Some notes on sufficient channels

Anna Jenčová

January 17, 2016

1 Preliminaries

Let $\mathcal{M}$ be a (σ-finite) von Neumann algebra and let $\mathcal{M}_*$ be its predual. We will also denote by $\mathfrak{S}(\mathcal{M})$ the set of normal states on $\mathcal{M}$. If $\mathcal{N}$ is another von Neumann algebra, a normal unital completely positive map $\mathcal{N} \to \mathcal{M}$ is called a quantum channel. A channel $\alpha : \mathcal{N} \to \mathcal{M}$ is faithful if $\alpha(a) = 0$ with a positive a implies $a = 0$.

Let $\alpha : \mathcal{N} \to \mathcal{M}$ be a channel, then α satisfies the Kadison-Schwarz inequality

$$\alpha(a^*a) \geq \alpha(a)^*\alpha(a), \qquad \forall a \in \mathcal{N}. \tag{1}$$

The set

$$\mathcal{M}_\alpha := \{a \in \mathcal{N},\ \alpha(a^*a) = \alpha(a)^*\alpha(a),\ \alpha(aa^*) = \alpha(a)\alpha(a)^*\}$$

is called the multiplicative domain of α. Note that $\mathcal{M}_\alpha$ is a subalgebra in $\mathcal{N}$ and

$$\mathcal{M}_\alpha = \{a \in \mathcal{N},\ \alpha(ab) = \alpha(a)\alpha(b),\ \alpha(ba) = \alpha(b)\alpha(a),\ \forall b \in \mathcal{N}\}$$

Moreover, the restriction $\alpha|_{\mathcal{M}_\alpha}$ is a homomorphism (by "subalgebra", "homomorphism", etc. I always mean a von Neumann subalgebra, etc.).

A conditional expectation on $\mathcal{M}$ is an idempotent channel $E : \mathcal{M} \to \mathcal{M}$. Let $\omega \in \mathfrak{S}(\mathcal{M})$ be faithful and let $\mathcal{N} \subseteq \mathcal{M}$ be a subalgebra. Then by Takesaki's theorem [6], an ω-preserving conditional expectation with range $\mathcal{N}$ exists if and only if $\sigma_t^\omega(\mathcal{N}) \subseteq \mathcal{N}$ for all $t \in \mathbb{R}$, where σ^ω is the modular group of ω. Moreover, the conditional expectation is uniquely determined by ω.

Let $\Phi : \mathcal{M} \to \mathcal{M}$ be a channel. The set of fixed points $\{a \in \mathcal{M}, \Phi(a) = a\}$ will be denoted by $\mathcal{F}_\Phi$. We will also denote the set of invariant states by $\mathcal{S}_\Phi = \{\varphi \in \mathfrak{S}(\mathcal{M}),\ \varphi \circ \Phi = \varphi\}$. If $\mathcal{S}_\Phi$ contains a faithful state ω, then $\mathcal{F}_\Phi$ is a subalgebra in the multiplicative domain $\mathcal{M}_\Phi$, invariant under the modular group σ_t^ω. Hence there exists a (unique) ω-preserving conditional expectation E_Φ on $\mathcal{M}$ onto $\mathcal{F}_\Phi$, moreover, it satisfies $E_\Phi \circ \Phi = \Phi \circ E_\Phi = E_\Phi$ and $\mathcal{S}_\Phi = \mathcal{S}_{E_\Phi}$.

Lemma 1. *Let $\Phi : \mathcal{M} \to \mathcal{M}$ be a channel and let E be a faithful conditional expectation on $\mathcal{M}$.*

(i) $E \circ \Phi = E \implies \Phi \circ E = E$.

(ii) $\Phi \circ E = E$ *if and only if* $E(\mathcal{M}) \subseteq \mathcal{F}_\Phi$. *Moreover, in this case* $E \circ \Phi$ *is a conditional expectation with the same range as* E.

(iii) Let $\omega \in \mathfrak{S}(\mathcal{M})$ *be a faithful state invariant under both* Φ *and* E. *Then* $E \circ \Phi = E$ *if and only if* $\Phi \circ E = E$.

Proof. Assume $E \circ \Phi = E$ and let $a = E(a)$. Then

$$\begin{aligned}0 &\le E((\Phi(a) - a)^*(\Phi(a) - a)) = E(\Phi(a)^*\Phi(a) - \Phi(a)^*a - a^*\Phi(a) + a^*a) \\ &= E(\Phi(a)^*\Phi(a)) - a^*a \le E(\Phi(a^*a)) - a^*a = 0\end{aligned}$$

so that $\Phi(a) = a$. This proves (i).

Assume that $\Phi \circ E = E$, then it is easy to see that $F := E \circ \Phi$ is an idempotent channel, hence a conditional expectation. Moreover, $F(\mathcal{M}) = E(\Phi(\mathcal{M})) \subseteq E(\mathcal{M})$, but since $F \circ E = E$, we obtain $F(\mathcal{M}) = E(\mathcal{M})$. The first part of (ii) is quite trivial. The statement (iii) follows by (i), (ii) and the uniqueness part of Takesaki's theorem.

□

2 Sufficient channels

A quantum statistical experiment is a pair $\mathcal{E} = (\mathcal{M}, \mathcal{S})$, where $\mathcal{M}$ is a von Neumann algebra and $\mathcal{S} \subseteq \mathfrak{S}(\mathcal{M})$is any set of normal states. Let $\alpha : \mathcal{N} \to \mathcal{M}$ be a quantum channel. We say that α is sufficient with respect to $\mathcal{E}$ if there is a channel $\beta : \mathcal{M} \to \mathcal{N}$ such that

$$\varphi \circ \alpha \circ \beta = \varphi, \qquad \forall \varphi \in \mathcal{S}.$$

Note that in this case, $\alpha \circ \beta$ is a channel on $\mathcal{M}$ under which all states in $\mathcal{S}$ are invariant. Let

$$\mathcal{I}_{\mathcal{E}} := \{\Phi : \mathcal{M} \to \mathcal{M},\ \Phi \circ \varphi = \varphi,\ \forall \varphi \in \mathcal{S}\}.$$

It is easy to see that $\mathcal{I}_{\mathcal{E}}$ is a semigroup, that is, closed under composition. Moreover, $\mathcal{I}_{\mathcal{E}}$ is convex and closed in the pointwise w*-topology.

2.1 The minimal sufficient subalgebra

In the rest of the paper, we will assume that $\mathcal{S}$ is faithful, which means that the weak closure of the convex hull of $\mathcal{S}$ contains a faithful state, which we will denote by ω. Then by the results of [1], $\mathcal{I}_{\mathcal{E}}$ contains a conditional expectation $E_{\mathcal{E}}$ such that

$$E_{\mathcal{E}} \circ \Phi = \Phi \circ E_{\mathcal{E}} = E_{\mathcal{E}}, \qquad \Phi \in \mathcal{I}_{\mathcal{E}}. \tag{2}$$

Lemma 2. *Assume that $\omega \in \bar{co}(\mathcal{S})$ is faithful. Then*

(i) Let $\Phi : \mathcal{M} \to \mathcal{M}$ be a channel. Then $\Phi \in \mathcal{I}_{\mathcal{E}}$ if and only if $E_{\mathcal{E}} \circ \Phi = E_{\mathcal{E}}$ or, equivalently, $\Phi \circ E_{\mathcal{E}} = E_{\mathcal{E}}$.

