Quantum Error Correction - Notes

Ben Karsberg

2021-22

1 von Neumann Algebras

- At some point, we will need the theory of *von Neumann algebras*, finite dimensional ones only
- Let's go through this
- Suppose $\mathcal{H}$ is a finite-dimensional Hilbert space, and denote the set of linear operators on $\mathcal{H}$ as $\mathcal{L}(\mathcal{H})$
- We denote the identity on $\mathcal{H}$ as $I \in \mathcal{L}(\mathcal{H})$

  Definition 1.1 (von Neumann algebra)**.** A **von Neumann algebra** on $\mathcal{H}$ is a set $M \subseteq \mathcal{L}(\mathcal{H})$ such that:

  - $\forall \lambda \in \mathbb{C},\ \lambda I \in M$
  - $\forall x \in M,\ x^\dagger \in M$
  - $\forall x,\ y \in M,\ xy \in M$
  - $\forall x,\ y \in M,\ x + y \in M$
- Essentially: a von Neumann algebra on $\mathcal{H}$ is a set of linear operators which is closed under Hermitian conjugation, addition, multiplication, and contains all scalar multiples of the identity
- We note that this definition is only true for *finite dimensional* von Neumann algebras
- The 'true' definition is topological, but reduces to this above definition when $\mathcal{H}$ is finite dimensional, and this is the only case we need
- We often define a von Neumann algebra through its generators, writing $M = \langle a, b, \ldots \rangle_{vN}$
- For example, if x, y, z denote the Pauli matrices, $\langle z \rangle_{vN}$ is the algebra of 2×2 diagonal matrices, $\langle z, x \rangle_{vN} = \mathcal{L}(\mathbb{C}^2)$
- Any von Neumann algebra induces two 'natural' associated algebras:

  Definition 1.2 (Commutant)**.** Given von Neumann algebra M on $\mathcal{H}$, the **commutant** of M, denoted M', is
  $$M' \equiv \{ y \in \mathcal{L}(\mathcal{H}) \,|\, xy = yx,\ \forall x \in M \} \tag{1.1}$$

  Definition 1.3 (Center)**.** Given von Neumann algebra M on $\mathcal{H}$, the **center** of M, denoted Z_M, is
  $$Z_M \equiv M \cap M' \tag{1.2}$$
- Basically, the commutant M' is the set of all linear operators which commute with the von Neumann algebra M, and the center Z_M is the subset of these which are themselves in M
- These are easily checked to be von Neumann algebras themselves

1.1 Projections and Partial Isometries

- Two recurrent classes of linear operators are the projections and partial isometries

  Definition 1.4 (Projection)**.** A linear map $p \in \mathcal{L}(\mathcal{H})$ is called a **projection** if $p^\dagger = p$ and $p^2 = p$

  Definition 1.5 (Partial Isometry)**.** A linear map $a \in \mathcal{L}(\mathcal{H})$ is called a **partial isometry** if $a^\dagger a = p$, where P is a projection

- Projections meet our usual intuition of projections, and partial isometries are isometries (distance preserving transformations) on the orthogonal complement to their kernel (sometimes called the *initial subspace*)

- Projections always have a subspace $p\mathcal{H}$ on which they act identically, and they annihilate the orthogonal complement $(1-p)\mathcal{H}$ (i.e. $\ker p = (1-p)\mathcal{H}$)

- Partial isometries are characterised by the following theorem:

  Theorem 1.1. *Suppose $a \in \mathcal{L}(\mathcal{H})$ is a partial isometry, so $a^\dagger a = p$ for some projection $p \in \mathcal{L}(\mathcal{H})$. Then, $a^\dagger$ is also a partial isometry, obeying $aa^\dagger = q$ where $q \in \mathcal{L}(\mathcal{H})$ is also a projection, and there exists a unitary $u \in \mathcal{L}(\mathcal{H})$ such that $q = upu^\dagger$. This means p and q have equal rank, and we can in fact choose u such that $a = up$.*

  Proof. We first show $a^\dagger$ is indeed a partial isometry. First, note that any $|v\rangle \in (1-p)\mathcal{H}$ is also annihilated by a, since

  $$\|a\,|v\rangle\|^2 = \langle v|a^\dagger a|v\rangle = \langle v|p|v\rangle = 0 \implies a\,|v\rangle = 0 \tag{1.3}$$

  We can represent a in block-matrix form according to the direct sum representation $\mathcal{H} = p\mathcal{H} \oplus (1-p)\mathcal{H}$ as

  $$a = \begin{pmatrix} A & \mathbf{0} \\ B & \mathbf{0} \end{pmatrix} \tag{1.4}$$

  where only the first column can be non-zero. Computing $a^\dagger a = p$, the upper-left block must act identically on $p\mathcal{H}$, so we find $A^\dagger A + B^\dagger B = I_{p\mathcal{H}}$. From this block representation, we can easily compute $(aa^\dagger)^2 = aa^\dagger$, so $a^\dagger$ is a partial isometry and $q = aa^\dagger$ is a projection. To see that p and q have equal rank, we first note that for any $|v\rangle \in p\mathcal{H}$:

  $$qa\,|v\rangle = aa^\dagger a\,|v\rangle = ap\,|v\rangle = a\,|v\rangle \implies |v\rangle \in q\mathcal{H} \tag{1.5}$$

