}\,\psi = \{A + \Phi(A) \mid A \in \mathfrak{S}\}$, *and* $\ker\psi = \mathfrak{I}$; *in particular* $\dim \mathrm{fix}\,\psi = \dim \mathfrak{S} = \mathrm{rank}\, P$, *and the kernel of ψ is an ideal in $\mathfrak{A}$.*

ii) *For $m \in \mathbb{N}$, ψ is m-positive, iff Φ is. In particular, Φ is completely positive, iff ψ is.*

Remark 3.9. Informally, one can say: Fixed point spaces of m-positive Schwarz maps in a von Neumann algebra are in one-to-one correspondence with graphs of m-positive Schwarz maps between direct summands of the von Neumann algebra.

Proof. Denoting $\mathcal{F} := \operatorname{fix}\psi$, proposition 1.56a) implies

$$P \in \mathcal{F}' = (*\text{-Alg}(\mathcal{F}))' = \mathfrak{A}',$$

hence both $\mathfrak{S}$ and $\mathfrak{I}$ are two-sided ideals in $\mathfrak{A}$, and $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{I}$. For $I \in \mathfrak{I}$ we have that $PI = 0$, hence by the properties of support projections $\psi(I) = \psi(PI) = 0$; thus $\mathfrak{I} \subseteq \ker\psi$.

We denote the projection from $\mathfrak{A}$ onto $\mathfrak{S}$ by

$$\pi := \operatorname{Proj}_{\mathfrak{S}} : \mathfrak{A} \longrightarrow \mathfrak{S}, \quad A \longmapsto PA,$$

Note that π is a surjective $*$-homomorphism. Since $\mathfrak{I} \subseteq \ker\psi$, we have $\psi = \phi \circ \pi$, where $\phi := \psi_{\restriction\mathfrak{S}}$ denotes the restriction of ψ to $\mathfrak{S}$. We define $\chi : \mathfrak{S} \longrightarrow \mathfrak{S}$ by $\chi := \pi \circ \phi$.

Then, by definition, the following diagram is commutative:

$$\begin{tikzcd}
\mathfrak{A} \arrow[r, bend left, "\pi"] \arrow[rr, bend right, "\psi"'] & \mathfrak{S} \arrow[r, bend left, "\phi"] \arrow[rr, bend right, "\chi"'] & \mathfrak{A} \arrow[r, bend left, "\pi"] & \mathfrak{S}
\end{tikzcd}$$

Note that $\chi \circ \pi = \pi \circ \psi$. The relevant properties of ψ are also shared by χ:

- Schwarz inequality: π is positive; hence for $S \in \mathfrak{S}$ we have $S = \pi(S)$ and

$$\begin{aligned}\chi(S)^*\chi(S) &= \chi(\pi(S))^*\,\chi(\pi(S)) = \pi(\psi(S))^*\,\pi(\psi(S)) \\ &= \pi(\psi(S)^*\psi(S)) \le \pi(\psi(S^*S)) = \chi(\pi(\underbrace{S^*S}_{\in\mathfrak{S}})) = \chi(S^*S).\end{aligned}$$

- Unitality: $\chi(1_{\mathfrak{S}}) = \chi \circ \pi(1_{\mathfrak{A}}) = \pi \circ \psi(1_{\mathfrak{A}}) = \pi(1_{\mathfrak{A}}) = 1_{\mathfrak{S}}$.

- Idempotence: Since $\psi = \phi \circ \pi$ is idempotent, we have that $\phi \circ \pi \circ \phi \circ \pi = \phi \circ \pi$. By surjectivity of π it follows that $\phi \circ \pi \circ \phi = \phi$, hence $\chi \circ \chi = \pi \circ \phi \circ \pi \circ \phi = \pi \circ \phi = \chi$.

Next, we claim $\operatorname{fix}\chi = \pi(\operatorname{fix}\psi)$. Indeed, for $S \in \operatorname{fix}\chi$ we can define $F := \psi(S) \in \operatorname{fix}\psi$ and get $S = \chi(S) = \chi \circ \pi(S) = \pi \circ \psi(S) = \pi(F)$, hence $S \in \pi\,(\operatorname{fix}\psi)$. Conversely, for $F \in \operatorname{fix}\psi$ we have $\chi(\pi(F)) = \chi \circ \pi(F) = \pi \circ \psi(F) = \pi(F)$, hence $\pi(F) \in \operatorname{fix}\chi$.

It readily follows that $*\text{-Alg}(\operatorname{fix}\chi) = *\text{-Alg}(\pi(\mathcal{F})) = \pi(*\text{-Alg}(\mathcal{F})) = \pi(\mathfrak{A}) = \mathfrak{S}$.

Now we consider the support projection of χ, denoted by $E \in \mathfrak{S}$. Since $P = 1_{\mathfrak{S}}$, it obviously holds that $E \le P$, so $H := P - E$ is a positive element of $\mathfrak{S}$, and from

$$\begin{aligned}\psi(H) &= \psi \circ \psi(H) = \phi \circ \underbrace{\pi \circ \phi}_{=\chi} \circ \pi(H) = \phi \circ \chi(H) \\ &= \phi\big(\chi(1_{\mathfrak{S}}) - \chi(E)\big) = \phi(0) = 0\end{aligned}$$

it follows with part (b) of proposition 1.55 that $0 = PHP = 1_{\mathfrak{S}} H 1_{\mathfrak{S}} = H$, hence $E = P = 1_{\mathfrak{S}}$. By proposition 1.56b), $\operatorname{fix}\chi$ is a $*$-algebra. Putting together the above results gives $\operatorname{fix}\chi = *\text{-Alg}(\operatorname{fix}\chi) = \mathfrak{S}$, so that in fact we have $\chi = \mathrm{id}_{\mathfrak{S}}$, i.e. $\pi \circ \psi = \pi \circ \phi \circ \pi = \chi \circ \pi = \pi$, which means that

$$\mathrm{Proj}_{\mathfrak{S}}(\psi(S)) = S \quad \text{for all } S \in \mathfrak{S}.$$

To adapt the notation to the statement in the theorem, we define $\Phi : \mathfrak{S} \longrightarrow \mathfrak{I}$ by $\Phi := \mathrm{Proj}_{\mathfrak{I}} \circ \phi$, which yields the desired representation $\psi = (\mathrm{id}_{\mathfrak{S}} + \Phi) \circ \mathrm{Proj}_{\mathfrak{S}}$. Φ is unital since $\Phi(1_{\mathfrak{S}}) = \mathrm{Proj}_{\mathfrak{I}}(\phi(1_{\mathfrak{S}})) = \mathrm{Proj}_{\mathfrak{I}}(1_{\mathfrak{A}}) = 1_{\mathfrak{I}}$. If we plug in the above form of ψ into the Schwarz inequality for ψ, we get for $S \in \mathfrak{S}$ that

$$\begin{aligned} &(S + \Phi(S))^* (S + \Phi(S)) \leq S^*S + \Phi(S^*S) \\ \Longrightarrow\ &\underbrace{S^*\Phi(S)}_{=0} + \underbrace{\Phi(S)^*S}_{=0} + \Phi(S)^*\Phi(S) \leq \Phi(S^*S), \end{aligned}$$

where the first two terms of the second line vanish because they lie in $\mathfrak{S} \cap \mathfrak{I} = \{0\}$. Thus Φ is a Schwarz map as well. Claim i) about the fixed points of ψ follows from ($S \in \mathfrak{S}$, $I \in \mathfrak{I}$)

$$S + I \in \operatorname{fix}\psi \iff S + I = \psi(S + I) = S + \Phi(S) \iff I = \Phi(S).$$

To prove (ii), note that $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{I}$ implies $\mathfrak{A} \otimes \mathcal{M}_m = (\mathfrak{S} \otimes \mathcal{M}_m) \oplus (\mathfrak{I} \otimes \mathcal{M}_m)$; and by Note 1.50, ψ is m-positive iff both of $(\mathrm{Pr}_{\mathfrak{S}} \otimes \mathrm{id}_{\mathcal{M}_m}) \circ (\psi \otimes \mathrm{id}_{\mathcal{M}_m}) = \mathrm{Pr}_{\mathfrak{S}} \otimes \mathrm{id}_{\mathcal{M}_m}$ and $(\mathrm{Pr}_{\mathfrak{I}} \otimes \mathrm{id}_{\mathcal{M}_m}) \circ (\psi \otimes \mathrm{id}_{\mathcal{M}_m}) = \Phi \otimes \mathrm{id}_{\mathcal{M}_m}$ are positive. The former is always positive, because it is a $*$-homomorphism; the positivity of the latter is precisely the condition for Φ being m-positive. $\square$

The following corollary is a reformulation of theorem 3.8 regarding concrete block-algebras. This will be of use when we will translate the characterisation from the Heisenberg picture (unital maps) into the Schrödinger picture (trace-preserving maps).

Corollary 3.10. *Let $\mathcal{B}_j := \mathcal{M}_{d_j} \otimes \mathbb{I}_{\nu_j}$ and $\mathfrak{A} := \bigtimes_{j=1}^n \mathcal{B}_j$. Let $p_j : \mathfrak{A} \longrightarrow \mathcal{B}_j$ denote the j-th coordinate map and $\iota_j : \mathcal{B}_j \longrightarrow \mathfrak{A}$ the canonical embedding of the j-th block into $\mathfrak{A}$. We equip $\mathscr{L}(\mathcal{H})$ with the Hilbert-Schmidt scalar product, so that the adjoint of p_j is $p_j^* = \iota_j$ (cf. proposition 1.33).*

Let $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ be an idempotent unital Schwarz map with fixed points $\mathcal{F} := \operatorname{fix}\psi$, and suppose that $\mathfrak{A}$ is generated by $\mathcal{F}$ as a $*$-algebra. Then the following holds true:

There is a unique decomposition of the set $\{1, \dots, n\}$ of "block indices" into two disjoint subsets S and I, and there exist unital Schwarz maps $\varphi_{s,i} : \mathcal{B}_s \longrightarrow \mathcal{B}_i$ ($s \in S$, $i \in I$) with the following properties:

1. *The image under ψ of an element $(B_j)_{j=1}^n$ does not depend on the I-blocks, i.e. $\psi \circ \iota_i = 0$ for $i \in I$.*

2. *The S-blocks are preserved under ψ, i.e. $p_s \circ \psi \circ \iota_s = \mathrm{id}_{\mathcal{B}_j}$ for $s \in S$, and $p_{s_1} \circ \psi \circ \iota_{s_2} = 0$ for $s_1, s_2 \in S$ with $s_1 \neq s_2$.*

3. *ψ maps the S-blocks via the $\varphi_{s,i}$ into the I-blocks, i.e. $p_i \circ \psi \circ \iota_s = \varphi_{s,i}$.*

In other words: Up to permutation of the blocks in such a way that the S-blocks come first, the action of ψ is given by

$$\psi\begin{pmatrix} S_1 & & & & & \\ & \ddots & & & & \\ & & S_k & & & \\ & & & I_k & & \\ & & & & \ddots & \\ & & & & & I_l \end{pmatrix},$$

$$= \begin{pmatrix} S_1 & & & & & \\ & \ddots & & & & \\ & & S_k & & & \\ & & & \Phi_1(S_1,\cdots,S_k) & & \\ & & & & \ddots & \\ & & & & & \Phi_l(S_1,\cdots,S_k) \end{pmatrix},$$

where $S_j \in \mathcal{B}_j$ $(j \in S = \{1,\ldots,k\})$ and $I_j \in \mathcal{B}_{j+k}$ $(j \in \{1,\ldots,l\})$.

Moreover, if ψ is m-positive $(m \in \mathbb{N})$, then so are all the $\varphi_{s,i}$.

Now we are in the position to verify, that we loose no information by restricting the channel to the $*$-algebra generated by the fixed points, as long as the algebra generated by the fixed points has no "multiple" blocks:

Proposition 3.11. *Let $\mathcal{H}$ be a finite dimensional Hilbert space and $\mathfrak{B} = \mathscr{L}(\mathcal{H})$. Let $\Psi : \mathfrak{B} \longrightarrow \mathfrak{B}$ be an idempotent unital Schwarz map, denote by $\mathfrak{A} \subseteq \mathfrak{B}$ the $*$-algebra generated by* $\operatorname{fix}\Psi$ *and let $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ the restriction of Ψ to $\mathfrak{A}$ (cf. proposition 3.3). Assume that $\mathfrak{A}$ is unitarily equivalent to a product of matrix algebras, $\mathfrak{A} \cong \bigtimes_{j=1}^n \mathcal{M}_{d_j}$ (i.e. $\nu_j = 1$ for all j in corollary 1.48). Then the Hilbert-Schmidt-orthogonal complement $\mathcal{C}$ of $\mathfrak{A}$ in $\mathfrak{B}$ lies in the kernel of Ψ.*

Proof. Let P, $\mathfrak{S}$, $\mathfrak{I}$ and Φ be as in theorem 3.8 and let $\mathcal{C}$ denote the Hilbert-Schmidt-orthogonal complement of $\mathfrak{A}$ in $\mathfrak{B}$. Without loss of generality we may assume that $\mathfrak{A}$ itself is block-diagonal, i.e. $\mathcal{H} = \mathbb{C}^d$, $\mathfrak{B} = \mathcal{M}_d$ and $\mathfrak{A} = \bigtimes_{j=1}^n \mathcal{M}_{d_j}$. Decomposing $\mathfrak{B} = \mathcal{M}_d$ into block matrices of sizes $d_i \times d_j$, the diagonal blocks form $\mathfrak{A}$, whereas the non-diagonal blocks belong to $\mathcal{C}$.