(ii) Let $\varphi \in \mathfrak{S}(\mathcal{M})$, then $\varphi \circ \Phi = \varphi$ for all $\Phi \in \mathcal{I}_{\mathcal{E}}$ if and only if $\varphi \circ E_{\mathcal{E}} = \varphi$.

(iii) The range of $E_{\mathcal{E}}$ is the set $\mathcal{F}_{\mathcal{E}}$ of fixed points of all maps in $\mathcal{I}_{\mathcal{E}}$,

$$\mathcal{F}_{\mathcal{E}} := \cap_{\Phi \in \mathcal{I}_{\mathcal{E}}} \mathcal{F}_{\Phi}.$$

The proof is almost trivial, but I include it just for the case. The part (iii) is proved also in [1].

Proof. Since $E_{\mathcal{E}} \in \mathcal{I}_{\mathcal{E}}$, $\varphi \circ E_{\mathcal{E}} = \varphi$ for all $\varphi \in \mathcal{S}$. Let Φ be a channel such that $E_{\mathcal{E}} \circ \Phi = E_{\mathcal{E}}$, then

$$\varphi \circ \Phi = \varphi \circ E_{\mathcal{E}} \circ \Phi = \varphi \circ E_{\mathcal{E}} = \varphi.$$

The statement (i) now follows by Lemma 1 and (2). The statement (ii) follows similarly by (2) and $E_{\mathcal{E}} \in \mathcal{I}_{\mathcal{E}}$. For (iii), note that the range of $E_{\mathcal{E}}$ is contained in $\mathcal{F}_{\mathcal{E}}$ by (i) and Lemma 1. On the other hand, since $E_{\mathcal{E}} \in \mathcal{I}_{\mathcal{E}}$, we have $\mathcal{F}_{\mathcal{E}} \subseteq \mathcal{F}_{E_{\mathcal{E}}} = E_{\mathcal{E}}(\mathcal{M})$.

□

Proposition 1. *[2] Let $\mathcal{E} = (\mathcal{M}, \mathcal{S})$ and let $\omega \in \bar{co}(\mathcal{S})$ be faithful. Then*

(i) $\mathcal{F}_\mathcal{E}$ is a sufficient subalgebra with respect to $\mathcal{E}$, in the sense that the inclusion $\mathcal{F}_\mathcal{E} \hookrightarrow \mathcal{M}$ is a sufficient channel with respect to $\mathcal{E}$.

(ii) Any subalgebra $\mathcal{N} \subseteq \mathcal{M}$ is sufficient with respect to $\mathcal{E}$ if and only if $\mathcal{F}_\mathcal{E} \subseteq \mathcal{N}$ (that is, $\mathcal{F}_\mathcal{E}$ is minimal sufficient).

(iii) If $\mathcal{N} \subseteq \mathcal{M}$ is the range of an ω-preserving conditional expectation F on $\mathcal{M}$, then $\mathcal{N}$ is sufficient with respect to $\mathcal{E}$ if and only if $F \in \mathcal{I}_\mathcal{E}$.

Proof. The statement (i) is immediate from $\varphi \circ E_\mathcal{E} = \varphi$. For (ii), let $\mathcal{N} \subseteq \mathcal{M}$ be sufficient with respect to $\mathcal{E}$. Then there is a channel $\beta : \mathcal{M} \to \mathcal{N} \subseteq \mathcal{M}$, such that $\beta \in \mathcal{I}_\mathcal{E}$. But then $\mathcal{F}_\mathcal{E} = E_\mathcal{E}(\mathcal{F}_\mathcal{E}) = \beta \circ E_\mathcal{E}(\mathcal{F}_\mathcal{E}) \subseteq \mathcal{N}$. Conversely, let $\mathcal{F}_\mathcal{E} \subseteq \mathcal{N}$, then $E_\mathcal{E}$ is obviously a recovery channel for $\mathcal{N}$. (iii) follows from (ii) and Lemma 1.

□

The following theorem has been proved by Petz [3]. For the definition and basic properties of cocycle derivatives, see [5].

Theorem 1. *Let $\mathcal{E}$ and $\mathcal{F}_\mathcal{E}$ be as above. Then $\mathcal{F}_\mathcal{E}$ is generated by the cocycle derivatives $[D\rho, D\omega]_t$, $\rho \in \mathcal{S}$, $t \in \mathbb{R}$.*

Proof. Since $\varphi = \varphi \circ E_\mathcal{E}$ for all $\varphi \in \bar{co}(\mathcal{S})$, we have by [5,],

$$[D\varphi, D\omega]_t = [D\varphi \circ E_\mathcal{E}, D\omega \circ E_\mathcal{E}]_t = [D\varphi|_{\mathcal{F}_\mathcal{E}}, D\omega|_{\mathcal{F}_\mathcal{E}}]_t \in \mathcal{F}_\mathcal{E}, \quad \forall \varphi \in \mathcal{S}.$$

It follows that the subalgebra $\mathcal{M}_1$ generated by the cocycle derivatives is contained in $\mathcal{F}_\mathcal{E}$. Moreover, $\mathcal{M}_1$ is invariant under σ^ω. Let F be the ω-preserving conditional expectation onto $\mathcal{M}_1$. Since $\sigma^\omega|_{\mathcal{M}_1} = \sigma^{\omega|_{\mathcal{M}_1}}$, $[D\varphi, D\omega]_t$ satisfies the cocycle condition with respect to $\omega|_{\mathcal{M}_1}$, hence by [5,], there is a (unique) faithful normal semifinite weight ψ on $\mathcal{M}_1$ such that $[D\varphi, D\omega]_t = [D\psi, D\omega|_{\mathcal{M}_1}]_t$. On the other hand, we have

$$[D\psi, D\omega|_{\mathcal{M}_1}]_t = [D\psi \circ F, D\omega \circ F]_t = [D\psi \circ F, D\omega]_t, \quad t \in \mathbb{R}.$$

It follows that $\varphi = \psi \circ F$, in particular, $\varphi \circ F = \varphi$. Since this is true for all $\varphi \in \mathcal{S}$, we have $F \in \mathcal{I}_\mathcal{E}$, so that $F = E_\mathcal{E} \circ F = E_\mathcal{E}$ and $\mathcal{M}_1 = \mathcal{F}_\mathcal{E}$.

□

We now consider an important example.

Example 1. Let $\Phi : \mathcal{M} \to \mathcal{M}$ be a channel and let $\mathcal{S} = \mathcal{S}_\Phi$, the set of invariant states. Suppose that there is a faithful state $\omega \in \mathcal{S}_\Phi$. Then $\mathcal{F}_\mathcal{E} = \mathcal{F}_\Phi$ and $E_\mathcal{E} = E_\Phi$. Indeed, since $\mathcal{S} = \mathcal{S}_{E_\Phi}$, we have $E_\Phi \in \mathcal{I}_\mathcal{E}$, so that $E_\Phi \circ E_\mathcal{E} = E_\mathcal{E}$. On the other hand, since $\varphi \circ E_\Phi \in \mathcal{S}$ and hence $\varphi \circ E_\Phi \circ E_\mathcal{E} = \varphi \circ E_\Phi$ for all $\varphi \in \mathfrak{S}(\mathcal{M})$, we obtain $E_\mathcal{E} = E_\Phi \circ E_\mathcal{E} = E_\Phi$.