  We also find that for all $|v_1\rangle, |v_2\rangle \in p\mathcal{H}$, we have:

  $$\langle v_1|a^\dagger a|v_2\rangle = \langle v_1|p|v_2\rangle = \langle v_1|v_2\rangle \tag{1.6}$$

  So, if we choose $|v_i\rangle$ to be an orthonormal basis of $p\mathcal{H}$, then the vectors $a\,|v_i\rangle$ are orthonormal too and are in $q\mathcal{H}$. Therefore $\dim p\mathcal{H} \leq \dim q\mathcal{H}$. Repeating this argument for $q\mathcal{H}$ and $a^\dagger$, we find too that $\dim p\mathcal{H} \leq \dim q\mathcal{H}$, so $\dim p\mathcal{H} = \dim q\mathcal{H}$, and hence p and q must have equal rank.
  Any two projections of equal rank are always unitarily equivalent, so we therefore must have $q = upu^\dagger$ for a unitary $u \in \mathcal{L}(\mathcal{H})$. We can also choose u such that $u\,|v\rangle = a\,|v\rangle$ for any $|v\rangle \in p\mathcal{H}$ (**why??**), which gives us $a = up$. □

- If projections p and q are related by some partial isometry a in this way, we say p and q are *equivalent*, and write $p \sim q$ (this is indeed an equivalence relation between projections)

- Partial isometries also pop up in the polar decomposition:

  Theorem 1.2 (Polar Decomposition)**.** *Suppose $x \in \mathcal{L}(\mathcal{H})$. Then there exists non-negative matrix $|x|$ and partial isometry a such that $x = a|x|$, where $a^\dagger a = p$ projects onto the orthogonal complement* $\ker x^\perp$. *Moreover, a and $|x|$ are both unique.*

  Proof. First, define $|x| \equiv \sqrt{x^\dagger x}$ (i.e. $|x|^2 = x^\dagger x$), which is clearly non-negative. Note that

  $$|x|\,|v\rangle = 0 \iff \langle v||x|^2|v\rangle = \langle v|x^\dagger x|v\rangle = 0 \iff x\,|v\rangle = 0 \tag{1.7}$$

  for $|v\rangle \in \mathcal{H}$, so $\ker x = \ker|x|$. Now, $|x|$ is invertible on $\ker|x|^\perp = \ker x^\perp \equiv p\mathcal{H}$ for some projection onto this subspace; so define $a \equiv x\,(|x|^{-1} \oplus 0_{\ker x})$, and compute

  $$a^\dagger a = \left(|x|^{-1} \oplus 0_{\ker x}\right)|x|^2\left(|x|^{-1} \oplus 0_{\ker x}\right) = I_{p\mathcal{H}} \oplus 0_{(1-p)\mathcal{H}} = p \tag{1.8}$$

  Note that $x = a|x|$ implies $x^\dagger x = |x|a^\dagger a|x| = |x|p|x| = |x|^2$, so $|x|$ is unique. Also, if $a'|x| = a|x|$, if we right-multiply by $(|x|^{-1} \oplus 0_{\ker x})$ we find $a = a'$, so a is also unique. □

1.2 The Bicommutant Theorem

- This is arguably the single most important result about von Neumann algebras

  Theorem 1.3. *For any von Neumann algebra M on $\mathcal{H}$, we have $M'' \equiv (M')' = M$*

- Before proving this, note the subtlety: $M'' \supseteq M$ by definition, but $M'' \subseteq M$ isn't immediate as there may be operators commuting with everything in M' which are outside M, so this is what we need to show

  Proof. This proof relies on a 'doubling' trick. Instead of considering the action of M on $\mathcal{H}$, we extend M to a new von Neumann algebra $I \otimes M$ on $\mathcal{H} \otimes \mathcal{H}$.
  Denote $\dim\mathcal{H} = n$; then elements of $\mathcal{L}(\mathcal{H} \otimes \mathcal{H})$ can be viewed as $n \times n$ block matrices, where each block is itself $n \times n$. Elements of $I \otimes M$ are block diagonal in this representation, with each diagonal block being the same $x \in M$:

  $$I \otimes x = \begin{pmatrix} x & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & x \end{pmatrix} \tag{1.9}$$

  In other words, we are doing a block decomposition based on the fact that $\mathcal{H} \otimes \mathcal{H} \cong \oplus_{i=1}^n \mathcal{H}_i$. To find the commutant, consider an arbitrary element $y \in \mathcal{L}(\mathcal{H} \otimes \mathcal{H})$, where each block is an arbitrary element $y_{ij} \in \mathcal{L}(\mathcal{H})$. Left and right-multiplying by the matrix $I \otimes x$ shows that in order for $y \in (I \otimes M)'$, we need each individual block y_{ij} to commute with x, so since x is arbitrary we must have $y_{ij} \in M'$. This determines the commutant to be the set of all block matrices with all blocks being arbitrary elements of M'.
  Now consider those elements of $(I \otimes M)'$ where all blocks are zero except for one, which is taken to be the identity. Any element of $(I \otimes M)''$ must certainly commute with all these elements, and some matrix multiplication confirms that such an operator much have the same element $z \in M''$ on each diagonal block with all other blocks zero. This defines the bicommutant $(I \otimes M)''$.
  Now, consider an arbitrary vector $|v\rangle \in \mathcal{H} \otimes \mathcal{H}$, and the subspace $V \subseteq \mathcal{H} \otimes \mathcal{H}$ defined by $V \equiv (I \otimes M)\,|v\rangle$. We claim that the projection p_V onto V commutes with all elements of $I \otimes M$. To see this, first note that V is invariant under the action of $I \otimes M$. This implies that for all $x \in I \otimes M$, $p_V x p_V = x p_V$. Fix such an x; since $x^\dagger \in I \otimes M$, we have