Since we have a orthogonal direct sum of vector spaces $\mathfrak{B} = \mathfrak{A} \oplus \mathcal{C} = \mathfrak{S} \oplus \mathfrak{I} \oplus \mathcal{C}$ and Ψ maps into $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{I}$, there are two linear maps $\alpha : \mathcal{C} \longrightarrow \mathfrak{S}$ and $\beta : \mathcal{C} \longrightarrow \mathfrak{I}$ such that $\Psi(C) = \alpha(C) + \beta(C)$ for all $C \in \mathcal{C}$. As Ψ is hermiticity-preserving, so are α and β (note that $\mathcal{C}$ is a hermitian subspace). By the formula from theorem 3.8 and idempotence of Ψ we get $\alpha(C) + \beta(C) = \psi(\alpha(C) + \beta(C)) = \alpha(C) + \Phi \circ \alpha(C)$ for all $C \in \mathcal{C}$; hence $\beta = \Phi \circ \alpha$. Thus we have to show that $\alpha = 0$.

Consider an matrix block lying in $\mathcal{C}$, i.e. an index pair $i, j \in \{1,\ldots,n\}$ with $i \neq j$, and let $X \in \mathfrak{B}$ such that it has non-zero entries only in the (i,j)-block. Then the Schwarz inequality for Ψ reads as $\Psi(X)^*\Psi(X) \leq \Psi(X^*X)$. Note that X^*X is an element of either $\mathfrak{S}$ or $\mathfrak{I}$ (depending on the value of j), so either $\Psi(X^*X) = X^*X + \Phi(X^*X)$ or $\Psi(X^*X) = 0$, so in either case $\Psi(X^*X) \leq X^*X + \Phi(X^*X)$. We consider the $\mathfrak{S}$-component of the Schwarz inequality: We have $\Psi(X)^*\Psi(X) = \alpha(X)^*\alpha(X) + \beta(X)^*\beta(X)$, whose $\mathfrak{S}$-component is $\alpha(X)^*\alpha(X)$, thus in either case case we get $0 \leq \alpha(X)^*\alpha(X) \leq X^*X$. Since X^*X lives in the (j,j)-block, so must $\alpha(X)^*\alpha(X)$, and since this block constitutes an ideal in $\mathfrak{A}$, also $\alpha(X)$ and $\alpha(X)^*$ can be non-zero only in the (j,j)-block (cf. corollary 1.19).

However, X^* lives in the (j,i)-block, so by the previous argument, $\alpha(X^*)$ lives in the (i,i)-block. But by Hermiticity $\alpha(X^*) = \alpha(X)^*$ is zero outside the (j,j)-block and outside the (i,i)-block, hence is zero. □

Note that the condition $\nu_j = 1$ is necessary, as the following example shows:

Example 3.12. Let $\mathcal{H} = \mathbb{C}^2$ and $\mathfrak{B} = \mathcal{M}_2$. Fix $\lambda \in [0, 1]$ and define

$$\Psi : \mathcal{M}_2 \longrightarrow \mathcal{M}_2, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} \lambda a + (1-\lambda)d & 0 \\ 0 & \lambda a + (1-\lambda)d \end{pmatrix}.$$

Ψ is obviously unital, idempotent and positive. Its range and fix point set is $\mathfrak{A} := \operatorname{ran}\Psi = \operatorname{fix}\Psi = \mathbb{C} \cdot \mathbb{I}_2 = \mathcal{M}_1 \otimes (\mathbb{C}\mathbb{I}_2)$, which is an abelian $\mathcal{C}^*$-algebra, so Ψ is even completely positive (since $\mathfrak{A}$ is commutative, c.f. Corollary 2.9) and in particular a Schwarz map. But the matrix

$$X := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathfrak{B},$$

which is orthogonal to $\mathfrak{A}$, is mapped to $\Psi(X) = (\lambda - (1-\lambda))\,\mathbb{I}_2 = (2\lambda - 1)\mathbb{I}_2$, which is non-zero, unless $\lambda = 1/2$.

Question 3.13. *In the general case $\nu_j \geq 1$, how much "freedom" is there in the choice of the images $\Psi(C)$, $C \in \mathcal{C}$?*

3.4. Uniqueness of a channel under a given fixed point set

Definition 3.14. Let $\mathfrak{A}$ be a von Neumann algebra on a finite dimensional Hilbert space, and let $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ be a unital idempotent Schwarz map. We call a triple $(\mathfrak{S}, \mathfrak{I}, \Phi)$ *compression triple for* ψ, if $\mathfrak{S}$ and $\mathfrak{I}$ are ideals in $\mathfrak{A}$ with $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{I}$, $\Phi : \mathfrak{S} \longrightarrow \mathfrak{I}$ is a unital Schwarz map, and the action of ψ is given by

$$\psi(S + I) = S + \Phi(S) \text{ for all } S \in \mathfrak{S},\ I \in \mathfrak{I}.$$

With this notion, theorem 3.8 states that a unital idempotent map ψ admits a compression triple, if the fixed points of ψ generate the whole domain of definition of ψ as a $*$-algebra. We now investigate, under which additional constraints the compression triple is already determined by the fixed point set.

Proposition 3.15. *Let $\mathfrak{A}$ be a von Neumann algebra on a finite dimensional Hilbert space, and let $\mathcal{F} \subseteq \mathfrak{A}$ be a self-adjoint subspace. Assume that $\mathfrak{A}$ is generated by $\mathcal{F}$ as $*$-algebra. Then there is at most one compression triple $(\mathfrak{S}, \mathfrak{I}, \Phi)$ in $\mathfrak{A}$, such that $\mathcal{F}$ is the set of fixed points of a unital Schwarz map $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$.*

In particular, the fixed point triple for ψ constructed in theorem 3.8 is unique, and for given $\mathcal{F}$, there is at most one unital idempotent Schwarz map $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ whose set of fixed points is $\mathcal{F}$.

Proof. Suppose there are two fixed point triples, i.e. $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{I} = \tilde{\mathfrak{S}} \oplus \tilde{\mathfrak{I}}$, and there exist unital Schwarz maps $\Phi : \mathfrak{S} \longrightarrow \mathfrak{I}$ and $\tilde{\Phi} : \tilde{\mathfrak{S}} \longrightarrow \tilde{\mathfrak{I}}$, such that

$$\mathcal{F} = \{S + \Phi(S) \mid S \in \mathfrak{S}\} = \left\{\tilde{S} + \tilde{\Phi}(\tilde{S}) \,\middle|\, \tilde{S} \in \tilde{\mathfrak{S}}\right\}.$$

In the remainder of the proof, we will write elements of $\mathfrak{A}$ as column vectors with respect to the direct sum decomposition

$$\mathfrak{A} = (\mathfrak{S} \cap \tilde{\mathfrak{S}}) \oplus (\mathfrak{S} \cap \tilde{\mathfrak{I}}) \oplus (\mathfrak{I} \cap \tilde{\mathfrak{S}}) \oplus (\mathfrak{I} \cap \tilde{\mathfrak{I}}).$$

The following maps can then be represented by 4×4 matrices having positive maps as entries:

$$\Pr_{\mathfrak{S}} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{pmatrix}, \quad \Pr_{\tilde{\mathfrak{S}}} = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{pmatrix},$$

$$\Phi \circ \Pr_{\mathfrak{S}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \phi_{11} & \phi_{12} & 0 & 0 \\ \phi_{21} & \phi_{22} & 0 & 0 \end{pmatrix}, \quad \tilde{\Phi} \circ \Pr_{\tilde{\mathfrak{S}}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ \tilde{\phi}_{11} & 0 & \tilde{\phi}_{12} & 0 \\ 0 & 0 & 0 & 0 \\ \tilde{\phi}_{21} & 0 & \tilde{\phi}_{22} & 0 \end{pmatrix}.$$

The key observation is now, that the set $\mathcal{F}$ is the range of and invariant under both of the maps $\Phi \circ \Pr_{\mathfrak{S}} + \Pr_{\mathfrak{S}}$ and $\tilde{\Phi} \circ \Pr_{\tilde{\mathfrak{S}}} + \Pr_{\tilde{\mathfrak{S}}}$, so that we have

$$\left(\Phi \circ \Pr_{\mathfrak{S}} + \Pr_{\mathfrak{S}}\right) = \left(\tilde{\Phi} \circ \Pr_{\tilde{\mathfrak{S}}} + \Pr_{\tilde{\mathfrak{S}}}\right)\left(\Phi \circ \Pr_{\mathfrak{S}} + \Pr_{\mathfrak{S}}\right)$$

or, equivalently (the second equation follows analogously)

$$0 = \left(\tilde{\Phi} \circ \Pr_{\tilde{\mathfrak{S}}} + \Pr_{\tilde{\mathfrak{S}}} - 1\right)\left(\Phi \circ \Pr_{\mathfrak{S}} + \Pr_{\mathfrak{S}}\right) = \left(\Phi \circ \Pr_{\mathfrak{S}} + \Pr_{\mathfrak{S}} - 1\right)\left(\tilde{\Phi} \circ \Pr_{\tilde{\mathfrak{S}}} + \Pr_{\tilde{\mathfrak{S}}}\right).$$

If we calculate explicitly, we get

$$\begin{aligned} 0 &= \begin{pmatrix} 0 & 0 & 0 & 0 \\ \tilde{\phi}_{11} & -1 & \tilde{\phi}_{12} & 0 \\ 0 & 0 & 0 & 0 \\ \tilde{\phi}_{21} & 0 & \tilde{\phi}_{22} & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \phi_{11} & \phi_{12} & 0 & 0 \\ \phi_{21} & \phi_{22} & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 0 & 0 \\ \tilde{\phi}_{11} + \tilde{\phi}_{12}\phi_{11} & \tilde{\phi}_{12}\phi_{12} - 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \tilde{\phi}_{21} - \phi_{21} + \tilde{\phi}_{22}\phi_{11} & \tilde{\phi}_{22}\phi_{12} - \phi_{22} & 0 & 0 \end{pmatrix} \end{aligned}$$

and the same equation with ϕ and $\tilde{\phi}$ interchanged. The $(2,2)$-component of this matrix equation then reads as $\tilde{\phi}_{12} = (\phi_{12})^{-1}$. Moreover, by considering the $(2,1)$-components, the sum $\tilde{\phi}_{11} + \tilde{\phi}_{12}\phi_{11}$ of two positive maps is zero, hence both summands must vanish. Thus we have $\phi_{11} = 0$ and $\tilde{\phi}_{11} = 0$.

As Φ is unital and schwarz, so is ϕ_{12}, and the same holds for $\tilde{\phi}_{12} = (\phi_{12})^{-1}$. By corollary 2.14, ϕ_{12} a $*$-isomorphism.

Now, the "fixpoint set" $\mathcal{F}$ can be written as

$$\mathcal{F} = \left\{ \begin{pmatrix} S_1 \\ S_2 \\ \phi_{12}(S_2) \\ \phi_{21}(S_1) + \phi_{22}(S_2) \end{pmatrix} \middle| \, S_1 \in \mathfrak{S} \cap \tilde{\mathfrak{S}},\ S_2 \in \mathfrak{S} \cap \tilde{\mathfrak{J}} \right\};$$

and knowing that ϕ_{12} is a $*$-isomorphism, we consider the second and third components, which constitute the ideal $\mathfrak{X} := (\mathfrak{S} \cap \tilde{\mathfrak{J}}) \oplus (\mathfrak{J} \cap \tilde{\mathfrak{S}})$, and write

$$\begin{aligned} \mathfrak{X} &= \Pr_{\mathfrak{X}}(\mathfrak{A}) = \Pr_{\mathfrak{X}}(*\text{−Alg}(\mathcal{F})) = *\text{-Alg}\left(\Pr_{\mathfrak{X}} \mathcal{F}\right) \\ &= *\text{-Alg} \underbrace{\left\{ \begin{pmatrix} S_2 \\ \phi_{12}(S_2) \end{pmatrix} \middle| \, S_2 \in \mathfrak{S} \cap \tilde{\mathfrak{J}} \right\}}_{\text{This already is a }*\text{-algebra!}} = \left\{ \begin{pmatrix} S_2 \\ \phi_{12}(S_2) \end{pmatrix} \middle| \, S_2 \in \mathfrak{S} \cap \tilde{\mathfrak{J}} \right\}. \end{aligned}$$

Considering the dimensions we infer that $\mathfrak{J} \cap \tilde{\mathfrak{S}} = \{0\}$, and since ϕ_{12} is a linear isomorphism also $\mathfrak{S} \cap \tilde{\mathfrak{J}} = \{0\}$. So we have $\mathfrak{S} = \tilde{\mathfrak{S}}$ and hence $(\mathfrak{S}, \mathfrak{J}, \Phi) = (\tilde{\mathfrak{S}}, \tilde{\mathfrak{J}}, \tilde{\Phi})$. □

3.5. Translation into the Schrödinger Picture

Here we restate the results from chapter 3.3 for channels in the Schrödinger picture. Recall the definitions and properties of adjoint channels from Chapter 2.2.