2.2 The case $\mathcal{M} = B(\mathcal{H})$

Assume now that $\mathcal{M} = B(\mathcal{H})$ for a separable Hilbert space $\mathcal{H}$. Then since $\mathcal{F}_\mathcal{E}$ is the range of a normal conditional expectation, it must be an atomic subalgebra in $B(\mathcal{H})$, [7]. Hence there is a decomposition $\mathcal{H} = \oplus_n \mathcal{H}_n^L \otimes \mathcal{H}_n^R$, such that

$$\mathcal{F}_\mathcal{E} = \bigoplus_n B(\mathcal{H}_n^L) \otimes I_{\mathcal{H}_n^R}$$

Let $p_n : \mathcal{H} \to \mathcal{H}_n^L \otimes \mathcal{H}_n^R$ be orthogonal projections. Then since $p_n \in \mathcal{Z}(\mathcal{F}_\mathcal{E})$, we must have

$$E_\mathcal{E}(a) = \sum_{i,j} E_\mathcal{E}(p_i a p_j) = \sum_i p_i E_\mathcal{E}(p_i a p_i) p_i, \quad a \in B(\mathcal{H})$$

Further, we have for $a_n \in B(\mathcal{H}_n^L)$, $b_n \in B(\mathcal{H}_n^R)$

$$E_\mathcal{E}(a_n \otimes b_n) = E_\mathcal{E}((a_n \otimes I_{\mathcal{K}_n})(I_{\mathcal{H}_n^L} \otimes b_n)) = (a_n \otimes I) E_\mathcal{E}(I \otimes b_n) = E_\mathcal{E}(I \otimes b_n)(a_n \otimes I)$$

so that $E_\mathcal{E}(I_{\mathcal{H}_n^L} \otimes b_n)$ is in the center of $B(\mathcal{H}_n^L) \otimes I$ and hence is a multiple of identity. Since $E_\mathcal{E}$ is a channel, it follows that there exists some density operator $\omega_n \in B(\mathcal{H}_n^R)$, such that

$$E_\mathcal{E}(I_{\mathcal{H}_n^L} \otimes b_n) = \mathrm{Tr}\,[\omega_n b_n] I_{\mathcal{H}_n^R} =: \phi_{\omega_n}(b_n)$$

Hence

$$E_\mathcal{E} = \sum_n (id_{B(\mathcal{H}_n^L)} \otimes \phi_{\omega_n})(p_n \cdot p_n). \tag{3}$$

Let $\varphi \in \mathcal{S}$ and let ρ_φ be the corresponding density operator. Then it follows that

$$\rho_\varphi = E_\mathcal{E}^*(\rho_\varphi) = \sum_n \lambda_n^\varphi \rho_n^\varphi \otimes \omega_n,$$

where $\rho_n^\varphi = (\lambda_n^\varphi)^{-1} \mathrm{Tr}_{\mathcal{H}_n^R}(p_n \rho_\varphi p_n)$ if $\lambda_n^\varphi := \mathrm{Tr}\,[\rho_\varphi p_n] > 0$. Note that ρ_n^φ is a density operator on $\mathcal{H}_n^L$ and $\{\lambda_n^\varphi\}$ is a probability distribution. Since $E_\mathcal{E}$ is normal, we must have $\psi \circ E_\mathcal{E} = E_\mathcal{E}$ also for all $\psi \in \bar{co}(\mathcal{S})$, in particular for the faithful state ω. It follows that $\mathrm{supp}(\omega_n) = I_{\mathcal{H}_n^R}$ for all n.

Theorem 2. *Let $\mathcal{M} = B(\mathcal{H})$ for a separable Hilbert space and let $\mathcal{S}$ and $\mathcal{I}_{\mathcal{E}}$ be as above. Then there is a decomposition $\mathcal{H} = \oplus_n \mathcal{H}_n^L \otimes \mathcal{H}_n^R$ and faithful density operators ω_n on $B(\mathcal{H}_n^R)$ such that*

(i) A density operator ρ on $\mathcal{H}$ is Φ-invariant, that is $\Phi^*(\rho) = \rho$, for all $\Phi \in \mathcal{I}_{\mathcal{E}}$ if and only if

$$\rho = \sum_n \lambda_n \rho_n \otimes \omega_n,$$

for some density operators ρ_n on $\mathcal{H}_n^L$ and a probability distribution $\{\lambda_n\}$.

(ii) A channel Φ on $B(\mathcal{H})$ is in $\mathcal{I}_{\mathcal{E}}$ if and only if the restriction $\Phi_n = \Phi|_{B(\mathcal{H}_n^L \otimes \mathcal{H}_n^R)}$ has the form

$$\Phi_n = id_{B(\mathcal{H}_n^L)} \otimes \Psi_n^\Phi$$

for some channel Ψ_n^Φ on $B(\mathcal{H}_n^R)$ such that $(\Psi_n^\Phi)^*(\omega_n) = \omega_n$.

Moreover, for each n, ω_n is the unique element in $\mathfrak{S}(\mathcal{H}_n^R)$ that is invariant under all Ψ_n^Φ, $\Phi \in \mathcal{I}_{\mathcal{E}}$.

Proof. By Lemma 2, ρ is Φ-invariant for all $\Phi \in \mathcal{I}_{\mathcal{E}}$ if and only if $E_{\mathcal{E}}^*(\rho) = \rho$. The statement (i) now follows easily from (3).

For (ii), assume that $\Phi \in \mathcal{I}_{\mathcal{E}}$. Then $\mathcal{F}_{\mathcal{E}} \subseteq \mathcal{F}_\Phi \subseteq \mathcal{M}_\Phi$. Hence for all n, $\Phi(p_n) = p_n$ and $\Phi(p_n B(\mathcal{H}) p_n) \subseteq p_n B(\mathcal{H}) p_n$. Therefore the restriction Φ_n defines a channel on $B(\mathcal{H}_n^L \otimes \mathcal{H}_n^R)$. Further, for any $a_n \in B(\mathcal{H}_n^L)$, $b_n \in B(\mathcal{H}_n^R)$,

$$\begin{aligned}\Phi_n(a_n \otimes b_n) = \Phi_n((a_n \otimes I)(I \otimes b_n)) &= (a_n \otimes I)\Phi_n(I \otimes b_n) \\ = \Phi_n((I \otimes b_n)(a_n \otimes I)) &= \Phi_n(I \otimes b_n)(a_n \otimes I)\end{aligned}$$

It follows that $\Phi_n(I \otimes b_n) \in (B(\mathcal{H}_n^L) \otimes I)' = I \otimes B(\mathcal{H}_n^R)$. It is now easy to see that $\Phi_n(I \otimes b_n) = I \otimes \Psi_n^\Phi(b_n)$ for some channel Ψ_n^Φ on $B(\mathcal{H}_n^R)$, $\Phi_n = id_{B(\mathcal{H}_n^L)} \otimes \Psi_n^\Phi$ and that for any $\varphi \in \mathcal{S}$,

$$\rho_\varphi = \Phi^*(\rho_\varphi) = \sum_n \lambda_n^\varphi \rho_n^\varphi \otimes (\Psi_n^\Phi)^*(\omega_n).$$

Since $\mathcal{S}$ is faithful, for any n there must be some $\varphi \in \mathcal{S}$ such that $\lambda_n^\varphi > 0$. It follows that for all n, ω_n must be Ψ_n^Φ-invariant.