$p_V x^\dagger p_V = x^\dagger p_V$ too, so taking adjoints we find that $p_V x = x p_V$ for all $x \in I \otimes M$. Therefore p_V commutes with everything in $(I \otimes M)''$, which implies that any element of $(I \otimes M)''$ with $z \in M''$ on the diagonal blocks must also preserve V. This means that its action on $|v\rangle$ must be equivalent to the action of some element of $I \otimes M$ with $x \in M$ on the diagonal blocks. Now if we choose a basis $|v_i\rangle$ of $\mathcal{H}$ and set $|v\rangle = \oplus_i |v_i\rangle$, we find that $z = x$ and hence that $M'' \subseteq M$. Since $M \subseteq M''$ by definition, we must have $M'' = M$. □

- Note that we **need** the identity axiom for this proof to be valid, else we may not have $|v\rangle \in V$ and so we could not conclude that $z\,|v\rangle \in V$

1.3 Properties of von Neumann Algebras

- We now state and prove some basic properties of von Neumann algebras

Proposition 1. *Suppose $x \in M$ is Hermitian. Then, the projections onto the eigenspaces of x are also in M. Also, if $f : D \to \mathbb{C}$ with $D \subseteq \mathbb{R}$ is an arbitrary function, and all eigenvalues of x are in D, then $f(x) \in M$.*

Proof. Since any $y \in M'$ commutes with x, we must have that all eigenprojectors commute with all such y. This means that the projectors are in $M'' = M$ by the bicommutant theorem. Once we have all the projectors p_i corresponding to eigenvalues λ_i, we can decompose $x = \sum_i \lambda_i p_i$ which allows us to define $f(x) = \sum_i f(\lambda_i) p_i$, which is clearly in M. □

Proposition 2. *Any $x \in M$ can be written as a linear combination of at most 4 unitary elements of M.*

Proof. First, note that $x \in M$ can be written as a linear combination of two Hermitian elements of M via

$$x = \frac{x + x^\dagger}{2} + i\frac{x - x^\dagger}{2i} \tag{1.10}$$

so we just need to show that Hermitian operators can be written as a linear combination of two unitaries. Suppose then that $x^\dagger = x$. We can rescale x so that its largest eigenvalue has magnitude less than 1, in which case we can write

$$x = \frac{1}{2}\left(x + i\sqrt{1 - x^2}\right) + \frac{1}{2}\left(x - i\sqrt{1 - x^2}\right) \tag{1.11}$$

The operators $x \pm i\sqrt{1 - x^2}$ are unitary, and by prop. 1 they are in M too. □

Proposition 3. *Suppose $p \in M$ is a projection. Then pMp defines a von Neumann algebra on $p\mathcal{H}$, and its commutant on $p\mathcal{H}$ is $M'p$.*

Proof. pMp can be easily (but tediously) checked to be a von Neumann algebra satisfying the axioms. To show that $M'p$ is the commutant, we can abuse the bicommutant theorem and just show that $pMp = (M'p)'$. Suppose that $x \in \mathcal{L}(p\mathcal{H})$ commutes with yp for all $y \in M'$. If we define $x_0 \equiv x \oplus 0_{(1-p)\mathcal{H}}$, then clearly $x = p x_0 p$. To check that $x_0 \in M$, we again use the bicommutant theorem - if x_0 commutes with all $y \in M'$, then it will be in $M'' = M$. But $x_0 y = x_0 p y = x_0 y p = y p x_0 = y x_0$, so we are done. □

Proposition 4. *Suppose $x \in M$, and that it has unique polar decomposition $x = a|x|$. Then a and $|x|$ are both in M too.*

Proof. $|x| = \sqrt{x^\dagger x} \in M$ by prop. 1. To show $a \in M$, we show that it commutes with M', and hence is in M by the bicommutant theorem. By prop. 2, it suffices to show a commutes with any unitary element $u \in M'$. First, note that $u(a|x|) = (a|x|)u = au|x|$ since $x = a|x|$ and $|x|$ are both in M. But then by theorem 1.2, the projection $a^\dagger a$ onto the orthogonal complement $\ker x^\perp = \ker |x|^\perp$ is also in M. This therefore means that $(au)^\dagger (au) = u^\dagger (a^\dagger a) u = a^\dagger a u^\dagger u = a^\dagger a = a^\dagger u^\dagger u a = (ua)^\dagger (ua)$, so by uniqueness of the polar decomposition of $ua|x|$, we have $ua = au$. □

1.4 Factors

- A special type of von Neumann algebras are *factors*

  Definition 1.6 (Factor)**.** A von Neumann algebra M on $\mathcal{H}$ is called a **factor** if its center $Z_M \equiv M \cap M'$ contains only scalar multiples of the identity I.

- Factors have a special role, and they have some nice properties:

  Proposition 5. *Suppose M is a factor, and p and q are nonzero projectors in M. Then there exists a unitary $u \in M$ such that $puq \neq 0$.*

  Proof. The proof is by contradiction. Suppose that $puq = 0$ for all unitaries $u \in M$. Then we also have that $u^\dagger puq = 0$ for all unitaries. So define a new projection r which annihilates only those vectors in $\cap_{u \in M} \ker u^\dagger pu$ (i.e. $\ker r = \cap_{u \in M} \ker u^\dagger pu$). We note two things:

  - Any vector in $q\mathcal{H}$ is annihilated by $u^\dagger pu$, and so is also annihilated by r, so r is not the identity.
  - Since $p \neq 0 \implies u^\dagger pu \neq 0$, r is non-zero too.