Proposition 3.16. *Let $\mathfrak{A}$ be a von Neumann algebra on a finite dimensional Hilbert space $\mathcal{H}$, and let $T : \mathfrak{A} \longrightarrow \mathfrak{A}$ be trace-preserving, n-positive and idempotent ($n \in \{2, 3, 4, \dots\} \cup \{\infty\}$). Suppose that $(\ker T)^\perp$ (i.e., the Hilbert-Schmidt-orthogonal complement of $\ker T$ in $\mathfrak{A}$) generates whole $\mathfrak{A}$ as a $*$-algebra. Then there exist two ideals $\mathfrak{S}$ and $\mathfrak{J}$ in $\mathfrak{A}$ and a trace-preserving n-positive map $\Gamma : \mathfrak{J} \longrightarrow \mathfrak{S}$ such that $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{J}$, and T can be written as*

$$T(S + I) = S + \Gamma(I) \quad \textit{for} \quad S \in \mathfrak{S},\ I \in \mathfrak{J}.$$

Moreover we have that $\operatorname{fix} T = \operatorname{ran} T = \mathfrak{S}$ and $\ker T = \{I - \Gamma(I) \mid I \in \mathfrak{J}\}$.

Proof. Consider the channel in the Heisenberg picture $\psi := T^*$, which is unital (since T is trace-preserving), idempotent, and n-positive (since T is); in particular ψ is a Schwarz map, and from

$$\operatorname{fix} \psi = \operatorname{ran} \psi = (\ker \psi^*)^\perp = (\ker T)^\perp$$

it follows that $\mathrm{fix}\,\psi$ generates $\mathfrak{A}$ as a $*$-algebra. By Theorem 3.8 there exist ideals $\mathfrak{S}$ and $\mathfrak{I}$ of $\mathfrak{A}$, such that $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{I}$, and a unital n-positive map $\Phi : \mathfrak{S} \longrightarrow \mathfrak{I}$, such that $\psi(S + I) = S + \Phi(S)$ for $S \in \mathfrak{S}$, $I \in \mathfrak{I}$.

Let us denote by $\mathcal{E}_{\mathfrak{S}} : \mathfrak{S} \longrightarrow \mathfrak{A}$ (resp. $\mathcal{E}_{\mathfrak{I}} : \mathfrak{I} \longrightarrow \mathfrak{A}$) the natural embeddings. The Hilbert-Schmidt-adjoints of $\mathcal{E}_{\mathfrak{S}}$ and $\mathcal{E}_{\mathfrak{I}}$ are the canonical projections $P_{\mathfrak{S}} = \mathrm{Proj}_{\mathfrak{S}}$ and $P_{\mathfrak{I}} = \mathrm{Proj}_{\mathfrak{I}}$, respectively. From

$$\psi = (\mathcal{E}_{\mathfrak{S}} + \mathcal{E}_{\mathfrak{I}} \circ \Phi) \circ P_{\mathfrak{S}}$$

we see by taking adjoints

$$T = \psi^* = P_{\mathfrak{S}}^* \circ (\mathcal{E}_{\mathfrak{S}}^* + \Phi^* \circ \mathcal{E}_{\mathfrak{I}}^*) = \mathcal{E}_{\mathfrak{S}} \circ (P_{\mathfrak{S}} + \Phi^* \circ P_{\mathfrak{I}}) = \mathrm{Proj}_{\mathfrak{S}} + \Phi^* \circ \mathrm{Proj}_{\mathfrak{I}},$$

so the asserted formula in the proposition holds, if we define $\Gamma := \Phi^*$, which is trace-preserving and n-positive by Proposition 2.8. Furthermore it holds that $\mathrm{fix}T = \mathrm{ran}\,T = (\ker T^*)^{\perp} = (\ker\psi)^{\perp} = \mathfrak{I}^{\perp} = \mathfrak{S}$ (where $\cdot^{\perp}$ means taking the Hilbert-Schmidt-orthogonal complement in $\mathfrak{A}$), as well as the following equivalence for $I \in \mathfrak{I}$, $S \in \mathfrak{S}$:

$$S + I \in \ker T \iff 0 = T(S + I) = S + \Phi^*(I) \iff S = -\Phi^*(I).$$

$\square$

Chapter 4.

Compression of Quantum Effects

This chapter is devoted to the task of "compressing" states of a given quantum system as small as possible, under the restriction that the measurement statistics of a given set $\mathcal{F}$ of effects shall not be altered. More precisely, if $\mathcal{H}$ is the Hilbert space representing the system, we seek a intermediate "storage system" with $\mathcal{C}^*$-algebra $\mathscr{A} := \mathcal{M}_d \otimes \mathcal{D}_k$ ($d, k \in \mathbb{N}$) consisting of a d-level quantum storage and a k-bit classical storage. Since in real applications, quantum storage is considered by far more expensive than classical storage, our aim shall be to make d as small as possible. The operation of encoding and decoding the states shall be accomplished by two channels[1] $E^* : \mathscr{A} \longrightarrow \mathscr{L}(\mathcal{H})$ (for "encode") and $D^* : \mathscr{A} \longrightarrow \mathscr{L}(\mathcal{H})$ (for "decode"). The conservation of the measurement statistics then reads as $E \circ D(f) = f$ for all $f \in \mathcal{F}$, or, equivalently, $\mathcal{F} \subseteq \operatorname{fix}(E \circ D)$.

In order to measure how many states the quantum system must have at least, we will assign a "quantum dimension" to $\mathcal{F}$, specifying how much "quantum dimensions" are required to compress $\mathcal{F}$ without losses. We will distinguish, whether we allow for the classical side channel $\mathcal{D}_k$, and which "grade of positivity" m both the encoding and the decoding channel shall have.[2] Naturally, if one wants to implement quantum compression physically, only completely positive channels are allowed, i.e. $m = \infty$.

Throughout the whole chapter, let $\mathcal{H}$ be a finite-dimensional Hilbert space.

4.1. Quantum Dimensions

Definition 4.1. Let $\mathcal{F} \subseteq \mathscr{L}(\mathcal{H})$, and $m \in \{1, 3/2, 2, 3, 4, \dots\} \cup \{\infty\}$. The *quantum dimension* of $\mathcal{F}$ (of positivity m), denoted $\operatorname{qdim}_m(\mathcal{F})$, is defined as the minimum of all $d \in \mathbb{N}_0$, such that there exist $k \in \mathbb{N}$ and two m-positive unital maps $E : \mathscr{L}(\mathcal{H}) \longrightarrow \mathcal{M}_d \otimes \mathcal{D}_k$ ("Encode") and $D : \mathcal{M}_d \otimes \mathcal{D}_k \longrightarrow \mathscr{L}(\mathcal{H})$ ("Decode") that satisfy $D \circ E(f) = f$ for all $f \in \mathcal{F}$, i.e. $\mathcal{F} \subseteq \operatorname{fix}(D \circ E)$.

Not allowing for the classical side channel, we define the *proper quantum dimension* of $\mathcal{F}$ (of positivity m), denoted $\operatorname{pqdim}_m(\mathcal{F})$, as the minimum of all $d \in \mathbb{N}_0$, such that there

[1] In this informal description, when we say we want to encode and decode the quantum states, we are speaking of the channels E^* and D^* in the Schrödinger picture. In the later discussion, E and D always refer to channels in the Heisenberg picture, i.e. they map effects to effects and the input and output algebras are reversed.

[2] Recall the different meanings for m-positive from Section 1.7: plainly positive ($m = 1$), Schwarz map ($m = 3/2$), n-positive ($m = n \in \mathbb{N}$) or completely positive ($m = \infty$).

exist m-positive unital maps $E : \mathscr{L}(\mathcal{H}) \longrightarrow \mathcal{M}_d$ and $D : \mathcal{M}_d \longrightarrow \mathscr{L}(\mathcal{H})$ that satisfy $E \circ D(f) = f$ for all $f \in \mathcal{F}$.

In both cases, a pair (E, D) achieving the above conditions is called *admissible* for the given $\mathcal{F}$ and m; if it achieves the above conditions for the minimal d, it is called *optimal*.

We want to note a few more or less obvious properties of the (proper) quantum dimension functions.

Proposition 4.2. *The (proper) quantum dimension functions* $(\mathrm{p})\mathrm{qdim}_m : 2^{\mathscr{L}(\mathcal{H})} \longrightarrow \{0, 1, \ldots, \dim \mathcal{H}\}$ *satisfy the following properties:*

i) *In the definition of (proper) quantum dimension, one can restrict the set of admissible pairs (E, D) of channels to ones, where $D \circ E$ is idempotent. Moreover, instead of $\mathscr{L}(\mathcal{H})$, the domain of E and the codomain of D need not be the whole $\mathscr{L}(\mathcal{H})$, but may only be a sub-$*$-algebra $\mathscr{A}$ that contains $\mathcal{F} \cup \{\mathrm{id}_{\mathcal{H}}\}$.*

ii) $\mathrm{qdim}_m(\emptyset) = \mathrm{pqdim}_m(\emptyset) = 0$, *and* $(\mathrm{p})\mathrm{qdim}_m(\mathcal{F}) \leq \dim \mathcal{H}$ *for all m and all $\mathcal{F}$.*[3]

iii) *Monotonicity in $\mathcal{F}$: $\mathcal{F}_1 \subseteq \mathcal{F}_2 \implies$* $(\mathrm{p})\mathrm{qdim}_m(\mathcal{F}_1) \leq (\mathrm{p})\mathrm{qdim}_m(\mathcal{F}_2)$.

iv) *Monotonicity in m: $m_1 \leq m_2 \implies$* $(\mathrm{p})\mathrm{qdim}_{m_1}(\mathcal{F}) \leq (\mathrm{p})\mathrm{qdim}_{m_2}(\mathcal{F})$.

v) *We have* $\mathrm{qdim}_m(\mathscr{L}(\mathcal{H})) = \mathrm{pqdim}_m(\mathscr{L}(\mathcal{H})) = \dim \mathcal{H}$.

vi) *Invariance under $*$-isomorphisms: If $\mathcal{K}$ is another finite-dimensional Hilbert space, $\mathfrak{A} \subseteq \mathscr{L}(\mathcal{H})$ and $\mathfrak{B} \subseteq \mathscr{L}(\mathcal{K})$ are von Neumann algebras with $\mathcal{F} \cup \{\mathrm{id}_{\mathcal{H}}\} \subseteq \mathfrak{A}$ and $\mathrm{id}_{\mathcal{K}} \in \mathfrak{B}$, and $\phi : \mathfrak{A} \longrightarrow \mathfrak{B}$ is a $*$-isomorphism, then* $(\mathrm{q})\mathrm{dim}_m(\phi(\mathcal{F})) = (\mathrm{q})\mathrm{dim}_m(\mathcal{F})$.

vii) $\mathrm{pqdim}_m(\mathcal{F}) = \dim \mathcal{H}$ *for all $m \geq 3/2$, whenever $\mathcal{F}$ generates whole $\mathscr{L}(\mathcal{H})$ as a $*$-algebra.*

viii) $\mathrm{qdim}_m(\mathcal{F}) = \dim \mathcal{H}$ *for all $m \geq 3/2$, whenever $\mathcal{F}$ generates whole $\mathscr{L}(\mathcal{H})$ as a $*$-algebra.*

Proof. (i) To see that $D \circ E$ can without loss of generality be made idempotent, define T as the Cesaro mean of the map $D \circ E$, i.e. $T := \lim_{N \to \infty} N^{-1} \sum_{n=1}^{N} (D \circ E)^n$ (cf. Proposition 3.2), so that $T = T \circ D \circ E = D \circ E \circ T = T \circ T$; and replace E by $\tilde{E} := E \circ T$ and D by $\tilde{D} := T \circ D$. Then $\tilde{D} \circ \tilde{E} = T \circ D \circ E \circ T = T$ is idempotent, as demanded, and has the same fixed points as $D \circ E$. For the second part, suppose that E is only defined on a sub-$*$-algebra $\mathfrak{A}$ of $\mathscr{L}(\mathcal{H})$ containing $\mathcal{F}$ and $\mathrm{id}_{\mathcal{H}}$. Obviously, the canonical embedding $\iota : \mathfrak{A} \hookrightarrow \mathscr{L}(\mathcal{H})$ is completely positive as a $*$-homomorphism. Hence the adjoint map $\phi := \iota^*$, given by the Hilbert-Schmidt-orthogonal projection from $\mathscr{L}(\mathcal{H})$

[3] The notation "(p)qdim" means that the respective (in)equality applies for both qdim and pqdim.

onto $\mathfrak{A}$, is completely positive, too, by Proposition 2.8. It is unital since $\mathrm{id}_{\mathcal{H}} \in \mathfrak{A}$, and it fixes $\mathcal{F}$. The extension of E defined by $\tilde{E} := E \circ \phi$ then does the job.

(ii), (iii), and (iv) should be clear from the definition.