Conversely, if Φ has this form, then again $\Phi(p_n) = p_n$, so that p_n is in the multiplicative domain of Φ. By (3), we have for all $a \in B(\mathcal{H})$

$$E_{\mathcal{E}}(\Phi(a)) = \sum_n (id_{B(\mathcal{H}_n^L)} \otimes \phi_{\omega_n})(p_n \Phi(a) p_n) = \sum_n (id_{B(\mathcal{H}_n^L)} \otimes \phi_{\omega_n})(\Phi_n(p_n a p_n))$$
$$= \sum_n (id_{B(\mathcal{H}_n^L)} \otimes \phi_{\omega_n} \circ \Psi_n^{\Phi})(p_n a p_n) = E_{\mathcal{E}}(a),$$

so that $\Phi \in \mathcal{I}_{\mathcal{E}}$ by Lemma 2.

To prove the last statement, assume that for some n, $\omega_n' \in \mathfrak{S}(\mathcal{H}_n^R)$ is invariant under all channels Ψ_n^{Φ}, $\Phi \in \mathcal{I}_{\mathcal{E}}$. Then for any $\rho_n \in \mathfrak{S}(\mathcal{H}_n^L)$, $\rho_n \otimes \omega_n'$ is an invariant state for all $\Phi \in \mathcal{I}_{\mathcal{E}}$, so that $\rho_n \otimes \omega_n' = E_{\mathcal{E}}^*(\rho_n \otimes \omega_n') = \rho_n \otimes \omega_n$, hence $\omega_n' = \omega_n$.

$\square$

In particular, in the situation of Example 1, we obtain that if $\mathcal{M} = B(\mathcal{H})$, the invariant states of Φ are precisely those of the form as in (i) and Φ has the property (ii), where for all n, ω_n must be the unique invariant state for Ψ_n^{Φ}.

2.3 Characterizations of sufficient channels

Throughout this section, α is a faithful channel $\mathcal{N} \to \mathcal{M}$. The next result follows immediately from definition of a sufficient channel and Lemma 2.

Proposition 2. *α is sufficient with respect to $\mathcal{E}$ if and only if there is some channel $\beta : \mathcal{M} \to \mathcal{N}$ such that $\alpha \circ \beta = E_{\mathcal{E}}$.*

Lemma 3. *Let $\mathcal{M}_0 \subseteq \mathcal{M}$ be the range of a faithful normal conditional expectation E. Then $\alpha \circ \beta = E$ for some some channel $\beta : \mathcal{M} \to \mathcal{N}$ if and only if there is a subalgebra $\mathcal{N}_0 \subseteq \mathcal{N}$, such that $\alpha|_{\mathcal{N}_0}$ is an isomorphism onto $\mathcal{M}_0$. Moreover, in this case:*

(i) $\beta|_{\mathcal{M}_0} = (\alpha|_{\mathcal{N}_0})^{-1}$.

(ii) *$\mathcal{N}_0$ is the range of a conditional expectation $\tilde{E} = \beta \circ E \circ \alpha$.*

(iii) *If $\omega \in \mathfrak{S}(\mathcal{M})$ is faithful and such that E preserves ω, then $\tilde{E}$ preserves $\omega \circ \alpha$ and we have*

$$\sigma_t^{\omega}(\alpha(a)) = \alpha(\sigma_t^{\omega \circ \alpha}(a)), \qquad \forall t \in \mathbb{R},\ a \in \mathcal{N}_0.$$

Proof. Assume that $\alpha \circ \beta = E$ and put $\mathcal{N}_0 = \beta(\mathcal{M}_0)$. Then for $a \in \mathcal{M}_0$,

$$a^*a = \alpha \circ \beta(a^*a) \geq \alpha(\beta(a)^*\beta(a)) \geq \alpha(\beta(a))^*\alpha(\beta(a)) = a^*a. \qquad (4)$$

Since α is faithful, this implies that $\mathcal{N}_0$ is a subalgebra and $\alpha|\mathcal{N}_0$ is an isomorphism onto $\mathcal{M}_0$. Conversely, if $\alpha|_{\mathcal{N}_0}$ is an isomorphism, put $\beta' := (\alpha|_{\mathcal{N}_0})^{-1} \circ E$, then clearly $\alpha \circ \beta' = E$. Moreover, it is easy to see that $\tilde{E} := \beta' \circ \alpha$ is a conditional expectation. Since for any $a \in \mathcal{N}_0$, $\tilde{E}(a) = a$, we have $\mathcal{N}_0 \subseteq \tilde{E}(\mathcal{N}) \subseteq \beta'(\mathcal{M}) \subseteq \mathcal{N}_0$. Hence $\mathcal{N}_0$ is the range of $\tilde{E}$.

Let now $\beta : \mathcal{M} \to \mathcal{N}$ be any channel such that $\alpha \circ \beta = E$, then from (4) we see that $\beta|_{\mathcal{M}_0}$ is an isomorphism and it is clear that $\beta|_{\mathcal{M}_0} = (\alpha|_{\mathcal{N}_0})^{-1}$. Then

$$\beta \circ E \circ \alpha = (\alpha|_{\mathcal{N}_0})^{-1} \circ E \circ \alpha = \beta' \circ \alpha = \tilde{E}.$$

To prove (iii), let ω be a faithful state such that $\omega \circ E = \omega$, then $\omega \circ \alpha \circ \tilde{E} = \omega \circ E \circ \alpha = \omega \circ \alpha$. It follows that $\sigma_t^{\omega\circ\alpha}|_{\mathcal{N}_0} = \sigma_t^{\omega\circ\alpha|_{\mathcal{N}_0}}$. Similarly, $\sigma_t^{\omega}|_{\mathcal{M}_0} = \sigma_t^{\omega|_{\mathcal{M}_0}}$. Since $\alpha|_{\mathcal{N}_0}$ is an isomorphism onto $\mathcal{M}_0$ and the restriction of β is its inverse, it is easy to see that

$$\sigma_t^{\omega\circ\alpha|_{\mathcal{N}_0}} = \beta \circ \sigma_t^{\omega|_{\mathcal{M}_0}} \circ \alpha|_{\mathcal{N}_0} = \beta \circ \sigma_t^{\omega} \circ \alpha|_{\mathcal{N}_0}.$$

Hence for $a \in \mathcal{N}_0$ and $t \in \mathbb{R}$,

$$\alpha(\sigma_t^{\omega\circ\alpha}(a)) = \alpha \circ \beta \circ \sigma_t^{\omega}(\alpha(a)) = \sigma_t^{\omega}(\alpha(a)).$$

□

Corollary 1. *α is sufficient for $\mathcal{E}$ if and only if there is some subalgebra $\mathcal{N}_0 \subseteq \mathcal{N}$ such that the restriction $\alpha|_{\mathcal{N}_0}$ is an isomorphism onto $\mathcal{F}_{\mathcal{E}}$. In this case, $\mathcal{N}_0 = \mathcal{F}_{\mathcal{E}\circ\alpha}$ and a channel $\beta : \mathcal{M} \to \mathcal{N}$ is a recovery map if and only if $\beta|_{\alpha(\mathcal{N}_0)} = (\alpha|_{\mathcal{N}_0})^{-1}$.*

Proof. The only thing left to prove is that $\mathcal{N}_0 = \mathcal{F}_{\mathcal{S}\circ\alpha}$. The rest follows by Proposition 2, Lemma 3 and Lemma 2 (i). We also have that $\mathcal{N}_0$ is the range of a conditional expectation $\tilde{E}$ and that $\tilde{E} = \beta \circ E_{\mathcal{E}} \circ \alpha$ for any recovery channel β. For any $\varphi \in \mathcal{S}$,

$$\varphi \circ \alpha \circ \tilde{E} = \varphi \circ \alpha \circ \beta \circ E_{\mathcal{E}} \circ \alpha = \varphi \circ E_{\mathcal{E}} \circ \alpha = \varphi \circ \alpha.$$