  Also note that $\ker r$ is preserved by the action of any unitary $\hat{u}$. To see this, suppose $|v\rangle \in \cap_{u \in M} \ker u^\dagger pu$; then:

  $$u^\dagger pu \, |v\rangle = 0 \; \forall u \in M \implies \hat{u} u^\dagger pu \hat{u}^\dagger \hat{u} \, |v\rangle = 0 \; \forall u \in M \tag{1.12}$$

  But if we have a complete set of unitaries $\{u\}$, then the set $\{u\hat{u}\}$ for fixed $\hat{u}$ is just a relabelling and is also the same complete set of unitaries (**can I prove this? Is there a neater way of expressing this argument?**). Therefore $\hat{u}$ preserves $\ker r$ as claimed. But this means r commutes with all unitaries $\hat{u}$ (since $\hat{u}$ acts within $\ker r$, and r is the identity on $\operatorname{dom} r$), and thus with everything in M. r is itself also in M since it commutes with everything in M'. To see this, note that for fixed $x \in M'$ and arbitrary $|v\rangle \in \cap_{u \in M} \ker u^\dagger pu$, $xu^\dagger pu \, |v\rangle = u^\dagger pux \, |v\rangle = 0$ for all u, since x commutes with $u^\dagger pu \in M$. Therefore, $rx \, |v\rangle = xr \, |v\rangle = 0$, and so r commutes with x. r is therefore a non-trivial element of Z_M, which contradicts M being a factor. □

- Before presenting the next property, we introduce a (partial) ordering on projections

- For projections p and q, if $p\mathcal{H} \subseteq q\mathcal{H}$ (or equivalently, $\ker p \supseteq \ker q$), we say $p \leq q$

- Note in particular that if $p\mathcal{H} \perp q\mathcal{H}$, then we can't compare p and q with this ordering

  Proposition 6. *Suppose M is a factor, and p and q are non-zero projectors in M. Then, there exists a partial isometry a such that $a^\dagger a \leq q$ and $aa^\dagger \leq p$.*

Proof. Define $x \equiv puq$, with $u \in M$ a unitary chosen so $x \neq 0$. By the polar decomposition, we have $x = a|x|$, and note that $\ker a = \ker|x|$. If $|v\rangle \in \ker q$, then $puq\,|v\rangle = x\,|v\rangle = a|x|\,|v\rangle = 0$, so $|v\rangle \in \ker|x| = \ker a$, which means $a^\dagger a \leq q$. Also, $qu^\dagger p = |x|a^\dagger$, if $|v\rangle$ is annihilated by p it must also be annihilated by $|x|a^\dagger$. From thm. 1.1, we know that $a^\dagger = a^\dagger a w^\dagger$, where w is a unitary that maps $\ker|x|$ to $\ker a^\dagger$, so $|x|a^\dagger\,|v\rangle = 0 \implies a^\dagger\,|v\rangle = 0$, so $aa^\dagger \leq p$. □

- We now introduce a special type of projection

Definition 1.7 (Minimal Projection)**.** Suppose M is a von Neumann algebra on $\mathcal{H}$, and p is a non-zero projection. We say p is a **minimal projection** if for any projection $q \in M$, we have $q \leq p$ iff $q = 0$ or $q = p$.

- Since $\mathcal{H}$ is finite dimensional, minimal projections must always exist in any von Neumann algebra
- To see this, suppose we have a non-zero, non-minimal projection p
- We can find a non-zero projection q of smaller rank such that $q \leq p$
- If q is non-minimal, we can repeat this, and since any projection of rank 1 is necessarily minimal, this procedure always finds a minimal projection
- Minimal projections are characterised by the following:

Theorem 1.4. *Suppose M is a von Neumann algebra on $\mathcal{H}$, and p is a minimal projection. Then $pMp = \mathbb{C}p$.*

Proof. pMp always contains $\mathbb{C}p$ trivially. If it contains any other operators, then by prop. 1 it has a non-trivial projection q. But such a q contradicts p being minimal. □

- Minimal projections existing is a consequence of $\mathcal{H}$ being finite dimensional
- In the infinite dimensional case, factors containing a minimal projection are called *type I*, while those that don't are called *type II/III*

1.5 Classification of Finite Dimensional von Neumann Algebras

- We are now in a position to classify all von Neumann algebras on finite dimensional Hilbert spaces
- The trickiest step is classifying factors - we start with this

Theorem 1.5 (Factor Classification)**.** *Suppose M is a factor on $\mathcal{H}$. Then there exists a tensor factorisation $\mathcal{H} = \mathcal{H} \otimes \overline{\mathcal{A}}$ such that $M = \mathcal{L}(\mathcal{H}_A) \otimes I_{\overline{A}}$, and moreover $M' = I_A \otimes \mathcal{L}_{\mathcal{H}_{\overline{A}}}$*