(v) Although this property seems plausible, it is not obvious a priori. For $\dim \mathcal{H} \geq 2$, these are direct consequences of Proposition 2.20 and Corollary 2.21; for $\dim \mathcal{H} = 1$ it suffices to note that $d = 0$ is not possible, since "intermediate" system $\mathcal{M}_d \otimes \mathcal{D}_k = \mathcal{M}_0 \otimes \mathcal{D}_k = \{0\}$ is trivial, hence $D \circ E = 0$.

(vi) Take an optimal pair (E, D) for $\mathcal{F}$, where E can by (i) assumed to be only defined on $\mathfrak{A}$. The pair $(\tilde{E}, \tilde{D})$ with $\tilde{E} := E \circ \phi^{-1}$ and $\tilde{D} := \phi \circ D$ then is admissible for $\phi(\mathcal{F})$. This shows $(\mathrm{q})\mathrm{dim}_m(\phi(\mathcal{F})) \leq (\mathrm{q})\mathrm{dim}_m(\mathcal{F})$. "$\geq$ " follows by changing the roles of $\mathfrak{A}$ and $\mathfrak{B}$ and considering ϕ^{-1} instead of ϕ.

(vii) Let (E, D) be an admissible pair for $\mathcal{F} \subseteq \mathscr{L}(\mathcal{H})$ and $m \geq 3/2$. The map $T := D \circ E$ is a unital Schwarz map having $\mathcal{F}$ as fixed points; by Proposition 3.5 it is already the identity map on $\mathscr{L}(\mathcal{H})$. Hence $E : \mathscr{L}(\mathcal{H}) \longrightarrow \mathcal{M}_d$ is injective, hence by dimensional reasoning $d \geq \dim \mathcal{H}$, which shows $\mathrm{pqdim}_m(\mathcal{F}) \geq \dim \mathcal{H}$. The other inequality "$\leq$" follows by (ii).

(viii) As in (vii), for any admissible pair (E, D), $T := D \circ E$ has to be the identity map. Here we can decompose the intermediate space into ideals

$$\mathcal{M}_d \otimes \mathcal{D}_k = \bigoplus_{j=1}^{k} \underbrace{\mathcal{M}_d \otimes \{|e_j\rangle\langle e_j|\}}_{=:\mathfrak{I}_j},$$

which leads to a decomposition $E = \sum_{j=1}^{n} E_j$ with $E_j(X) := E(X) \cdot 1_{\mathfrak{I}_j}$ for $X \in \mathscr{L}(\mathcal{H})$. By Note 1.50 all E_j are positive (since E is) and add up to E. Hence, setting $T_j := D \circ E_j$, we have a set of positive maps T_j adding up to $T = \mathrm{id}_{\mathscr{L}(\mathcal{H})}$. By Proposition 2.20, all T_j are a multiple of the identity, hence at least one T_j is injective, hence (since T_j maps into $\mathfrak{I}_j$, which is unitarily equivalent to $\mathcal{M}_d$) we can infer $(\dim \mathcal{H})^2 \leq \dim \mathfrak{I}_j = \dim \mathcal{M}_d = d^2$. Thus $\mathrm{qdim}_m(\mathcal{F}) \geq \dim \mathcal{H}$, and "$\leq$" again follows by (ii). □

Next, we take one step towards finding optimal compression channels, in that combine (proper) quantum dimensions with the theory developed in Chapter 3.

Proposition 4.3. *Let $\mathcal{F} \subseteq \mathscr{L}(\mathcal{H})$ and $m \in \{3/2, 2, 3, 4, \dots\}$. Define $\mathfrak{A} := *\!-\!\mathrm{Alg}(\mathcal{F})$. Then for $d \in \mathbb{N}$, the following statements are equivalent:*

i) *There exist $k \in \mathbb{N}$ and two m-positive unital maps $\mathfrak{A} \xrightarrow{D} \mathcal{M}_d \otimes \mathcal{D}_k \xrightarrow{E} \mathfrak{A}$ with $\mathcal{F} \subseteq \mathrm{fix}(E \circ D)$.*

ii) $\mathrm{qdim}_m(\mathcal{F}) \leq d$.

iii) *There exists a unital idempotent Schwarz map $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ with $\mathcal{F} \subseteq \mathrm{fix}\,\psi$ and a compression triple $(\mathfrak{S}, \mathfrak{I}, \Phi)$ for ψ with m-positive Φ, and $\mathrm{qdim}_m(\mathfrak{S}) \leq d$.*

Regarding proper *quantum dimensions, the following statements are equivalent:*

iv) *There exist two m-positive unital maps* $\mathfrak{A} \xrightarrow{D} \mathcal{M}_d \xrightarrow{E} \mathfrak{A}$ *with* $\mathcal{F} \subseteq \mathrm{fix}(E \circ D)$.

v) $\mathrm{pqdim}_m(\mathcal{F}) \leq d$.

vi) *There exists a unital idempotent Schwarz map* $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ *with* $\mathcal{F} \subseteq \mathrm{fix}\,\psi$ *and a compression triple* $(\mathfrak{S}, \mathfrak{I}, \Phi)$ *for* ψ *with m-positive* Φ, *and* $\mathrm{pqdim}_m(\mathfrak{S}) \leq d$.

Proof. Since there is only a marginal difference between proving "$(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$" and proving "$(iv) \Leftrightarrow (v) \Leftrightarrow (vi)$", we will do both in one go. For the different "compression algebras", we will write as $\mathscr{B} := \mathcal{M}_d \otimes \mathcal{D}_k$ for the first and $\mathscr{B} := \mathcal{M}_d$ for the latter case.

"$(i) \Leftrightarrow (ii)$" is just a reformulation of Definition 4.1, making use of Proposition 4.2i).

"$(ii) \Rightarrow (iii)$". By Proposition 4.2i) there exist two unital m-positive maps $\mathfrak{A} \xrightarrow{D} \mathscr{B} \xrightarrow{E} \mathfrak{A}$, such that $\psi := E \circ D$ is idempotent, and $\mathcal{F} \subseteq \mathrm{fix}\,\psi$. From $\mathfrak{A} = *{-}\mathrm{Alg}(\mathcal{F}) \subseteq *{-}\mathrm{Alg}(\mathrm{fix}\,\psi) \subseteq \mathfrak{A}$ it follows that $\mathrm{fix}\,\psi$ generates $\mathfrak{A}$ as $*$-algebra. We invoke Theorem 3.8, which gives us a decomposition $\mathfrak{A} = \mathfrak{S} \oplus \mathfrak{I}$ into two-sided ideals, and an m-positive unital map $\Phi : \mathfrak{S} \longrightarrow \mathfrak{I}$, such that $\psi(S + I) = S + \Phi(S)$ for $S + I \in \mathfrak{S} \oplus \mathfrak{I}$; in other words, $(\mathfrak{S}, \mathfrak{I}, \Phi)$ is a compression triple for ψ. We define an admissible pair $\left(\tilde{E}, \tilde{D}\right)$ for $\mathfrak{S}$ as follows:

$$\begin{aligned} \tilde{D} :\quad & \mathfrak{S} \longrightarrow \mathscr{B}, && S \longmapsto D(S + \Phi(S)), \\ \tilde{E} :\quad & \mathscr{B} \longrightarrow \mathfrak{S}, && B \longmapsto 1_{\mathfrak{S}} \cdot E(B). \end{aligned}$$

By construction, these maps are unital and m-positive. We easily see that $\tilde{E} \circ \tilde{D} = \mathrm{id}_{\mathfrak{S}}$, since for $S \in \mathfrak{S}$ we have

$$(\tilde{E} \circ \tilde{D})(S) = 1_{\mathfrak{S}} \cdot E(D(S + \Phi(S)) = 1_{\mathfrak{S}} \cdot \psi(\underbrace{S + \Phi(S)}_{\in \mathrm{fix}\,\psi}) = 1_{\mathfrak{S}} \cdot (S + \underbrace{\Phi(S)}_{\in \mathfrak{I}}) = S.$$

Hence $\left(\tilde{E}, \tilde{D}\right)$ is indeed admissible for $\mathfrak{S}$.

"$(iii) \Rightarrow (ii)$". Let $\left(\tilde{E}, \tilde{D}\right)$ be an admissible pair for $\mathfrak{S}$, i.e. $\tilde{D} : \mathfrak{S} \longrightarrow \mathcal{M}_d$, $\tilde{E} : \mathcal{M}_d \longrightarrow \mathfrak{S}$. Note that since $\mathfrak{S}$ is already a $*$-algebra, we indeed can by Proposition 4.2i) assume that the domain of $\tilde{D}$ and the codomain of $\tilde{E}$ is $\mathfrak{S}$, and we immediately get $\tilde{E} \circ \tilde{D} = \mathrm{id}_{\mathfrak{S}}$. We define

$$\begin{aligned} D :\quad & \mathfrak{A} \longrightarrow \mathscr{B}, && A \longmapsto \tilde{D}(1_{\mathfrak{S}} \cdot A), \\ E :\quad & \mathscr{B} \longrightarrow \mathfrak{A}, && B \longmapsto \tilde{E}(M) + \Phi(\tilde{E}(M)), \end{aligned}$$

which are again unital m-positive maps, and check that (E, D) is admissible for $\mathcal{F}$. Indeed, for $F \in \mathcal{F}$ we have by properties of compression triples (Definition 3.14) $F \in \mathrm{fix}\,\psi$, hence $F = 1_{\mathfrak{S}} F + \Phi(1_{\mathfrak{S}} F)$, and the calculation

$$(E \circ D)(F) = \tilde{E}(\tilde{D}(1_{\mathfrak{S}} \cdot F)) + \Phi(\tilde{E}(\tilde{D}(1_{\mathfrak{S}} \cdot A))) = 1_{\mathfrak{S}} F + \Phi(1_{\mathfrak{S}} F) = F$$

shows $\mathcal{F} \subseteq \mathrm{fix}(E \circ D)$, as desired. $\square$

4.1.1. Quantum dimensions of sub-$*$-algebras

In this section we calculate the quantum dimensions of sub-$*$-algebras of $\mathscr{L}(\mathcal{H})$. Note that by Corollary 1.46 they are $*$-isomorphic to direct products of full matrix algebras, so our task is to determine the (proper) quantum dimensions of algebras of the form $\times_j \mathcal{M}_{d_j}$. In the case where classical side information is allowed, it will follow that the quantum dimension of a set $\mathcal{F}$ is upper bounded the the size of the largest block contained in the $*$-isomorphy class of $*$-Alg$(\mathcal{F})$, using the estimate (p)qdim$_m(\mathcal{F}) \leq$ (p)qdim$_m$ ($*-$Alg$(\mathcal{F})$). Before we do that, we need a technical means to embed d-level quantum systems in D-level quantum systems for $D \geq d$:

Lemma 4.4. *Let $d, D \in \mathbb{N}$ with $d \leq D$. Then there exist unital, completely positive maps $\iota : \mathcal{M}_d \longrightarrow \mathcal{M}_D$ and $\pi : \mathcal{M}_D \longrightarrow \mathcal{M}_d$, such that $\pi \circ \iota = \mathrm{id}_{\mathcal{M}_d}$.*

Proof. If $d = D$, then we can take $\iota = \pi = \mathrm{id}_{\mathcal{M}_d}$, so let us assume $d < D$. A first "guess" for ι may be

$$\iota_1\left((a_{ij})_{i,j=1}^d\right) = (\tilde{a}_{ij})_{i,j=1}^D, \quad \text{where } \tilde{a}_{ij} = \begin{cases} a_{ij} & \text{for } i,j \in \{1,\dots,d\}, \\ 0 & \text{otherwise.} \end{cases}$$

Obviously, ι_1 is completely positive, but not unital, as

$$\iota_1(\mathbb{I}_d) = \sum_{j=1}^d |e_j^D\rangle\langle e_j^D| \neq \sum_{j=1}^D |e_j^D\rangle\langle e_j^D| = \mathbb{I}_D,$$

where $(e_1^D, \dots, e_D^D)$ denotes the canonical basis of $\mathbb{C}^D$. However, we can fill in the missing part by adding to ι_1 the map

$$\iota_2 : \quad \mathcal{M}_d \ni A \longmapsto \frac{\mathrm{tr}A}{d} \cdot (\mathbb{I}_D - \iota_1(\mathbb{I}_d)) \in \mathcal{M}_e,$$

which is completely positive, since $A \mapsto \mathrm{tr}A/d$ is completely positive and unital, and

$$(\mathbb{I}_D - \iota_1(\mathbb{I}_d)) = \sum_{j=d+1}^D |e_j^D\rangle\langle e_j^D| \geq 0.$$

Thus $\iota := \iota_1 + \iota_2$ does the job.