It follows that $\tilde{E} \in \mathcal{I}_{\mathcal{E}\circ\alpha}$, so that $E_{\mathcal{E}\circ\alpha} \circ \tilde{E} = \tilde{E} \circ E_{\mathcal{E}\circ\alpha} = E_{\mathcal{E}\circ\alpha}$. On the other hand, we have

$$\varphi \circ \alpha \circ E_{\mathcal{E}\circ\alpha} \circ \beta = \varphi \circ \alpha \circ \beta = \varphi,$$

so that $\alpha\circ E_{\mathcal{E}\circ\alpha}\circ\beta\in\mathcal{I}_{\mathcal{E}}$ and hence $(\alpha\circ E_{\mathcal{E}\circ\alpha}\circ\beta)\circ E_{\mathcal{E}}=E_{\mathcal{E}}$. By precomposing with α, it follows that

$$E_{\mathcal{E}}\circ\alpha=(\alpha\circ E_{\mathcal{E}\circ\alpha}\circ\beta)\circ E_{\mathcal{E}}\circ\alpha=\alpha\circ E_{\mathcal{E}\circ\alpha}\circ\tilde{E}=\alpha\circ E_{\mathcal{E}\circ\alpha}.$$

It follows that

$$E_{\mathcal{E}\circ\alpha}=\tilde{E}\circ E_{\mathcal{E}\circ\alpha}=\beta\circ E_{\mathcal{E}}\circ\alpha\circ E_{\mathcal{E}\circ\alpha}=\beta\circ E_{\mathcal{E}}\circ\alpha=\tilde{E}.$$

□

Corollary 2. *[4] α is sufficient for $\mathcal{E}$ if and only if*

$$\alpha([D\varphi\circ\alpha,D\omega\circ\alpha]_t)=[D\varphi,D\omega]_t,\qquad\forall t\in\mathbb{R},\ \varphi\in\mathcal{S}.$$

Proof. Assume that α is sufficient and let $u_t:=[D\varphi\circ\alpha,D\omega\circ\alpha]_t$ and $v_t:=\alpha(u_t)$. Then by Corollary 1 and Theorem 1, $u_t\in\mathcal{F}_{\mathcal{E}\circ\alpha}\subseteq\mathcal{M}_\alpha$, so that v_t is a unitary in $\mathcal{M}$ for all t. Moreover, by Lemma 3, $\alpha(\sigma_s^{\omega\circ\alpha}(u_t))=\sigma_s^\omega(v_t)$, this implies that v_t satisfies the cocycle condition with respect to ω. It follows that there is a unique $\psi\in\mathfrak{S}(\mathcal{M})$ such that $v_t=[D\psi,D\omega]_t$.

$\mathcal{F}_{\mathcal{E}\circ\alpha}$ is generated by the cocycle derivatives. It follows that $u_t:=\alpha([D\varphi\circ\alpha,D\omega\circ\alpha]_t)$ is a unitary in $\mathcal{M}$ and by Lemma 3 (iii),

Since $\tilde{E}$ is an $\omega\circ\alpha$-preserving conditional expectation onto $\mathcal{F}|_{\mathcal{S}\circ\alpha}$, this subalgebra is invariant under the modular group $\sigma^{\omega\circ\alpha}$. It follows that $\sigma_t^{\omega\circ\alpha}|_{\mathcal{F}_{\mathcal{E}\circ\alpha}}=\sigma_t^{\omega\circ\alpha|_{\mathcal{F}_{\mathcal{E}\circ\alpha}}}$. Similarly, $\sigma_t^\omega|_{\mathcal{F}_{\mathcal{E}}}=\sigma_t^{\omega|_{\mathcal{F}_{\mathcal{E}}}}$. Let β be any recovery map. Then since $\alpha|_{\mathcal{F}_{\mathcal{E}\circ\alpha}}$ is an isomorphism onto $\mathcal{F}_{\mathcal{E}}$ and the restriction of β is its inverse, it is easy to see that

$$\sigma_t^{\omega\circ\alpha|_{\mathcal{F}_{\mathcal{E}\circ\alpha}}}=\beta\circ\sigma_t^{\omega|_{\mathcal{F}_{\mathcal{E}}}}\circ\alpha=\beta\circ\sigma_t^\omega\circ\alpha|_{\mathcal{F}_{\mathcal{E}\circ\alpha}}.$$

Hence for $a\in\mathcal{F}_{\mathcal{E}\circ\alpha}$ and $t\in\mathbb{R}$,

$$\alpha(\sigma_t^{\omega\circ\alpha}(a))=\alpha\circ\beta\circ\sigma_t^\omega(\alpha(a))=\sigma_t^\omega(\alpha(a)).$$

□

Let us now return to the case when $\mathcal{M}=B(\mathcal{H})$.

Proposition 3. *Assume that $\mathcal{M}=B(\mathcal{H})$ and $\alpha:B(\mathcal{K})\to B(\mathcal{H})$ is a faithful channel. Let $\mathcal{H}=\oplus_n\mathcal{H}_n^L\otimes\mathcal{H}_n^R$ is the decomposition such that E has the form (3). Then the following are equivalent.*

(i) α is sufficient with respect to $\mathcal{E}$.

(ii) There is a decomposition $\mathcal{K} = \oplus_n \mathcal{K}_n^L \otimes \mathcal{K}_n^R$, unitaries $u_n : \mathcal{K}_n^L \to \mathcal{H}_n^L$ and faithful channels $\alpha_n^R : B(\mathcal{K}_n^R) \to B(\mathcal{H}_n^R)$ such that the restrictions $\alpha_n := \alpha|_{B(\mathcal{K}_n^L \otimes \mathcal{K}_n^R)}$ have the form

$$\alpha_n = u_n \cdot u_n^* \otimes \alpha_n^R$$

(iii) There is a decomposition $\mathcal{K} = \oplus_n \mathcal{K}_n^L \otimes \mathcal{K}_n^R$, unitaries $u_n : \mathcal{K}_n^L \to \mathcal{H}_n^L$ and faithful channels $\alpha_n^R : B(\mathcal{K}_n^R) \to B(\mathcal{H}_n^R)$ such that for all $\varphi \in \mathcal{S}$,

$$\alpha^*(\rho_\varphi) = \sum_n \lambda_n^\varphi u_n^* \rho_n^\varphi u_n \otimes (\alpha_n^R)^*(\omega_n)$$

Proof. Assume (i) and let $\mathcal{K} = \oplus_n \mathcal{K}_n^L \otimes \mathcal{K}_n^R$ be such that

$$\mathcal{F}_{\mathcal{E}\circ\alpha} = \bigoplus_n B(\mathcal{K}_n^L) \otimes I_{\mathcal{K}_n^R}$$

similarly to (3). By Corollary 1, α restricts to an isomorphism $\mathcal{F}_{\mathcal{E}\circ\alpha}$ onto $\mathcal{F}_{\mathcal{E}}$ and we may assume that $\alpha(B(\mathcal{K}_n^L) \otimes I_{\mathcal{K}_n^R}) = B(\mathcal{H}_n^L) \otimes I_{\mathcal{H}_n^R}$, so that there are unitaries $u_n : \mathcal{K}_n^L \to \mathcal{H}_n^L$ implementing this isomorphism. Further, similarly as in the proof of Theorem **??**, $\alpha(I_{\mathcal{K}_n^L} \otimes B(\mathcal{K}_n^R)) \subseteq I_{\mathcal{H}_n^L} \otimes B(\mathcal{H}_n^R)$, so that α induces a channel $\alpha_n^R : B(\mathcal{K}_n^R) \to B(\mathcal{H}_n^R)$, such that for all $a_n \in B(\mathcal{K}_n^L)$, $b_n \in B(\mathcal{K}_n^R)$,

$$\alpha(a_n \otimes b_n) = \alpha(a_n \otimes I)\alpha(I \otimes b_n) = u_n a_n u_n^* \otimes \alpha_n^R(b_n),$$

this is (ii). The implication (ii) $\implies$ (iii) is quite clear from Theorem **??**. Finally, let (iii) be true and let $\beta = \sum_n u_n \cdot u_n^* \otimes id_{\mathcal{H}_n^R} \circ E$, then it is clear that $\beta^*(\alpha^*(\rho_\varphi)) = \rho_\varphi$.