Proof. Let $\{p_1, p_2, \ldots\}$ be a maximal set of minimal projections, satisfying $p_i p_j = 0$ for $i \neq j$. Such a set always exists since we can take any single minimal projection and then keep adding more until we can no longer do so. Our first claim is that $\sum_i p_i = I$. Define

$$q = 1 - \sum_i p_i \tag{1.13}$$

and note that q is itself a projector, with $qp_i = p_i q = 0$ for all i. Assume $q \neq 0$. Since our set is maximal, q is not itself minimal, but we can generate a minimal projector by finding a non-zero projection $\hat{q}$ of smaller rank with $\hat{q} \leq q$ as described above, repeating

this process until we have a new minimal projector. $\hat{q}$ is not in our set of p_i's since its domain is mutually orthogonal to them all, which contradicts maximality. Hence $q = 0$, and $I = \sum_i p_i$.
For each i, we have a partial isometry a_i satisfying $a_i^\dagger a_i \leq p_i$ and $a_i a_i^\dagger \leq p_1$. By minimality, we must have $a_i^\dagger a_i = p_i$ and $a_i a_i^\dagger = p_1$. However, theorem 1.1 tells us that all the projectors are unitarily equivalent, and so have equal rank. Since $I = \sum_i p_i$ has full rank equal to $\dim \mathcal{H}$, this rank must divide $\dim \mathcal{H}$.
Moreover, since $I = \sum_i p_i$, we have $x = \sum_{i,j} p_i x p_j$ for any $x \in M$. We now note

$$p_i x p_j = p_i^2 x p_j^2 = a_i^\dagger a_i a_i^\dagger a_i x a_j^\dagger a_j a_j^\dagger a_j = a_i^\dagger p_1 a_i x a_j^\dagger p_1 a_i \tag{1.14}$$

Since p_1 is minimal, we have by theorem 1.4 that there exist complex coefficients $\lambda_{ij} \in \mathbb{C}$ such that $p_1 a_i x a_j^\dagger p_1 = \lambda_{ij} p_1$. Recalling that a_i maps $p_i \mathcal{H} \to p_1 \mathcal{H}$, we have:

$$p_i x p_j = \lambda_{ij} a_i^\dagger p_1 a_j = \lambda_{ij} a_i^\dagger a_j \tag{1.15}$$

and so finally, $x = \sum_{ij} \lambda_{ij} a_i^\dagger a_j$. This means that M is generated by the a_i's.
We now identify the algebra generated like this. Since $I = \sum_i p_i$, we have $\mathcal{H} = \oplus_i p_i \mathcal{H}$. We can therefore define a tensor product structure $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$ by taking $\mathcal{L}(\mathcal{H}_A) \otimes I_{\overline{A}}$ to be the block matrices where each block is an arbitrary multiple of the identity, and $I_A \otimes \mathcal{L}(\mathcal{H}_{\overline{A}})$ to be the set of block diagonal matrices with the same element of $\mathcal{L}(\mathcal{H}_{\overline{A}})$ in each diagonal block. We can choose a basis within each block so that a_i is represented as a block matrix with the identity in the $(1, i)$th block, with zeros elsewhere. Then, $a_i^\dagger a_j$ has the identity in the (i, j)th block with zeros elsewhere. These matrices clearly generate $\mathcal{L}(\mathcal{H}_A) \otimes I_{\overline{A}}$, which is thus M. It's not hard to verify that $M' = I_A \otimes \mathcal{H}(\mathcal{L}_{\overline{A}})$. □

- Note that this theorem justifies why they're called 'factors' - if a Hilbert space admits a factor, it factorises
- Let's now consider the general case where M is not necessarily a factor
- The basic logic is that since all elements of the center Z_M mutually commute, we can simultaneously diagonalise them in some basis
- By prop. 1, this means there is a family of mutually orthogonal projections $p_\alpha \in Z_M$ such that Z_M is equivalent to the set of operators $\sum_\alpha \lambda_\alpha p_\alpha$
- We then have the following proposition:

  Proposition 7. *Suppose M is a von Neumann algebra, with center Z_M spanned by mutually orthogonal projections p_α. Then for all α, $p_\alpha M p_\alpha$ is a factor on $p_\alpha \mathcal{H}$. Also, if $\alpha \neq \beta$, then $p_\alpha M p_\beta = 0$.*

  Proof. Suppose $p_\alpha M p_\alpha$ had a non-trivial central element c. Then, $c \oplus 0_{(1-p_\alpha)\mathcal{H}}$ is not in the span of the p_αs, but they span Z_M so no such c can exist, and so $p_\alpha M p_\alpha$ is a factor. Moreover, if $\alpha \neq \beta$, then $p_\alpha M p_\beta = M p_\alpha p_\beta = 0$. □

- What this proposition basically says is that if we decompose $\mathcal{H} = \oplus_\alpha p_\alpha \mathcal{H}$, then every element of M is block diagonal, and each diagonal block is itself a factor algebra
- Together with theorem 1.5, this implies the full classification of von Neumann algebras:

  Theorem 1.6 (Classification of von Neumann Algebras)**.** *Suppose M is a von Neumann algebra on finite dimensional Hilbert space $\mathcal{H}$. Then, we have a block decomposition $\mathcal{H} = \oplus_\alpha \left(\mathcal{H}_{A_\alpha} \otimes \mathcal{H}_{\overline{A}_\alpha}\right)$ in terms of which M and M' are block diagonal, with decompositions $M = \oplus_\alpha \left(\mathcal{L}(\mathcal{H}_{A_\alpha}) \otimes I_{\overline{A}_\alpha}\right)$ and $M' = \oplus_\alpha \left(I_{A_\alpha} \otimes \mathcal{L}(\mathcal{H}_{\overline{A}_\alpha})\right)$.*