Finding a suitable π is easy, for we can take

$$\pi\left((b_{ij})_{i,j=1}^D\right) = (b_{ij})_{i,j=1}^d = V^\dagger \cdot (b_{ij})_{i,j=1}^D \cdot V$$

with the $(D \times d)$-matrix $V = \sum_{j=1}^d \left|e_j^D\right\rangle\left\langle e_j^d\right|$. The map π is unital, completely positive as it is given in Kraus form, and $\pi \circ \iota = \mathrm{id}_{\mathcal{M}_d}$, as desired. □

Proposition 4.5. *Let $\mathfrak{A}$ be a $*$-algebra in $\mathcal{H}$, and let $m \in \mathbb{N} \cup \{3/2, \infty\}$. If the $*$-isomorphy class of $\mathfrak{A}$ is*

$$\mathfrak{A} \simeq \bigtimes_{j=1}^n \mathcal{M}_{d_j}, \quad \text{then} \quad \mathrm{qdim}_m(\mathfrak{A}) = \max_{j=1}^n d_j.$$

Proof. Without loss of generality we may assume $\mathfrak{A} = \bigtimes_{j=1}^n \mathcal{M}_{d_j}$ and arrange the order of the d_j such that $e := d_1 = \max_{j=1}^n d_j$. For $d \leq e$, $d \in \mathbb{N}$, let ι_d and π_d denote the maps from Lemma 4.4 and set $\mathscr{B} := \mathcal{M}_e \otimes \mathcal{D}_n$. We identify $\mathscr{B}$ with $\bigtimes_{j=1}^n \mathcal{M}_e$ via the unitary equivalence implemented by

$$U : \mathbb{C}^e \otimes \mathbb{C}^n \longrightarrow \bigtimes_{j=1}^n \mathbb{C}^e, \quad v \otimes w \longmapsto (v \cdot \langle e_j | w \rangle)_{j=1}^n .$$

Then, we simply define the maps

$$\begin{aligned} D : \quad \mathfrak{A} &\longrightarrow \mathscr{B}, \qquad (A_j)_{j=1}^n \longmapsto \left(\iota_{d_j}(A_j)\right)_{j=1}^n , \\ E : \quad \mathscr{B} &\longrightarrow \mathfrak{A}, \qquad (B_j)_{j=1}^n \longmapsto \left(\pi_{d_j}(B_j)\right)_{j=1}^n . \end{aligned}$$

Then both D and E are completely positive and unital by construction (cf. 1.33ii). Hence $\operatorname{qdim}_m(\mathfrak{A}) \leq e$.

In order to show $\operatorname{qdim}_m(\mathfrak{A}) \geq e$, assume that there exist $f, k \in \mathbb{N}$ and two unital m-positive maps $D : \mathfrak{A} \longrightarrow \mathcal{M}_f \otimes \mathcal{D}_k$ and $E : \mathcal{M}_f \otimes \mathcal{D}_k \longrightarrow \mathfrak{A}$ such that $E \circ D = \mathrm{id}_{\mathfrak{A}}$. Then Corollary 2.22 ($\mathscr{A} = \mathfrak{A}$, $\mathscr{B} = \bigtimes_{j=2}^n \mathcal{M}_{d_j}$ in the notation therein) immediately yields $f \geq e$. $\square$

In terms of compression of given points we can note the following result:

Corollary 4.6. *Let $\mathcal{F} \subset \mathscr{L}(\mathcal{H})$ be given with $\mathrm{id}_{\mathcal{H}} \in \mathcal{F}$, $m \in \{3/2, 2, 3, 4, \dots\} \cup \{\infty\}$, and assume that $*$-alg$(\mathcal{F}) \simeq \bigtimes_{j=1}^n \mathcal{M}_{d_j}$. Then we have*

$$\min_{j=1}^n d_j \leq \operatorname{qdim}_m(\mathcal{F}) \leq \max_{j=1}^n d_j .$$

Proof. Set $\mathfrak{A} := *\text{-Alg}(\mathcal{F})$. The upper bound follows from $\operatorname{qdim}_m(\mathcal{F}) \leq \operatorname{qdim}_m(\mathfrak{A})$ and Proposition 4.5. For the lower bound, by Proposition 4.3 there exists an idempotent Schwarz map $\psi : \mathfrak{A} \longrightarrow \mathfrak{A}$ with $\mathcal{F} \subseteq \operatorname{fix} \psi$ and a compression triple $(\mathfrak{S}, \mathfrak{I}, \Phi)$ for ψ, where $\operatorname{qdim}_m(\mathfrak{S}) = \operatorname{qdim}_m(\mathcal{F})$. Since $\mathfrak{S}$ is an ideal in $\mathfrak{A}$ and $\mathfrak{S} \neq \{0\}$ (otherwise ψ would be identically zero), $\mathfrak{S} \simeq \bigtimes_{j \in J} \mathcal{M}_{d_j}$, where J is an non-empty subset of $\{1, \dots, n\}$. Thus $\operatorname{qdim}_m(\mathcal{F}) = \operatorname{qdim}_m(\mathfrak{S}) = \max_{j \in J} d_j \geq \min_{j=1}^n d_j$. $\square$

4.1.2. Is there a difference whether we compress effects or "only" whole observables?

With regard to physical application, the reader might wonder, if it makes a difference whether we preserve *observables* (in the sense of self-adjoint operators) as required fixed points, or the set of *effects* associated to them in the sense of section 2.1.3.

Consider a self-adjoint observable (projection valued measure)

$$\mathcal{O} = \sum_{\lambda \in \sigma(\mathcal{O})} \lambda P_\lambda \in \mathscr{L}(\mathcal{H}),$$

which we want to measure (possibly among others), after we apply our compression-decompression procedure. We denoted $\mathcal{O}$ as already decomposed into its spectral fractions, so P_λ are the mutually orthogonal eigenprojections. We ask, if a channel that fixes $\mathcal{O}$ automatically fixes all P_λ.

Recall that the physical interpretation is that for a density matrix ρ, the probability of measuring λ is $\mathbb{P}_\rho[\mathcal{O} \doteq \lambda] = \operatorname{tr}(\rho P_\lambda)$, so the expectation value of $\mathcal{O}$ is

$$\mathbb{E}_\rho(\mathcal{O}) = \sum_{\lambda\in\sigma(\mathcal{O})} \lambda \cdot \mathbb{P}_\rho[\mathcal{O} \doteq \lambda] = \sum_{\lambda\in\sigma(\mathcal{O})} \operatorname{tr}(\rho\lambda P_\lambda) = \operatorname{tr}\left(\rho \sum_{\lambda\in\sigma(\mathcal{O})} \lambda P_\lambda\right) = \operatorname{tr}(\rho\mathcal{O}),$$

as one would expect. The our question amounts to whether we demand that, after applying our compression-decompression-channel T, only the expectation values should not change (i.e. $\mathbb{E}_\rho(\mathcal{O}) = \mathbb{E}_\rho(T(\mathcal{O}))$ for all ρ, thus $\mathcal{O} \in \operatorname{fix} T$), or the exact statistics, i.e. all measurement outcome probabilities $\mathbb{P}_\rho[\mathcal{O} \doteq \lambda]$ shall be equal. The latter translates to the requirement $\{P_\lambda \mid \lambda \in \sigma(\mathcal{O})\} \subset \operatorname{fix} T$. Clearly the latter implies the former, since the fixed points form a linear subspace. On the other hand, the $*$-algebra generated by them is the same, since every eigenprojections P of a self-adjoint operator $\mathcal{O}$ can be represented by a polynomial of $\mathcal{O}$.

4.2. Algorithmic construction of compression maps

Here we state an explicit algorithm for finding optimal compression channels for given fixed points – and thus in particular the compression dimension. For another optimised version using semidefinite programming, see [BRW, Algorithm 1 on p. 23].

Algorithm 4.7 (Compression with classical side channel). *Let the Hilbert space $\mathcal{H} = \mathbb{C}^d$, a self-adjoint subspace $\mathcal{F} \subset \mathscr{L}(\mathcal{H}) = \mathcal{M}_d$ with $\mathrm{id}_\mathcal{H} \in \mathcal{F}$, and a "positivity parameter" $m \in \{3/2, 2, 3, 4, \dots\}$ be given. We want to determine $\operatorname{qdim}_m(\mathcal{F})$ by constructively find a compression triple*[4] *$(\mathfrak{S}, \mathfrak{I}, \Phi)$ satisfying $\mathfrak{A} := *{-}\mathrm{Alg}(\mathcal{F}) = \mathfrak{S} \oplus \mathfrak{I}$ and $\mathcal{F} \subseteq \tilde{\mathcal{F}} := \{S + \Phi(S) \mid S \in \mathfrak{S}\}$, where the dimension of $\mathfrak{S}$ shall be as small as possible and Φ is m-positive*[5].

Step 1. *Calculate*[6] *$\mathfrak{A} := *{-}\mathrm{Alg}(\mathcal{F})$ and determine its standard form, i.e. find a unitary matrix $U \in \mathcal{U}(d)$, such that the conjugated algebra $\mathfrak{A}_1 := U\mathfrak{A}U^\dagger$ decomposes into the direct product of matrix algebras*

$$\mathfrak{A}_1 = \bigtimes_{j=1}^{n} \mathcal{M}_{d_j} \otimes \mathbb{I}_{\nu_j}$$

for suitable numbers $d_1, \dots, d_n$ and $\nu_1, \dots, \nu_n$. Set $\mathcal{F}_1 := U\mathcal{F}U^\dagger$.

[4] Recall that this means that $\psi := (\mathrm{id}_\mathfrak{S} + \Phi) \circ \mathrm{Proj}_\mathfrak{S}$ is an m-positive, unital and idempotent Schwarz map with fixed point set $\operatorname{fix}\psi = \tilde{\mathcal{F}}$.

[5] Note that for $m \geq d$ this means that Φ is completely positive.

[6] To find out what $*{-}\mathrm{Alg}(\mathcal{F})$ is, it may help to remember that by the double commutant theorem it is equal to $\mathcal{F}''$.

Step 2. *Obviously, those blocks with $\nu_j > 1$ can be easily compressed, namely by "forgetting" the redundant blocks. More precisely, we set* $\mathfrak{A}_2 := \bigtimes_{j=1}^{n} \mathcal{M}_{d_j}$ *and make use of the natural $*$-isomorphism* $V : \mathfrak{A}_1 \longrightarrow \mathfrak{A}_2$ *acting by* $(A_1 \otimes \mathbb{I}_{\nu_1}, \dots, A_n \otimes \mathbb{I}_{\nu_n}) \longmapsto (A_1, \dots, A_n)$ *for* $A_j \in \mathcal{M}_{d_j}$*. The new "fixed points" then have to be* $\mathcal{F}_2 := V(F_1)$*. Note that* $\mathfrak{A}_2$ *operates on a Hilbert space of dimension* $\sum_{j=1}^{n} d_j$*, whereas* $\mathfrak{A}_1$ *operated on* $\mathbb{C}^d$*, where* $d = \sum_{j=1}^{n} d_j \cdot \nu_j$*.*

Remark. We could have merged Step 1 and Step 2 into one Step consisting of finding a $*$-isomorphism $\tilde{V} : \mathfrak{A} \longrightarrow \mathfrak{A}_2$ such that $\mathfrak{A} = \bigtimes_{j=1}^{n} \mathcal{M}_{d_j}$, and setting $\mathcal{F}_2 = \tilde{V}(\mathcal{F})$.

Step 3. *For* $j \in \{1, \dots, n\}$*, let* $\mathcal{B}_j$ *denote the direct summand in* $\mathfrak{A} = \bigoplus_{j=1}^{n} \mathcal{B}_j$ *corresponding to the* $\mathcal{M}_{d_j}$*-block algebra*[7]*. In this crucial step we want to find a selection of blocks that shall belong to* $\mathfrak{S}$*, with its dimension is as small as possible, so that the existence of the desired compression triple can be achieved. In other words, we want to minimise the expression* $D(\mathcal{I}) := \max_{j \in \mathcal{I}} d_j$ *over the "variable"* $\mathcal{I} \in 2^{\{1,\dots,n\}}$ *under the following constraints:*

$$\begin{cases} \text{There is a compression triple } (\mathfrak{S}, \mathfrak{I}, \Phi) \text{ for } \mathfrak{A}_2 \text{ such that} \\ \mathfrak{S} = \bigoplus_{j \in \mathcal{I}} \mathcal{B}_j, \ \Phi \text{ is } m\text{-positive, and } \mathcal{F}_2 \subseteq \{S + \Phi(S) \mid S \in \mathfrak{S}\} \end{cases} \tag{$\star$}$$

As a first step, by dimensional reasoning we can rule out subsets $\mathcal{I}$ *where* $\sum_{j \in \mathcal{I}} d_j^2 < \dim \mathcal{F}_2$*. Then, we can sort the remaining candidates for* $\mathcal{I}$ *according to the number* $D(\mathcal{I})$ *and, beginning with one of the* $\mathcal{I}$ *which has the lowest* $D(\mathcal{I})$*, check via the following procedure, if* $\mathcal{I}$ *is satisfies the constraints.*