□

2.4 Maximal experiments

In the previous section, we described all sufficient channels for a given experiment. We will now fix a faithful channel $\alpha : \mathcal{N} \to \mathcal{M}$ and describe the (faithful) experiments on $\mathcal{M}$ such that α is sufficient.

Let ω be a faithful normal state on $\mathcal{M}$ and let $\omega_0 = \omega \circ \alpha$, then ω_0 is a faithful element in $\mathfrak{S}(\mathcal{N})$. Let σ_t^ω be the modular group of ω. Let

$$\mathcal{M}_{\alpha,\omega} := \{b \in \alpha(\mathcal{M}_\alpha),\ \sigma_t^\omega(b) \in \alpha(\mathcal{M}_\alpha),\ \forall t \in \mathbb{R}\}.$$

Then $\mathcal{M}_{\alpha,\omega}$ is the largest subalgebra in $\alpha(\mathcal{M}_\alpha)$, invariant under the modular group σ^ω. Let $E_{\alpha,\omega}$ be the ω-preserving conditional expectation onto $\mathcal{M}_{\alpha,\omega}$.

Proposition 4. *Let $\mathcal{S}_{\alpha,\omega} = \{\varphi \circ E_{\alpha,\omega},\ \varphi \in \mathfrak{S}(\mathcal{M})\}$ and $\mathcal{E}_{\alpha,\omega} = (\mathcal{M}, \mathcal{S}_{\alpha,\omega})$. Let $\phi \in \mathcal{S}(\mathcal{M})$ be a faithful state .Then*

(i) $\mathcal{M}_{\alpha,\omega}$ is the minimal sufficient subalgebra with respect to $\mathcal{E}_{\alpha,\omega}$.

(ii) α is sufficient with respect to $\mathcal{E}_{\alpha,\omega}$.

(iii) $E_{\alpha,\phi} = E_{\alpha,\omega}$ if and only if $\phi \in \mathcal{S}_{\alpha,\omega}$.

Proof. Assume that F is the conditional expectation onto the minimal sufficient subalgebra $\mathcal{F}_{\mathcal{E}_{\alpha,\omega}}$, then since $E_{\alpha,\omega} \in \mathcal{I}_{\mathcal{E}_{\alpha,\omega}}$, we must have $E_{\alpha,\omega} \circ F = F$ and simultaneously

$$\varphi \circ E_{\alpha,\omega} \circ F = \varphi \circ E_{\alpha,\omega}, \qquad \forall \varphi \in \mathcal{S}(\mathcal{M}).$$

Hence $F = E_{\alpha,\omega} \circ F = E_{\alpha,\omega}$. This proves (i).

Since the restriction $\alpha|_{\mathcal{M}_\alpha}$ is an isomorphism, the pre-image

$$\tilde{\mathcal{M}}_{\alpha,\omega} := \{a \in \mathcal{M}_\alpha, \alpha(a) \in \mathcal{M}_{\alpha,\omega}\}$$

is a subalgebra in $\mathcal{M}_\alpha$ and (ii) follows by Proposition 2.

Assume $\phi \in \mathcal{S}_{\alpha,\omega}$, then $\phi \circ E_{\alpha,\omega} = \phi$. It follows that $\mathcal{M}_{\alpha,\omega}$ is invariant under σ_t^ϕ, so that $\mathcal{M}_{\alpha,\omega} \subseteq \mathcal{M}_{\alpha,\phi}$. But then $\mathcal{M}_{\alpha,\phi}$ is sufficient with respect to $\mathcal{E}_{\alpha,\omega}$ and Proposition **??** applies (with ϕ in the role of ω). Hence $E_{\alpha,\omega} \circ E_{\alpha,\phi} = E_{\alpha,\omega}$ and $\omega \circ E_{\alpha,\phi} = \omega$. By the same reasoning as before, $\mathcal{M}_{\alpha,\phi} \subseteq \mathcal{M}_{\alpha,\omega}$. By uniqueness of the conditional expectation, $E_{\alpha,\omega} = E_{\alpha,\phi}$. The converse of (iii) is quite obvious.

□

Proposition 5. *Let $\omega, \phi \in \mathfrak{S}(\mathcal{M})$ be faithful. Then*

(i) $\mathcal{M}_{\alpha,\omega} \subseteq \mathcal{M}_{\alpha,\phi}$ if and only if

$$[D\omega|_{\mathcal{M}_{\alpha,\phi}}, D\phi|_{\mathcal{M}_{\alpha,\phi}}]_t [D\phi, D\omega]_t \in \mathcal{M}'_{\alpha,\omega}$$

(ii) $\mathcal{M}_{\alpha,\omega} = \mathcal{M}_{\alpha,\phi}$ *if and only if*

$$[D\omega|_{\mathcal{M}_{\alpha,\phi}}, D\phi|_{\mathcal{M}_{\alpha,\phi}}]_t[D\phi, D\omega]_t \in \mathcal{M}'_{\alpha,\omega} \cap \mathcal{M}'_{\alpha,\phi}$$

Proof. Suppose $\mathcal{M}_{\alpha,\omega} \subseteq \mathcal{M}_{\alpha,\phi}$. Then clearly $E_{\alpha,\phi} \circ E_{\alpha,\omega} = E_{\alpha,\omega}$. Put $F := E_{\alpha,\omega} \circ E_{\alpha,\phi}$, then it is easy to see that F is a conditional expectation and $F(\mathcal{M}) \subseteq \mathcal{M}_{\alpha,\omega}$. On the other hand, we have $F \circ E_{\alpha,\omega} = E_{\alpha,\omega}$, so that $\mathcal{M}_{\alpha,\omega} \subseteq F(\mathcal{M})$. It follows that F and $E_{\alpha,\omega}$ have the same range, but since F does not necessarily preserve ω, the conditional expectations might be not equal. Now put $\omega_0 = \omega|_{\mathcal{M}_{\alpha,\phi}}$, $\phi_0 = \phi|_{\mathcal{M}_{\alpha,\phi}}$. Then $\phi_0 \circ E_{\alpha,\phi} = \phi$ and $\omega_0 \circ E_{\alpha,\phi} = \omega \circ F =: \omega'$. By the chain rule for cocycle derivatives [5, Theorem VIII.3.7], we have

$$[D\phi, D\omega]_t = [D\phi, D\omega']_t[D\omega', D\omega]_t, \qquad \forall t \in \mathbb{R}.$$

Moreover, by [5, Corollary IX.4.22],

$$[D\phi, D\omega']_t = [D\phi_0 \circ E_{\alpha,\phi}, D\omega_0 \circ E_{\alpha,\phi}]_t = D[\phi_0, D\omega_0]_t, \quad \forall t \in \mathbb{R}$$

and

$$[D\omega', D\omega]_t = [D\omega \circ F, D\omega \circ E_{\alpha,\omega}]_t \in \mathcal{M}'_{\alpha,\omega}, \qquad \forall t \in \mathbb{R}.$$