- Note the abuse of notation: if we have a block diagonal operator x with diagonal blocks x_α, then we can just write $x = \oplus_\alpha x_\alpha$
- This theorem actually has an infinite dimensional analogue, but classifying factors is much trickier so we ignore it for now - infinite dimensional von Neumann algebras only really come up in QFT, and quantum computing is strictly quantum mechanical

1.6 Entropy

1.6.1 States

- So far, we've looked at von Neumann algebras as subsets of $\mathcal{L}(\mathcal{H})$
- In QM, hermitian operators correspond to observables, but we need to introduce states in order to do physics

  Definition 1.8 (States)**.** A linear operator $\rho \in \mathcal{L}(\mathcal{H})$ is called a **state** on $\mathcal{L}(\mathcal{H})$ if it is hermitian, non-negative, and has $\mathrm{Tr}(\rho) = 1$.

- Any state ρ has a canonical linear action $\mathbb{E}_\rho$ on $\mathcal{L}(\mathcal{H})$

  Definition 1.9 (Expectation)**.** For any hermitian $x \in \mathcal{L}(\mathcal{H})$, the **expectation value of** x **in the state** ρ is
  $$\mathbb{E}_\rho(x) = \mathrm{Tr}(\rho x) \tag{1.16}$$

- This can more generally be defined as a linear action on any $x \in \mathcal{L}(\mathcal{H})$
- In more mathematical presentations of this, states are often *defined* as linear, non-negative maps on $\mathcal{L}(\mathcal{H})$ obeying $\mathbb{E}_\rho(I) = 1$, but this is needlessly abstract for us
- Sometimes, one is interested only in observables which are elements of a von Neumann algebra M
- A generic state ρ will not necessarily be in M, and will often contain more information than necessary to compute expectation values of elements in M
- The following theorem gives a way to discard this additional information:

  Theorem 1.7. *Suppose M is a von Neumann algebra on $\mathcal{H}$, and ρ is a state on $\mathcal{H}$. Then, there exists a unique state $\rho_M \in M$ such that $\mathbb{E}_\rho(x) = \mathbb{E}_{\rho_M}(x)$ for all $x \in M$.*

  Proof. The basic point is to define
  $$\rho_M \equiv \int_{u \in M'} du\, u\rho u^\dagger \tag{1.17}$$
  where the integration is over the set of unitary elements $u \in M'$, using the invariant Haar measure du on this compact group. To see the unitary subgroup is indeed compact, recall that the unitary group is compact in general so any Cauchy convergent sequence of unitaries $u_n \in M'$ will converge to some unitary u, and by continuity of the commutator the limit u will also be in M'.
  Defined this way, ρ_M is clearly:

  – Hermitian, $\rho_M^\dagger = \rho_M$.
  – Non-negative.
  – Has trace one, $\mathrm{Tr}(\rho_M) = \mathrm{Tr}(u\rho u^\dagger) = 1$.

so is indeed a state. To show $\rho_M \in M$, we show that it commutes with any unitary $v \in M'$, and thus is in $M'' = M$ by the bicommutant theorem and the fact that von Neumann algebras are spanned by their unitary elements. So fix some unitary $v \in M'$. Then we have

$$v\rho_M = \int_{u \in M'} du\, vu\rho u^\dagger = \int_{u' \in M'} du'\, u'\rho u'^\dagger v = \rho_M v \tag{1.18}$$

where in the second equality we set $u' = vu \implies du' = vdu$, and use invariance of the measure.

The last thing to do is to show ρ_M is unique. Suppose there existed $\rho'_M \neq \rho_M$ obeying all the results of the theorem. Then, we must have $\mathrm{Tr}((\rho_M - \rho'_M)x) = 0$ for all $x \in M$. But if we take $x = \rho_M - \rho'_M$, we get $\mathrm{Tr}(\rho_M - \rho'_M)^2 = 0$, which implies $\rho_M = \rho'_M$. □

- This theorem essentially tells us that to compute expectations in M, we can always replace any state by an element of M
- Let's consider the case where M is a factor as an example - what is ρ_M?
- By theorem 1.5, we know there exists a factorisation $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$ such that $M = \mathcal{L}(\mathcal{H}_A) \otimes I_{\overline{A}}$
- If we define the reduced state

$$\rho_A \equiv \mathrm{Tr}_{\overline{A}}(\rho) \tag{1.19}$$

then the operator

$$\rho_M \equiv \rho_A \otimes \frac{I_{\overline{A}}}{|\overline{A}|} \tag{1.20}$$

obeys the results of theorem 1.7

- By uniqueness, the ρ_M defined here must be equivalent to (1.17)
- We can do the same procedure for a more general M which isn't necessarily a factor
- We know that there's a decomposition

$$\mathcal{H} = \oplus_\alpha \left(\mathcal{H}_{A_\alpha} \otimes \mathcal{H}_{\overline{A}_\alpha}\right) \tag{1.21}$$

in terms of which

$$M = \oplus_\alpha \left(\mathcal{L}\left(\mathcal{H}_{A_\alpha}\right) \otimes I_{\overline{A}_\alpha}\right) \tag{1.22}$$