1. *Set* $\mathfrak{S} := \bigoplus_{j \in \mathcal{I}} \mathcal{B}_j$*,* $\mathfrak{I} := \bigoplus_{j \notin \mathcal{I}} \mathcal{B}_j$ *and consider the operator system* $\mathfrak{S}_{\mathcal{F}} := \operatorname{Proj}_{\mathfrak{S}} \mathcal{F}_2 = 1_{\mathfrak{S}} \mathcal{F}_2 \subseteq \mathfrak{S}$*. Check, whether the following equivalent conditions are satisfied or not:*
   - *i)* $\forall\, S \in \mathfrak{S}_{\mathcal{F}} \quad \exists!\, I \in \mathfrak{I} : \quad S + I \in \mathcal{F}_2$
   - *ii)* $\mathfrak{I} \cap \mathcal{F}_2 = \{0\}$
   - *iii)* $\operatorname{Proj}_{\mathfrak{S}}$*, restricted to* $\mathcal{F}_2$*, is injective.*
   - *iv)* $\dim \mathcal{F}_2 = \dim \mathfrak{S}_{\mathcal{F}}$*.*
2. *If one (and then all) of the above conditions is not satisfied, then* $\mathcal{I}$ *does not fulfil* $(\star)$*, so we proceed with the next choice of* $\mathcal{I}$*. Otherwise, we define a map* $\tilde{\Phi} : \mathfrak{S}_{\mathcal{F}} \longrightarrow \mathfrak{I}$ *in the following way: For* $S \in \mathfrak{S}_{\mathcal{F}}$*,* $\tilde{\Phi}(S)$ *shall be the unique element* $I \in \mathfrak{I}$*, such that* $S + I \in \mathcal{F}_2$ *(well-defined per condition (i)). Note, that* $\tilde{\Phi}$ *can be written as* $\tilde{\Phi} = \operatorname{Proj}_{\mathfrak{I}} \circ \pi^{-1}$*, where* $\pi : \mathcal{F}_2 \longrightarrow \mathfrak{S}_{\mathcal{F}}$ *is given by* $\operatorname{Proj}_{\mathfrak{S}}$ *on its domain.*
3. *Check, if* $\tilde{\Phi}$ *is m-positive. If not,* $\mathcal{I}$ *does not fulfil* $(\star)$*, so pick the next candidate.*
4. *Check if* $\tilde{\Phi}$ *can be extended to an m-positive map* $\Phi : \mathfrak{S} \longrightarrow \mathfrak{I}$ *. If this is not the case,* $\mathcal{I}$ *does not fulfil* $(\star)$*, so try the next candidate. Otherwise, we have found an optimal candidate* $\mathcal{I}$ *that satisfies* $(\star)$*. Go to step 4!*

[7] More formally, $\mathcal{B}_j = \{(A_1, \dots, A_n) \in \mathfrak{A}_2 \mid A_k = 0 \text{ for } k \neq j\}$.

Step 4. *We have found a compression triple* $(\mathfrak{S}, \mathfrak{I}, \Phi)$ *for* $\mathfrak{A}_2$ *where* $\mathfrak{S} = \bigoplus_{j\in\mathcal{I}} \mathcal{B}_j$, $\Phi : \mathfrak{S} \longrightarrow \mathfrak{I}$ *is* m*-positive, and* $\mathcal{F}_2 \subseteq \{S + \Phi(S) \mid S \in \mathfrak{S}\}$ *with the lowest possible* $d := D(\mathcal{I})$*. Since* $\mathfrak{S}$ *has quantum dimension* d *by Proposition 4.5, we have* $\operatorname{qdim}_m(\mathcal{F}_2) = d$ *by Proposition 4.3.*

If one is interested in the actual compression maps, one has to use compression maps $D_{\mathfrak{S}} : \mathfrak{S} \longrightarrow \mathcal{M}_d \otimes \mathcal{D}_e$ *and*[8] $E_{\mathfrak{S}} : \mathcal{M}_d \otimes \mathcal{D}_e \longrightarrow \mathfrak{S}$ *from Proposition 4.5: let* $D_2 : \mathfrak{A}_2 \longrightarrow \mathcal{M}_d \otimes \mathcal{D}_e$ *be defined by* $D_2 := D_{\mathfrak{S}} \circ \operatorname{Proj}_{\mathfrak{S}}$*, and* $E_2 : \mathcal{M}_d \otimes \mathcal{D}_e \longrightarrow \mathfrak{A}_2$ *defined by* $E_2 := (\mathrm{id}_{\mathfrak{S}} + \Phi) \circ E_{\mathfrak{S}}$*. To "transform back" Steps 1 and 2 we finally take* $D(X) := D_2\big(V(UXU^\dagger)\big)$ *and* $E(Y) = U^\dagger \cdot \big[V^{-1} \circ E_2\big](Y) \cdot U$*.*

Proof of the claims made in algorithm 4.7. First we note, that the existence part of (i) is always fulfilled by construction: For Let $S \in \mathfrak{S}_{\mathcal{F}}$, say $S = \operatorname{Proj}_{\mathfrak{S}} F$ for some element $F \in \mathcal{F}_2$, the element $I := \operatorname{Proj}_{\mathfrak{I}} F$ satisfies $S + I = F \in \mathcal{F}_2$. Now we show that the statements (i) - (iv) are equivalent. Throughout this proof let us denote the restriction of the projection onto $\mathfrak{S}$ by $\pi : \mathcal{F}_2 \longrightarrow \mathfrak{S}_{\mathcal{F}}$, $\pi(F) = \operatorname{Proj}_{\mathfrak{S}} F$.

"*(i)* ⇒ *(ii)*". Setting $S = 0$ in (i), there exists a unique $I \in \mathfrak{I}$ such that $I \in \mathcal{F}_2$; in other words: the intersection $\mathfrak{I} \cap \mathcal{F}_2$ contains exactly one element, which obviously must be 0.

"*(ii)* ⇒ *(i)*". Let $S \in \mathfrak{S}_{\mathcal{F}}$ be given, and suppose that there are $I_1, I_2 \in \mathfrak{I}$ such that $S + I_1 \in \mathcal{F}_2$ and $S + I_2 \in \mathcal{F}_2$. Then their difference $S + I_1 - (S + I_2) = I_1 - I_2$ lies in $\mathfrak{I}$ and in $\mathcal{F}_2$, hence is zero by (ii).

"*(ii)* ⇔ *(iii)*" follows from

$$\ker \pi = \{F \in \mathcal{F}_2 \mid \pi(F) = 0\} = \{F \in \mathcal{F}_2 \mid F \in \mathfrak{I}\} = \mathfrak{I} \cap \mathcal{F}_2.$$

Finally, "*(iii)* ⇔ *(iv)*" is obvious, noting that all vector spaces involved are finite dimensional. ☐

4.3. Lossy Compression: an outlook

In this final section, we want to give an outlook for what happens, if we weaken the restriction that chosen effects shall be preserved without error. First, we determine which norms are good candidates to measure the error which is done when compressing and decompressing the effects. In the whole chapter, let $\mathcal{H}$ be a finite-dimensional Hilbert space ($\dim \mathcal{H} =: d$) describing the quantum mechanical system that we want to compress.

Let us assume that we want to preserve the observable Q with minimal error; i.e. the expected value of Q in all possible states $\rho \in \mathscr{S}(\mathcal{H})$ shall not differ too much after applying our channel T. Note that if Q is an effect, then the expectation value of Q is exactly the probability that the effect triggers. Mathematically, we thus want

$$\forall \rho \in \mathcal{S}(\mathcal{H}) : \quad \operatorname{tr}(\rho Q) \approx \operatorname{tr}(\rho T(Q))\,.$$

This motivates the following definition for a measuring the error we can make in the worst case by applying our compression procedure T.

[8] Recall that $\mathcal{D}_n$ denotes the von Neumann algebra of diagonal complex $n \times n$-matrices.

Definition 4.8. For $A \in \mathcal{E}(\mathcal{H})$ we define

$$\Delta(A) := \max_{\rho \in \mathcal{S}(\mathcal{H})} |\mathrm{tr}\,(\rho A) - \mathrm{tr}\,(\rho T(A))|\,.$$

Lemma 4.9. *For $A \in \mathcal{E}(\mathcal{H})$ we have $\Delta(A) = \left\| \left(\mathrm{id}_{\mathscr{L}(\mathcal{H})} - T\right)(A) \right\|$.*

Proof. "$\leq$". For $\rho \in \mathscr{S}(\mathcal{H})$ we can estimate

$$\begin{aligned} |\mathrm{tr}\,(\rho A) - \mathrm{tr}(\rho T(A))| &= |\mathrm{tr}\,(\rho(A - T(A)))| \leq \mathrm{tr}\,|\rho(A - T(A)| \\ &= \|\rho(A - T(A))\|_1 \leq \|\rho\|_1 \cdot \|A - T(A)\| = \|A - T(A)\|\,, \end{aligned}$$

where $\|\cdot\|_1$ denotes the trace norm $X \mapsto \mathrm{tr}\,|X| = \mathrm{tr}\sqrt{X^\dagger X}$, which is a special case of the Schatten-p-norms ($p \in [1; +\infty]$) $\|X\|_p = \left(\mathrm{tr}([X^* X]^{p/2}\right)^{1/p}$, and where we used a generalised Hölder inequality $\|XY\|_1 \leq \|X\|_p \|Y\|_q$, if $1/p + 1/q = 1$. Note that for $p = +\infty$ we retain the usual operator norm, which is also the $\mathcal{C}^*$-norm.

"$\geq$". Set $B := A - T(A)$, which is hermitian, hence by the spectral theorem can be written

$$B = \sum_{j=1}^{d} \lambda_j \, |e_j\rangle\langle e_j|\,, \quad \lambda_j \in \mathbb{R}, \quad (e_j) \text{ ONB of } \mathcal{H}.$$

Pick $\ell \in \{1, \ldots, d\}$ such that $|\lambda_\ell| = \max_{j=1}^{d} |\lambda_j|$. We choose $\rho := |e_\ell\rangle\langle e_\ell| \in \mathscr{S}(\mathcal{H})$ and evaluate the trace explicitly:

$$\begin{aligned} \Delta(A) &\geq |\mathrm{tr}(\rho A) - \mathrm{tr}(\rho T(A))| = |\mathrm{tr}(\rho B)| \\ &= \mathrm{tr}\,(|e_\ell\rangle\langle e_\ell|\, B) = |\lambda_\ell| = \|B\| = \|A - T(A)\|\,. \end{aligned}$$

□

Lemma 4.9 suggests that the problem of compressing a quantum system while retaining certain measurement outcomes within some error bounds can be seen as an optimisation problem. The task is to optimise the numbers $\Delta(Q)$ where we can vary the channel T. In general, we may want to add further restrictions on T (e.g. special structure such as $E \circ D$, where D maps to a Hilbert space of smaller dimension than d), because in the general case $T = \mathrm{id}_{\mathscr{L}(\mathcal{H})}$ is a trivial optimal point with $\Delta \equiv 0$.

Note that the set of quantum channels

$$\{T : \mathscr{L}(\mathcal{H}) \longrightarrow \mathscr{L}(\mathcal{H}) \mid T \text{ } m\text{-positive and unital}\}$$

is a compact convex set ($m \in \{1, 3/2, 2, 3, 4, \ldots\} \cup \{\infty\}$) within a finite-dimensional vector space, so convex optimisation may be an appropriate tool.

Appendix A.

Proof of the von Neumann double commutant theorem

A.1. Preliminaries

Before we can prove the von Neumann double commutant theorem, we recall some basic notions from the subject of topological vector spaces, which we will not prove, and define certain topologies on $\mathscr{L}(\mathcal{H})$.

In the present version of the statement and proof of the von Neumann double commutant theorem, we will consider Hilbert spaces of arbitrary – i.e. possibly infinite – dimension. At one point in the proof we may use the concept of *nets*, so we assume some degree of familiarity on the part of the reader.

A.1.1. General Topology in terms of Nets

Definition A.1. A non-empty set D, equipped with a binary relation $\preceq$, is called *directed*, if it is partially ordered, i.e. for all $x, y, z \in D$ we have that

$$x \preceq x, \quad x \preceq y \wedge y \preceq x \implies x = y, \text{ and } x \preceq y \wedge y \preceq z \implies x \preceq z,$$

and additionally

$$\forall x, y \in D \;\exists z \in D: \quad z \succeq x \wedge z \succeq y.$$

If D is a directed set, X is a non-empty set, and $x : D \longrightarrow X$ is a function, then x is called a *net*. Usually we will write $x_\delta := x(\delta)$ for $\delta \in D$ and $(x_\delta)_{\delta \in D} := x$. If (X, τ) is a topological space, $(x_\delta)_{\delta \in D} \subseteq X$ a net and $x_0 \in X$, we say that $(x_\delta)_{\delta \in D}$ *converges* to x_0 (with respect to τ) – in symbols $x_\delta \to x_0$ – if for all neighbourhoods U of x_0, x_δ eventually lies in U, i.e.

$$\exists \delta_0 \in D \;\forall \delta \succeq \delta_0: \; x_\delta \in U.$$

Fact A.2. *Let (X, τ) be a topological space, $(x_\delta)_{\delta \in D} \subseteq X$ a net.*

i) *X is a Hausdorff space, iff every net $(x_\delta)_{\delta \in D} \subseteq X$ has at most one limit point.*

ii) *A is open in X (i.e. $A \in \tau$), iff for every net $(x_\delta)_{\delta \in D} \subseteq X$ that converges to some element of A we have $x_\delta \in A$ eventually.*

iii) *A is closed in X (i.e. $X \setminus A \in \tau$), iff it contains all limit points of convergent nets $(x_\delta) \subseteq A$.*

A.1.2. Topological Vector Spaces

For a topological space (X, τ) we will write $\mathfrak{U}(x)$ for the set containing all neighbourhoods of $x \in X$, i.e. $\mathfrak{U}(x) := \{O \subseteq X \mid O^\circ \ni x\}$, where O° denotes the interior of O. A collection $\mathscr{B} \subseteq \mathfrak{U}(x)$ is called a *neighbourhood basis for* $x \in X$, if, for every $U \in \mathfrak{U}(x)$, there is a set $B \in \mathscr{B}$ which is contained in U.