Hence

$$[D\omega_0, D\phi_0]_t[D\phi, D\omega]_t = [D\phi_0, D\omega_0]_t^*[D\phi, D\omega]_t = [D\omega', D\omega]_t \in \mathcal{M}'_{\alpha,\omega}$$

Conversely, assume the condition in (i) holds and let $a \in \mathcal{M}_{\alpha,\omega}$. Then by the cocycle derivative theorem [5, Theorem VIII.3.3],

$$\begin{aligned}\sigma_t^{\phi}(a) &= [D\phi, D\omega]_t\sigma_t^{\omega}(a)[D\phi, D\omega]_t^* \\ &= [D\omega|_{\mathcal{M}_{\alpha,\phi}}, D\phi|_{\mathcal{M}_{\alpha,\phi}}]_t^*\sigma_t^{\omega}(a)[D\omega|_{\mathcal{M}_{\alpha,\phi}}, D\phi|_{\mathcal{M}_{\alpha,\phi}}]_t \in \alpha(\mathcal{M}_\alpha)\end{aligned}$$

It follows that $\mathcal{M}_{\alpha,\omega} \subseteq \mathcal{M}_{\alpha,\phi}$.

For (ii), assume the condition holds. Then $\mathcal{M}_{\alpha,\omega} \subseteq \mathcal{M}_{\alpha,\phi}$ by (i). Let ω_0 and ϕ_0 be as above, then

$$[D\omega, D\phi]_t = [D\phi, D\omega]_t^* = u_t^*[D\phi_0, D\omega_0]_t^* = [D\omega_0, D\phi_0]_t u_t^*,$$

where u_t is some unitary in $\mathcal{M}'_{\alpha,\omega} \cap \mathcal{M}'_{\alpha,\phi}$. For $a \in \mathcal{M}_{\alpha,\phi}$,

$$\sigma_t^{\omega}(a) = [D\omega, D\phi]_t\sigma_t^{\phi}(a)[D\omega, D\phi]_t^* = [D\omega_0, D\phi_0]_t\sigma_t^{\phi}(a)[D\omega_0, D\phi_0]_t^* \in \alpha(\mathcal{M}_\alpha),$$

so that $\mathcal{M}_{\alpha,\phi} \subseteq \mathcal{M}_{\alpha,\omega}$. The converse of (ii) is straightforward from (i).

□

We now show that the experiment $\mathcal{E}_{\alpha,\omega}$ is maximal in some sense.

Proposition 6. *Let $\mathcal{E} = (\mathcal{M}, \mathcal{S})$ be any experiment such that $\omega \in \bar{co}(\mathcal{S})$. Then the following are equivalent.*

(i) α is sufficient with respect to $\mathcal{E}$.

(ii) $\mathcal{F}_{\mathcal{E}} \subseteq \mathcal{M}_{\alpha,\omega}$.

(iii) $\mathcal{S} \subseteq \mathcal{S}_{\alpha,\omega}$.

Moreover, if any of the above holds, any recovery map for $\mathcal{E}_{\alpha,\omega}$ is a recovery map for $\mathcal{E}$.

Proof. Assume (i), then by Proposition 2, $\mathcal{F}_{\mathcal{E}} \subseteq \alpha(\mathcal{M}_\alpha)$. Since $\sigma_t^\omega(\mathcal{F}_{\mathcal{E}}) = \mathcal{F}_{\mathcal{E}}$, we have (ii). Further, assume $\mathcal{F}_{\mathcal{E}} \subseteq \mathcal{M}_{\alpha,\omega}$, then $\mathcal{M}_{\alpha,\omega}$ is sufficient for $\mathcal{E}$ and by Proposition **??**, $E_{\alpha,\omega} \in \mathcal{I}_{\mathcal{E}}$, this implies (iii). Finally, assume (iii), then since α is sufficient with respect to $\mathcal{E}_{\alpha,\omega}$, α is sufficient for $\mathcal{E}$ and any recovery map for $\mathcal{E}_{\alpha,\omega}$ is a recovery map for $\mathcal{E}$.

□

Lemma 4. *The pre-image $\tilde{\mathcal{M}}_{\alpha,\omega}$ satisfies*

$$\tilde{\mathcal{M}}_{\alpha,\omega} = \{a \in \mathcal{M}_\alpha,\ \sigma_t^\omega(\alpha(a)) = \alpha(\sigma_t^{\omega\circ\alpha}(a)),\ \forall t \in \mathbb{R}\}$$

Proof. Since α is sufficient with respect to $\mathcal{E}_{\alpha,\omega}$ and by Proposition 2, $\tilde{\mathcal{M}}_{\alpha,\omega} = \mathcal{F}_{\mathcal{E}_{\alpha,\omega}\circ\alpha}$, we have by Lemma **??** that $\sigma_t^\omega(\alpha(a)) = \alpha(\sigma_t^{\omega\circ\alpha}(a))$ holds for all $a \in \tilde{\mathcal{M}}_{\alpha,\omega}$ and $t \in \mathbb{R}$. For the converse, it suffices to show that the set on the right hand side is a subalgebra, the statement then follows easily. Since this set is invariant under taking adjoints and $\mathcal{M}_\alpha$ is a subalgebra, it is enough to prove that for any a in this set, $\alpha(\sigma_t^{\omega\circ\alpha}(a^*a)) = \sigma_t^\omega(\alpha(a^*a))$. We have

$$\alpha(\sigma_t^{\omega\circ\alpha}(a^*a)) \geq \alpha(\sigma_t^{\omega\circ\alpha}(a))^*\alpha(\sigma_t^{\omega\circ\alpha}(a)) = \sigma_t^\omega(\alpha(a)^*\alpha(a)) = \sigma_t^\omega(\alpha(a^*a)).$$

By applying ω to both sides, we obtain the equality.

□

2.5 The dual map

We will now describe a universal recovery map, sometime called the Petz dual, or the Petz recovery map.

Let $(\mathcal{H}_\omega, \pi_\omega, \Omega)$ be the GNS-triple with respect to ω, we will identify $\mathcal{M}$ with the representation $\pi_\omega(\mathcal{M})$. Let also $J : \mathcal{H}_\omega \to \mathcal{H}_\omega$ be the modular conjugation and σ_t^ω the modular group. Similarly, let $(\mathcal{H}_{\omega\circ\alpha}, \pi_{\omega\circ\alpha}, \Omega_0)$ be the GNS-triple with respect to $\omega \circ \alpha$ and we denote the modular conjugation by J_0. By [4], the map

$$\mathcal{M} \times \mathcal{M} \ni (a, b) \mapsto \langle a, b\rangle_\omega := \omega(a^* \sigma^\omega_{-i/2}(b)) = \langle a\Omega, Jb^*\Omega\rangle$$

defines a sesquilinear form on $\mathcal{M}$ and

$$\langle \alpha(a), b\rangle_\omega = \langle a, \alpha^*_\omega(b)\rangle_{\omega_0}, \quad a \in \mathcal{N},\ b \in \mathcal{M}$$

defines a channel $\alpha^*_\omega : \mathcal{M} \to \mathcal{N}$. This channel is called the dual map.