- Any state ρ can be written in block form wrt (1.21), and only blocks on the α diagonal contribute to expectations of M
- On each diagonal block, we can define

$$p_\alpha \rho_{A_\alpha} \equiv \mathrm{Tr}_{\overline{A}}(\rho_{\alpha\alpha}) \tag{1.23}$$

where p_α is a positive number chosen so $\mathrm{Tr}_{A_\alpha}(\rho_{A_\alpha}) = 1$

- The condition $\mathrm{Tr}(\rho) = 1$ implies that $\sum_\alpha p_\alpha = 1$
- We can then finally define the block diagonal state

$$\rho_M \equiv \oplus_\alpha \left(p_\alpha \rho_{A_\alpha} \otimes \frac{I_{\overline{A}_\alpha}}{|\overline{A}_\alpha|}\right) \tag{1.24}$$

which again obeys theorem 1.7

1.6.2 Example

- As an example for a simple case of a factor algebra, consider $\mathcal{H} = \mathcal{H}_2 \otimes \mathcal{H}_2$, so $M = \mathcal{L}(\mathcal{H}_2) \otimes I_2$ is a factor
- In other words, an arbitrary $x \in M$ looks like

$$x = \begin{pmatrix} x_{11} & 0 & x_{12} & 0 \\ 0 & x_{11} & 0 & x_{12} \\ x_{21} & 0 & x_{22} & 0 \\ 0 & x_{21} & 0 & x_{22} \end{pmatrix} \tag{1.25}$$

- Consider the state defined by

$$\rho = \begin{pmatrix} 1/2 & 1/4 & 0 & 1/4 \\ 1/4 & 1/4 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/4 & 0 & 0 & 1/4 \end{pmatrix} \tag{1.26}$$

  which gives $\mathbb{E}_\rho(x) = \frac{3}{4}x_{11} + \frac{1}{4}x_{22}$

- Following the procedure, we calculate the reduced state:

$$\rho_A = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix} \tag{1.27}$$

  and so

$$\rho_M = \begin{pmatrix} 3/8 & 0 & 0 & 0 \\ 0 & 3/8 & 0 & 0 \\ 0 & 0 & 1/8 & 0 \\ 0 & 0 & 0 & 1/8 \end{pmatrix} \tag{1.28}$$

  from which it is easy to find that $\mathbb{E}_{\rho_M}(x) = \frac{3}{4}x_{11} + \frac{1}{4}x_{22}$ as expected

1.7 Modified Trace and Entropy

- From (1.20), we see that ρ_M is closely related to ρ_A, and ρ_A is what is used to define the von Neumann entropy of ρ on system A/factor M via $S(\rho_A) = -\mathrm{Tr}_A(\rho_A \log \rho_A)$
- This gives a natural generalisation for the entropy of a state ρ on an arbitrary von Neumann algebra M:

$$S(\rho, M) \equiv -\sum_\alpha \mathrm{Tr}_{A_\alpha}\left(p_\alpha \rho_{A_\alpha} \log(p_\alpha \rho_{A_\alpha})\right) = -\sum_\alpha p_\alpha \log p_\alpha + \sum_\alpha p_\alpha S(\rho_{A_\alpha}) \tag{1.29}$$

- Let's arrive at this entropy from a more abstract perspective
- It would be ideal to extract this entropy directly from the state ρ_M, but there's some issues
- For example, suppose we just set the entropy of ρ on M to be $S(\rho_M)$; even when M is a factor, then

$$S(\rho_M) = -\mathrm{Tr}(\rho_M \log \rho_M) = -\mathrm{Tr}\left(\rho_A \otimes \frac{I_{\overline{A}}}{|\overline{A}|}\right) \log\left(\rho_A \otimes \frac{I_{\overline{A}}}{|\overline{A}|}\right) = S(\rho_A) + \log|\overline{A}| \tag{1.30}$$

  which disagrees with what we'd want by $\log|\overline{A}|$

- In the general case, the disagreement is $\sum_\alpha p_\alpha \log |\overline{A}_\alpha|$
- The issue stems from ρ_M being supported on the full Hilbert space; we haven't taken the partial trace, so the entropy from the $|\overline{A}_\alpha|$ system is contributing
- One way to deal with this is to introduce a *modified trace*
- For a von Neumman algebra M on $\mathcal{H}$, the trace of a minimal projection is usually not one itself
- For example, if M is a factor, then any minimal projection has the form $|v\rangle \langle v|_A \otimes I_{\overline{A}}$, which has trace $|\overline{A}|$
- The entropy of this state on $\mathcal{H}_A$ is clearly 0, which can be seen by just tracing out $\overline{A}$ - but can we see this from a perspective more inherent to M rather than the underlying systems?
- One canonical way to do this is to define a *normalised trace* on M, so $\hat{\mathrm{Tr}}p = 1$ for any minimal projection $p \in M$; this means

$$\hat{\mathrm{Tr}} \equiv \frac{1}{|\overline{A}|}\mathrm{Tr} \tag{1.31}$$

- If we further define

$$\hat{\rho}_M \equiv |\overline{A}|\rho_M \tag{1.32}$$

then for any $x \in M$, we have

$$\mathbb{E}_\rho(x) = \mathrm{Tr}\rho x = \mathrm{Tr}\rho_M x = \hat{\mathrm{Tr}}\hat{\rho}_M x \tag{1.33}$$