Recall the following notions from the subject of topological vector spaces: A *topological vector space* is a vector space X over a field $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ equipped with a topology τ, such that it is Hausdorff, and the addition map $+ : X \times X \longrightarrow X$ and the scalar multiplication map $\cdot : \mathbb{K} \times X \longrightarrow X$ are continuous (where $X \times X$ and $\mathbb{K} \times X$ are given the respective product topologies). Note that in a topological vector space, the *translation maps* $t_x : X \longrightarrow X$, $y \mapsto y + x$, are homeomorphisms (since they are continuous by definition and their inverse are given by $(t_x)^{-1} = t_{-x}$). Thus, t_x maps a neighbourhood basis for $y \in X$ onto a neighbourhood basis for $(x + y)$. Hence one only need to consider neighbourhood bases for one special point, e.g. 0, since it can be carried over to any other point $x \in X$ via t_x.

Let X be a $\mathbb{K}$-vector space. A map $p : X \longrightarrow [0, +\infty)$ is called *semi-norm*, if it is homogeneous (i.e. $p(\lambda x) = |\lambda|\, p(x)\ \forall \lambda \in \mathbb{K}\ \forall x \in X$) and satisfies the triangle inequality (i.e. $p(x+y) \leq p(x) + p(y)\ \forall x, y \in X$). A family $\mathcal{P}$ of semi-norms on a vector space X is called *separating*, if for each $x \in X \setminus \{0\}$, $\mathcal{P}$ contains a semi-norm p such that $p(x) \neq 0$.

Let $\mathcal{P}$ be a separating family of semi-norms on X. We say, that the topology τ on a topological vector space X is *induced by* $\mathcal{P}$, if the collection

$$U_\varepsilon^p := \{x \in X \mid p(x) < \varepsilon\}, \quad p \in \mathcal{P}, \quad \varepsilon > 0$$

forms a neighbourhood basis for 0. A basic fact from the subject of topological vector spaces is, that a topological vector space is locally convex (i.e. admits a neighbourhood basis for 0 consisting of convex sets), iff its topology is induced by a separating collection of semi-norms.

In finite dimensions all relevant topologies on a vector space are actually the same: the following result is a special case of [Sch, Ch. I, 3.2 on p.21].

Fact A.3. *Let $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ and let X be an n-dimensional ($n \in \mathbb{N}$) topological vector space over $\mathbb{K}$. Then X is homeomorphic to $\mathbb{K}^n$.*

In particular this means that for finite-dimensional X, there is a unique topology τ on X that renders (X, τ) a topological vector space; and $\mathbb{K}^n$ is the only n-dimensional topological vector space over $\mathbb{K}$, up to homeomorphisms.

As the von Neumann double commutant theorem regards closures of subsets of topological vector spaces, we will use the following criterion, which follows directly from the definitions:

Fact A.4. *Let X be a topological space, and let $\mathscr{B}$ be a neighbourhood basis for $x \in X$. Then, for $A \subseteq X$, we have the equivalence*

$$x \in \overline{A} \iff \forall B \in \mathscr{B} :\ A \cap B \neq \emptyset,$$

where $\overline{A}$ denotes the (topological) closure of A.

A.1.3. Topologies on $\mathscr{L}(\mathcal{H})$

On $\mathscr{L}(\mathcal{H})$, we consider the following topologies:

- The *(operator) norm topology* is induced by the operator norm

$$\mathscr{L}(\mathcal{H}) \ni A \mapsto \|A\| = \sup_{\|x\|=1} \|Ax\| .$$

- The *strong operator topology* is induced by the family of semi-norms

$$\mathcal{P}_{\text{strong}} := \{\mathscr{L}(\mathcal{H}) \ni A \mapsto \|Ax\| \mid x \in \mathcal{H}\} .$$

- The *weak operator topology* is induced by the family of semi-norms

$$\mathcal{P}_{\text{weak}} := \{\mathscr{L}(\mathcal{H}) \ni A \mapsto |\langle y|Ax\rangle| \mid x, y \in \mathcal{H}\} .$$

Using nets, one can classify convergence w.r.t. the above topologies as follows:

- A net $(A_\delta) \subset \mathscr{L}(\mathcal{H})$ *converges in norm* to $A \in \mathscr{L}(\mathcal{H})$, iff $\|A_\delta - A\| \to 0$.
- A net $(A_\delta) \subset \mathscr{L}(\mathcal{H})$ *converges strongly* (i.e., w.r.t. the strong operator topology) to $A \in \mathscr{L}(\mathcal{H})$, iff $A_\delta x \to Ax$ for all $x \in X$.
- A net $(A_\delta) \subset \mathscr{L}(\mathcal{H})$ *converges weakly* (i.e., w.r.t. the weak operator topology) to $A \in \mathscr{L}(\mathcal{H})$, iff $\langle y|A_\delta x\rangle \to \langle y|Ax\rangle$ for all $x, y \in X$.

A.1.4. Unitality and Degeneracy

Definition A.5. We call a $*$-sub-algebra $\mathscr{A}$ of $\mathscr{L}(\mathcal{H})$ *non-degenerate,* if

$$\overline{\operatorname{span}\{A\xi \mid A \in \mathscr{A},\, \xi \in \mathcal{H}\}} = \mathcal{H}.$$

We say that $\mathscr{A}$ *has trivial null space*, if

$$\bigcap_{A \in \mathscr{A}} \ker A = \{0\}.$$

Lemma A.6. *Let $\mathscr{A}$ be a $*$-subalgebra of $\mathscr{L}(\mathcal{H})$.*

i) *$\mathscr{A}$ furnishes a decomposition of $\mathcal{H}$ into the direct sum of the two orthogonal closed subspaces*

$$X := \bigcap_{A \in \mathscr{A}} \ker A \quad \textit{and} \quad Y := \overline{\operatorname{span}\{A\xi \mid A \in \mathscr{A},\, \xi \in \mathcal{H}\}}.$$

In particular, $\mathscr{A}$ is non-degenerate, iff it has trivial null space.

ii) *The set*

$$\mathscr{B} := \{\mathrm{Proj}_Y \circ A \circ \mathrm{Proj}_Y \mid A \in \mathscr{A}\} = \{A_{\restriction Y} : Y \longrightarrow Y \mid A \in \mathscr{A}\}$$

is a non-degenerate $*$-algebra in the Hilbert space Y, which is $*$-isomorphic to $\mathscr{A}$. Moreover, if $\mathscr{A}$ is strongly closed, then so is $\mathscr{B}$.

Proof. i) X is closed as intersection of closed sets, and Y is inherently closed. We show $Y^\perp = X$:

$$\begin{aligned} Y^\perp &= \left(\overline{\mathrm{span}\mathscr{A}\mathcal{H}}\right)^\perp = (\mathrm{span}\mathscr{A}\mathcal{H})^\perp = (\mathscr{A}\mathcal{H})^\perp = \left(\bigcup_{A\in\mathscr{A}} \operatorname{ran} A\right)^\perp \\ &= \bigcap_{A\in\mathscr{A}} (\operatorname{ran} A)^\perp = \bigcap_{A\in\mathscr{A}} \ker A^* = \bigcap_{A\in\mathscr{A}} \ker A = X. \end{aligned}$$

It follows that $Y = \mathcal{H}$ is equivalent to $X = \{0\}$, so $\mathscr{A}$ is non-degenerate, iff it has trivial null space.

ii) As a closed subspace of $\mathcal{H}$, Y is complete, hence a Hilbert space in its own right. Consider the restriction map

$$\phi : \begin{array}{ccc} \mathscr{A} & \longrightarrow & \mathscr{L}(Y) \\ A & \longmapsto & A_{\restriction Y} \end{array},$$

which is well-defined, since for $A \in \mathscr{A}$ we have

$$\operatorname{ran} A = (\ker A^*)^\perp \subseteq \left(\bigcap_{B\in\mathscr{A}} \ker B\right)^\perp = X^\perp = Y.$$

By definition of $\mathscr{B}$, ϕ is surjective, and it is easy to check that ϕ is a bijective $*$-homomorphism. Hence $\mathscr{B}$ is a $*$-algebra, which is non-degenerate, since it has trivial null space; indeed,

$$\begin{aligned} \bigcap_{B\in\mathscr{B}} \ker B &= \{\xi \in Y \mid B\xi = 0\,\forall B \in \mathscr{B}\} = \{\xi \in Y \mid A_{\restriction Y}\xi = 0\,\forall A \in \mathscr{A}\} \\ &= \{\xi \in Y \mid A\xi = 0\,\forall A \in \mathscr{A}\} = Y \cap X = \{0\}. \end{aligned}$$

Finally, assume in addition that $\mathscr{A}$ is strongly closed. We show that $\mathscr{B}$ is strongly closed, too. To that aim, let $(B_\delta) \subset \mathscr{B}$ be a net with $B_\delta \to B \in \mathscr{L}(Y)$ strongly, i.e. $\|(B_\delta - B)\eta\| \to 0$ for all $\eta \in Y$. We set $A_\delta = \phi^{-1}(B_\delta) \in \mathscr{A}$, and by extending the strong limit operator B to $A \in \mathscr{L}(\mathcal{H})$, defined by $A(\xi + \eta) = B\eta$ for $\xi \in X$, $\eta \in Y$. Then for $\xi \in X$, $\eta \in Y$ we have that $\|(A_\delta - A)(\xi + \eta)\| = \|(B_\delta - B)\eta\| \to 0$. So A_δ converges to A strongly, and since $\mathscr{A}$ is strongly closed, we infer that $A \in \mathscr{A}$. Noting that $\mathscr{B} \ni \phi(A) = A_{\restriction Y} = B$ completes the proof. □

A.2. Statement and proof

The statement and proof of the present version of the double commutant theorem is inspired by [Dix, Ch. I.3.4] and [Arv3, Ch. 1.2]. It shall state the following:

Theorem A.7 (J. von Neumann's double commutant theorem)**.** *Let $\mathscr{A}$ be a $*$-algebra of operators on the Hilbert space $\mathcal{H}$. Assume that $\mathscr{A}$ is strongly closed.*

Then $\mathscr{A}$ has a unit element P, which is the greatest projection in $\mathscr{A}$ and is equal to the orthogonal projection onto the subspace

$$Y := \overline{\operatorname{span}\{A\xi \mid A \in \mathscr{A},\ \xi \in \mathcal{H}\}} \subseteq \mathcal{H}.$$

Moreover, the double commutant of $\mathscr{A}$ is given by

$$\mathscr{A}'' = \mathscr{A} + \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}.$$

In particular, $\mathscr{A}$ is a von Neumann algebra, iff it contains $\mathrm{id}_{\mathcal{H}}$.

We firstly prove Theorem A.7 under the additional assumption of $\mathscr{A}$ being non-degenerate. In this case the first part becomes somewhat easier (since $P = \mathrm{id}_{\mathcal{H}}$), and the hard part to prove is the following statement:

Lemma A.8. *Let $\mathscr{A}$ be a non-degenerate $*$-algebra on the Hilbert space $\mathcal{H}$. Then $\mathscr{A}'' \subseteq \overline{\mathscr{A}}^{\text{strong}}$, i.e. every element in the double commutant of $\mathscr{A}$ lies in the strong closure of $\mathscr{A}$.*

Proof. Let $X \in \mathscr{A}''$. By definition of the strong operator topology, the collection

$$\mathscr{U} := \left\{ \bigcap_{j=1}^{n} U_{\varepsilon_j}^{p_{\xi_j}}(X) \,\middle|\, n \in \mathbb{N},\, \varepsilon_j > 0,\, \xi_j \in \mathcal{H} \right\},$$

where $U_{\varepsilon}^{p_\xi}(X) := \{A \in \mathscr{L}(\mathcal{H}) \mid \|(A - X)\xi\| < \varepsilon\}$, forms a finitely $\cap$-stable neighbourhood basis around $X \in \mathscr{L}(\mathcal{H})$ w.r.t. the strong topology. By Fact A.4 it thus suffices to show that X lies in every $U \in \mathscr{U}$.

Let us first treat the case $n = 1$, so let $\xi \in \mathcal{H}$ and $\varepsilon > 0$ be given. We define the closed subspace $Y := \overline{\mathscr{A}\xi} \subseteq \mathcal{H}$, let $P := \mathrm{Proj}_Y \in \mathscr{L}(\mathcal{H})$ denote the orthogonal projection onto Y, and claim that $P \in \mathscr{A}'$. Indeed, for any $\eta \in \mathcal{H}$ we can write $P\eta \in Y$ as the limit $P\eta = \lim_{k\to\infty} A_k\xi$ for a suitable sequence $(A_k)_{k\in\mathbb{N}} \subset \mathscr{A}$, so we have for all $B \in \mathscr{A}$ that

$$BP\eta = B \lim_{k\to\infty} A_k\xi = \lim_{k\to\infty} \underbrace{BA_k}_{\in\mathscr{A}} \xi \in Y;$$

hence $BP\eta = PBP\eta$. As η and B were arbitrary, we conclude that $BP = PBP$ for all $B \in \mathscr{A}$. Taking adjoints and replacing B by B^* yields $PB = PBP$ for all $B \in \mathscr{A}$, which together implies $BP = PBP = PB$ for all $B \in \mathscr{A}$, whence $P \in \mathscr{A}'$. In particular we obtain $XP = PX$ (since $X \in \mathscr{A}''$).

Next, we claim that $P\xi = \xi$. Indeed, for any $A \in \mathscr{A}$ we have (since $P \in \mathscr{A}'$)

$$\underbrace{A\xi}_{\in Y} = PA\xi = AP\xi \quad \Longrightarrow \quad A(\mathrm{id}_{\mathcal{H}} - P)\xi = 0,$$

so $(\mathrm{id}_{\mathcal{H}} - P)\xi \in \bigcap_{A\in\mathscr{A}} \ker A = \{0\}$, for $\mathscr{A}$ is non-degenerate and therefore has trivial null space. This shows $\xi = P\xi$.

Putting the two proceeding steps together, we get $X\xi = XP\xi = PX\xi \in Y = \overline{\mathscr{A}\xi}$, hence there exists $A \in \mathscr{A}$ satisfying $\|X\xi - A\xi\| < \varepsilon$. This completes the case $n = 1$.

Now, we reduce the general case $n > 1$ to the case $n = 1$ by suitably enlarging our Hilbert space. Consider $\mathcal{K} := \mathcal{H}^n$, i.e. the n-fold Cartesian product of $\mathcal{H}$ with scalar product

$$\langle (x_1, \cdots, x_n) | (y_1, \cdots, y_n) \rangle_{\mathcal{K}} = \sum_{j=1}^{n} \langle x_j | y_j \rangle_{\mathcal{H}}\,.$$

The elements of $\mathscr{L}(\mathcal{K})$ can be represented canonically as matrices $(T_{ij})_{i,j=1}^{n}$ with $T_{ij} \in \mathscr{L}(\mathcal{H})$. We consider the $*$-algebra of operators

$$\mathscr{D} := \{\mathrm{diag}(A, \cdots, A) \in \mathscr{L}(\mathcal{K}) \mid A \in \mathscr{A}\}\,.$$

Obviously, $\mathscr{D}$ has trivial null space, iff $\mathscr{A}$ has. We calculate $\mathscr{D}'$ and $\mathscr{D}''$:

$$\begin{aligned}
(C_{ij}) \in \mathscr{D}' \quad &\Longleftrightarrow \quad \forall A \in \mathscr{A} :\ \mathrm{diag}(A, \cdots, A) \cdot (C_{ij}) = (C_{ij}) \cdot \mathrm{diag}(A, \cdots, A) \\
&\Longleftrightarrow \quad \forall A \in \mathscr{A} :\ (AC_{ij}) = (C_{ij}A) \\
&\Longleftrightarrow \quad C_{ij} \in \mathscr{A}' \quad \forall i, j \in \{1, \ldots, n\},
\end{aligned}$$

so $\mathscr{D}' = \mathrm{Mat}_n(\mathscr{A}')$. Moreover,

$$\begin{aligned}
(D_{ij}) \in \mathscr{D}'' \quad &\Longleftrightarrow \quad \forall\, (B_{ij}) \in \mathrm{Mat}_n(\mathscr{A}') :\ \cdot (B_{ij})\, (D_{ij}) = (D_{ij}) \cdot (B_{ij}) \\
&\Longleftrightarrow \quad \forall\, (B_{ij}) \in \mathrm{Mat}_n(\mathscr{A}') :\ \left(\sum_{k=1}^{n} B_{ik} D_{kj}\right) = \left(\sum_{k=1}^{n} D_{ik} B_{kj}\right).
\end{aligned}$$

Choosing $(B_{ij}) = (\delta_{il}\delta_{jm}\mathrm{id}_{\mathcal{H}})_{ij} \in \mathrm{Mat}_n(\mathscr{A}')$ for fixed $l, m \in \{1, \ldots, n\}$, we see that $(D_{ij}) \in \mathscr{D}''$ implies $\delta_{il} D_{mj} = D_{il}\delta_{jm}$ for all i, j, l, m. Taking $i = l = 1$, we see that $D_{mj} = D_{11}\delta_{jm}$ for all j and m. Hence (D_{ij}) must be of the form $\mathrm{diag}(E, \cdots, E)$ for some $E \in \mathscr{L}(\mathcal{H})$. Considering the last condition in the equivalence chain above, we actually can infer $E \in \mathscr{A}''$. Conversely, each operator matrix $\mathrm{diag}(E, \cdots, E)$ with $E \in \mathscr{A}''$ fulfils that condition; hence we conclude

$$\mathscr{D}'' = \big\{\mathrm{diag}(E, \cdots, E) \bigm| E \in \mathscr{A}''\big\}\,.$$

Now, given $\xi_1, \ldots, \xi_n \in \mathcal{H}$ and $\varepsilon_1, \ldots, \varepsilon_n > 0$, we set $\varepsilon := \min_{j=1}^{n} \varepsilon_j$ and $\xi := (\xi_1, \cdots, \xi_n) \in \mathcal{K}$. Applying the already established case $n = 1$ to $Z := \mathrm{diag}(X, \cdots, X) \in$

$\mathscr{D}''$, there exists an element $B = \operatorname{diag}(A, \cdots, A) \in \mathscr{D}$ such that $\|B\xi - Z\xi\|_{\mathcal{K}} < \varepsilon$. Writing this out explicitly, we get (Pythagoras)

$$\sum_{j=1}^{n} \|(A - X)\xi_j\|^2 < \varepsilon^2,$$

which by positivity of the summands implies $\|(A - X)\xi_j\| < \varepsilon \le \varepsilon_j$ for all $j \in \{1, \dots, n\}$, hence $A \in U_{\varepsilon_j}^{p_{\xi_j}}(X)$ for all j. □

Now we can finally prove the full double commutant theorem:

Proof of von Neumann's double commutant theorem. We denote the subspace under consideration as

$$Y := \overline{\operatorname{span}\{A\xi \mid A \in \mathscr{A},\ \xi \in \mathcal{H}\}} = \overline{\operatorname{span} \bigcup_{A \in \mathscr{A}} \operatorname{ran} A} \subseteq \mathcal{H},$$

and let $P := \operatorname{Proj}_Y \in \mathscr{L}(\mathcal{H})$ denote the orthogonal projection onto Y.[1] By Lemma A.6ii),

$$\mathscr{B} := \{P \circ A \circ P \mid A \in \mathscr{A}\} = \{A_{\restriction Y} : Y \longrightarrow Y \mid A \in \mathscr{A}\}$$

is a strongly closed, non-degenerate $*$-algebra.

We apply lemma A.8 to $\mathscr{B}$ and get $\mathscr{B}'' \subseteq \mathscr{B}$, in particular $P_{\restriction Y} = \mathrm{id}_Y \in \mathscr{B}'' \subseteq \mathscr{B}$. Note that the restriction map $\phi : \mathscr{A} \longrightarrow \mathscr{B}$, $A \mapsto A_{\restriction Y}$ is a $*$-isomorphism by Lemma A.6ii), and that id_Y is the unit element and the greatest projection of $\mathscr{B}$. Hence $I := \phi^{-1}(\mathrm{id}_Y) \in \mathscr{A}$ is the unit element and greatest projection of $\mathscr{A}$ (cf. Note 1.26). Using the decomposition $\mathcal{H} = X \oplus Y$ from Lemma A.6i), we see that $I_{\restriction Y} = \mathrm{id}_Y$, and $I_{\restriction X} = 0$ (as $X = \cap_{A \in \mathscr{A}} \ker A$), so we obtain $P = I \in \mathscr{A}$.

We finally prove $\mathscr{A}'' = \mathscr{A} + \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}$. The "$\supseteq$"-direction is clear; so in order to prove "$\subseteq$", we consider the non-degenerate $*$-algebra of operators $\tilde{\mathscr{A}} := \mathscr{A} + \mathbb{C} \cdot \mathrm{id}_{\mathcal{H}}$. We claim that $\tilde{\mathscr{A}}$ is strongly closed. If $\mathrm{id}_{\mathcal{H}} \in \mathscr{A}$, then $\tilde{\mathscr{A}} = \mathscr{A}$ and there is nothing to show, so we consider the case $\mathrm{id}_{\mathcal{H}} \notin \mathscr{A}$. Note that this means that $X \neq \{0\}$. Consider a net $(A_\delta + \lambda_\delta \mathrm{id}_{\mathcal{H}})_\delta \subseteq \tilde{\mathscr{A}}$ that strongly converges to $C \in \mathscr{L}(\mathcal{H})$. Using Lemma A.6i) again, we get for $\xi \in X$ that $A_\delta \xi = 0$ by Lemma A.6i), so $\lambda_\delta \xi \to C\xi$ for all $\xi \in X$, which is only possible if λ_δ converges to some $\lambda \in \mathbb{C}$. But then, $A_\delta = (A_\delta + \lambda_\delta \mathrm{id}_{\mathcal{H}}) - \lambda_\delta \mathrm{id}_{\mathcal{H}}$ converges strongly to $C - \lambda \mathrm{id}_{\mathcal{H}}$, which lies in $\mathscr{A}$ by strong closedness. Hence $C = \underbrace{(C - \lambda \mathrm{id}_{\mathcal{H}})}_{\in \mathscr{A}} + \lambda \mathrm{id}_{\mathcal{H}} \in \tilde{\mathscr{A}}$, so $\tilde{\mathscr{A}}$ is strongly closed.

Obviously we have $\tilde{\mathscr{A}}' = \mathscr{A}'$, hence $\tilde{\mathscr{A}}'' = \mathscr{A}''$. So lemma A.8 applied to $\tilde{\mathscr{A}}$ yields $\mathscr{A}'' = \tilde{\mathscr{A}}'' \subseteq \tilde{\mathscr{A}}$. □

[1] Mind that, by now, we don't know whether P lies in $\mathscr{A}$.

Bibliography

[Arv1] Arveson, W. B.: Subalgebras of C^*-Algebras, Acta Math. 123 (1969), 141–224

[Arv2] Arveson, W.: Subalgebras of C^*-Algebras. II, Acta Math. 128 (1972), 271–308

[Arv3] Arveson, W.: An Invitation to C*-Algebras, Springer, New York–Heidelberg–Berlin, 1976

[Bar] Bargmann, V.: Note on Wigner's Theorem on Symmetry Operations, Journal of Mathematical Physics, 5 (7): 862, 1964

[BRW] Bluhm, A., Rauber, L., Wolf, M. M.: Quantum compression, relative to a set of measurements, Ann. Henri Poincaré (2018) 19: 1891, arXiv:1708.04898

[Dix] Dixmier, J.: Von Neumann Algebras, Translated from the second French edition by F. Jellett, North-Holland Publishing Co., Amsterdam–New York, 1981

[Lan] Lang, S.: Algebra, Revised Third Edition, Springer, New York, 2002

[Key] Keyl, M.: Fundamentals of Quantum Information Theory, arXiv:quant-ph/0202122, 1 Feb 2008

[Kra] Kraus, K.: States, Effects, and Operations, Springer, Berlin-Heidelberg-New York-Tokyo, 1983

[Lud] Ludwig, G.: Foundations of Quantum Mechanics I, Springer, New York-Heidelberg-Berlin, 1983

[Pau] Paulsen, V.: Completely Bounded Maps and Operator Algebras, Cambridge University Press, 2003

[Pre] Preskill, J.: Lecture Notes for Ph219/CS219: Quantum Information, Chapter 3, available at http://www.theory.caltech.edu/people/preskill/ph219/chap3_15.pdf, Updated July 2015

[PWPR] Perez-Garcia, D., Wolf, M. M., Petz, D., Ruskai, M. B.: Contractivity of positive and trace preserving maps under L_p norms, J. Math. Phys. 47, 083506 (2006), arXiv:math-ph/0601063, 30 Jan 2006

[Sch] Schaefer, H. H.: Topological Vector Spaces, Third Printing Corrected, Springer, New York–Heidelberg–Berlin, 1971

[Tak] Takesaki, M.: Theory of Operator Algebras I, 1st ed., Springer, New York–Heidelberg–Berlin, 1979

[Wol] Wolf, M. M.: Quantum channels and operations, Lecture notes available at http://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf, 2012

Erklärung

Ich versichere hiermit an Eides statt, dass ich die vorliegende Arbeit selbstständig angefertigt und ohne fremde Hilfe verfasst habe, keine außer den von mir angegebenen Hilfsmitteln und Quellen dazu verwendet habe und die den benutzten Werken inhaltlich und wörtlich entnommenen Stellen als solche kenntlich gemacht habe.

Lahnau, den 27. August 2018