- From (1.20), we can then define the entropy $S(\rho, M)$ by using the normalised trace and normalised $\hat{\rho}_M$:

$$S(\rho, M) \equiv -\hat{\mathrm{Tr}}\hat{\rho}_M \log \hat{\rho}_M = -\mathrm{Tr}_A \rho_A \log \rho_A = S(\rho_A) \tag{1.34}$$

which gives an 'intrinsic' definition of the entropy of ρ on a factor M

- It is just the expectation value of the operator $-\log \hat{\rho}_M$ in the state ρ_M
- In the case where M is not a factor, it's a bit trickier
- We just define a normalised trace $\hat{\mathrm{Tr}}$ again so that $\hat{\mathrm{Tr}}p = 1$ for any minimal projection $p \in M$; however, this time it turns out that $\hat{\mathrm{Tr}}$ is **not** proportional to Tr
- We are only interested in defining $\hat{\mathrm{Tr}}$ for elements of M; recalling the block decomposition (1.21), no elements of M mix between different blocks, so we can normalise the trace independently in each block without breaking the usual defining characteristic property of trace that $\hat{\mathrm{Tr}}xy = \hat{\mathrm{Tr}}yx,\ \forall x, y \in M$
- We can then just define $\hat{\mathrm{Tr}}$ as the unique linear operation on M such that $\hat{\mathrm{Tr}}xy = \hat{\mathrm{Tr}}yx,\ \forall x, y \in M$, which also gives $\hat{\mathrm{Tr}}p = 1$ for any minimal projection p
- Explicitly in terms of decompositions (1.21) and (1.22), if $x \in M$ has representation

$$x = \oplus_\alpha \left(x_\alpha \otimes I_{\overline{A}_\alpha}\right) \tag{1.35}$$

then

$$\hat{\mathrm{Tr}}x = \sum_\alpha \hat{\mathrm{Tr}}_\alpha \left(x_\alpha \otimes I_{\overline{A}_\alpha}\right) = \sum_\alpha \mathrm{Tr}_{A_\alpha} x_\alpha \tag{1.36}$$

- Moreover, given any $\rho_M \in M$, we can introduce $\hat{\rho}_M$ again defined so that for any $x \in M$, we have
$$\mathbb{E}_\rho(x) = \text{Tr}\rho x = \text{Tr}\rho_M x = \hat{\text{Tr}}\hat{\rho}_M x \tag{1.37}$$

- Explicitly, from (1.24) we have
$$\hat{\rho}_M = \oplus_\alpha \left(p_\alpha \rho_{A_\alpha} \otimes I_{\overline{A}_\alpha}\right) \tag{1.38}$$

- At long last, we can define the entropy of ρ on algebra M by
$$S(\rho, M) \equiv -\hat{\text{Tr}}\hat{\rho}_M \log \hat{\rho}_M \tag{1.39}$$
which can be shown to be equivalent to (1.29)

1.8 Properties of Entropy

- For ease of reference, the entropy of ρ on M is
$$S(\rho, M) \equiv -\sum_\alpha \text{Tr}_{A_\alpha}\left(p_\alpha \rho_{A_\alpha} \log(p_\alpha \rho_{A_\alpha})\right) = -\sum_\alpha p_\alpha \log p_\alpha + \sum_\alpha p_\alpha S(\rho_{A_\alpha}) \tag{1.40}$$

- Schematically, this has a 'classical' piece given by the Shannon entropy of the probability distribution p_α for the center Z_M, and a 'quantum' piece given by the weighted average of the von Neumann entropy of each block over this distribution

- It has the following properties:
  - $S(\rho, M) = S(u\rho u^\dagger, M)$ for any unitary $u \in M$
  - $S(\rho, M) \geq 0$, with equality iff ρ_M is a minimal projection
  - $S(\rho, M) \leq \log\left(\hat{\text{Tr}}I\right) = \log\left(\sum_\alpha |A_\alpha|\right)$, with equality iff $\rho_{A_\alpha} = I_{A_\alpha}/|A_\alpha|$ and $p_\alpha = |A_\alpha|/\sum_\beta |A_\beta|$
  - $S\left(\sum_i \lambda_i \rho_i\right) \geq \sum_i \lambda_i S(\rho_i)$, where the ρ_i are any set of states and $\sum_i \lambda_i = 1$
  - If ρ is pure, then $S(\rho, M) = S(\rho, M')$

- We also have an analogous definition for relative entropy

  Definition 1.10 (Relative Entropy)**.** Given two states $\rho, \sigma \in M$, the **relative entropy** between them is
$$\begin{aligned} S(\rho|\sigma, M) &\equiv \hat{\text{Tr}}\left(\hat{\rho}_M \log \hat{\rho}_M - \hat{\rho}_M \log \hat{\sigma}_M\right) \\ &= -S(\rho, M) + \mathbb{E}_\rho(-\log \hat{\sigma}_M) \\ &= \sum_\alpha p_\alpha^{\{\rho\}} \log \frac{p_\alpha^{\{\rho\}}}{p_\alpha^{\{\sigma\}}} + \sum_\alpha p_\alpha^{\{\rho\}} S(\rho_{A_\alpha}|\sigma_{A_\alpha}) \end{aligned} \tag{1.41}$$

  This again has a classical contribution which measures the distinguishability of distributions $p_\alpha^{\{\rho\}}$ and $p_\alpha^{\{\sigma\}}$ on the center Z_M, and a quantum piece averaging the relative entropy on each block

  As usual, $S(\rho|\sigma, M) \geq 0$ with equality iff $\rho_M = \sigma_M$