Lemma 5. *$\tilde{\mathcal{M}}_{\alpha,\omega}$ is the fixed point set of $\alpha^*_\omega \circ \alpha$ and $\mathcal{M}_{\alpha,\omega}$ is the fixed point set of $\alpha \circ \alpha^*_\omega$.*

Proof. (This was proved in [4].) Let $a \in \tilde{\mathcal{M}}_{\alpha,\omega}$ and let $b \in \mathcal{N}$. Then

$$\begin{aligned}\langle b\Omega_0, J_0\alpha^*_\omega \circ \alpha(a)\Omega_0\rangle &= \langle b, \alpha^*_\omega \circ \alpha(a)\rangle_\omega = \langle \alpha(b), \alpha(a)\rangle_\omega \\ &= \omega(\alpha(b)^* \sigma^\omega_{-i/2}(\alpha(a)))\end{aligned}$$

By analytic continuation, we obtain $\sigma^\omega_{-i/2}(\alpha(a)) = \alpha(\sigma^{\omega\circ\alpha}_{-i/2}(a))$ and $\sigma^{\omega\circ\alpha}_{-i/2}(a) \in \tilde{\mathcal{M}}_{\alpha,\omega} \subseteq \mathcal{M}_\alpha$. It follows that

$$\begin{aligned}\langle b\Omega_0, J_0\alpha^*_\omega \circ \alpha(a)\Omega_0\rangle &= \omega(\alpha(b)^*\alpha(\sigma^{\omega\circ\alpha}_{-i/2}(a))) = \omega \circ \alpha(b^*\sigma^{\omega\circ\alpha}_{-i/2}(a)) \\ &= \langle b\Omega_0, J_0 a\Omega_0\rangle\end{aligned}$$

Since Ω_0 is cyclic and separating, this implies $\alpha^*_\omega \circ \alpha(a) = a$.

For the converse, note that ω is invariant under $\alpha \circ \alpha^*_\omega$. Indeed, for any $b \in \mathcal{M}$,

$$\omega(\alpha \circ \alpha^*_\omega(b)) = \langle 1, \alpha \circ \alpha^*_\omega(b)\rangle_\omega = \langle 1, \alpha^*_\omega(b)\rangle_{\omega\circ\alpha} = \langle 1, b\rangle\omega = \omega(b).$$

It follows that the fixed point set $\mathcal{F}_{\alpha\circ\alpha^*_\omega}$ is a subalgebra in $\mathcal{M}$. Moreover, for $b \in \mathcal{F}_{\alpha\circ\alpha^*_\omega}$,

$$b^*b = \alpha \circ \alpha^*_\omega(b^*b) \geq \alpha(\alpha^*_\omega(b)^*\alpha^*_\omega(b)) \geq \alpha \circ \alpha^*_\omega(b^*)\alpha \circ \alpha^*_\omega(b) = b^*b.$$

It follows that $\alpha^*_\omega(b) \in \mathcal{M}_\alpha$ and $b = \alpha(\alpha^*_\omega(b)) \in \alpha(\mathcal{M}_\alpha)$. Since $\mathcal{F}_{\alpha\circ\alpha^*_\omega}$ is also invariant under σ^ω_t, we obtain $\mathcal{F}_{\alpha\circ\alpha^*_\omega} \subseteq \mathcal{M}_{\alpha,\omega}$. On the other hand, it is easy to see that for any $a \in \mathcal{F}_{\alpha^*_\omega\circ\alpha}$, $\alpha(a) \in \mathcal{F}_{\alpha\circ\alpha^*_\omega}$. Now by the first part of the proof and Lemma 4,

$$\mathcal{M}_{\alpha,\omega} = \alpha(\tilde{\mathcal{M}}_{\alpha,\omega}) \subseteq \alpha(\mathcal{F}_{\alpha^*_\omega\circ\alpha}) \subseteq \mathcal{F}_{\alpha\circ\alpha^*_\omega} \subseteq \mathcal{M}_{\alpha,\omega},$$

so that all the inclusions are in fact equalities. The proof now follows from the fact that $\alpha|_{\mathcal{M}_\alpha}$ is an isomorphism.

□

Corollary 3. *α^*_ω is a recovery channel for $\mathcal{E}_{\alpha,\omega}$.*

Proof. Put $\Phi = \alpha \circ \alpha^*_\omega$, then by Lemma 5 and Example 1, $\mathcal{M}_{\alpha,\omega} = \mathcal{F}_\Phi$ is the minimal sufficient subalgebra with respect to $\mathcal{S}_\Phi$ and $\varphi \circ \Phi = \varphi$ if (and only if) $\varphi \circ E_{\alpha,\omega} = \varphi$. Hence α^*_ω is a recovery channel for $\mathcal{E}_{\alpha,\omega}$.

□

Theorem 3. *[4] The following are equivalent.*

(i) α is sufficient for $\mathcal{E}$.

(ii) $\varphi \circ \alpha \circ \alpha^*_\omega = \varphi$, for all $\varphi \in \mathcal{S}$.

(iii) $\alpha^*_\omega = \alpha^*_\phi$ for all faithful states $\phi \in \bar{co}(\mathcal{S})$.

Proof. The equivalence of (i) and (ii) is clear from Corollary 3 and Proposition 6. Assume (iii), and let $\varphi \in \mathcal{S}$, then $\phi := \frac{1}{2}(\varphi + \omega)$ is a faithful state in $\bar{co}(\mathcal{S})$, hence $\phi \circ \alpha \circ \alpha^*_\omega = \phi \circ \alpha \circ \alpha^*_\phi = \phi$. This clearly implies that $\varphi \circ \alpha \circ \alpha^*_\omega = \varphi$, so that (i) is true.

Finally, suppose (i) and let $\phi \in \bar{co}(\mathcal{S})$ be faithful. Let Ω_ϕ be the vector state for ϕ in the standard representation obtained from the GNS triple, then $\Omega_\phi = [D\phi, D\omega]_{-i/2}\Omega$. Similarly, $\Omega_{\phi\circ\alpha} = [D\phi \circ \alpha, D\omega \circ \alpha]_{-i/2}\Omega_0$. Put $u_t = [D\phi, D\omega]_t$ and $v_t = [D\phi\circ\alpha, D\omega\circ\alpha]_t$, then by (i) $v_t \in \mathcal{M}_\alpha$ and $u_t = \alpha(v_t)$, so that for any $a \in \mathcal{N}$, $b \in \mathcal{M}$ and $t \in \mathbb{R}$,

$$\begin{aligned}\langle \alpha(a)u_t\Omega, JbJu_t\Omega\rangle &= \langle \alpha(v_t^* a v_t)\Omega, Jb\Omega\rangle = \langle v_t^* a v_t\Omega_0, J_0\alpha^*_\omega(b)J_0\Omega_0\rangle \\ &= \langle a v_t\Omega_0, J_0\alpha^*_\omega(b)J_0 v_t\Omega_0\rangle.\end{aligned}$$

The statement (iii) now follows by analytic continuation.

□

Example 2. Let $\Phi : \mathcal{M} \to \mathcal{M}$ be a quantum channel and let ω be a faithful normal invariant state. Let

$$\mathcal{N}(\Phi) := \cap_n \mathcal{M}_{\Phi^n}, \qquad \mathcal{N}(\Phi, \omega) := \cap_n \tilde{\mathcal{M}}_{\Phi^n,\omega}$$

where $\Phi^n = \Phi \circ \cdots \circ \Phi$ is the n-fold composition of Φ with itself. It is quite clear that $\mathcal{N}(\Phi)$ is invariant under Φ (note that this is not necessarily true for $\mathcal{M}_\Phi$). Observe also that

$$\begin{aligned}\mathcal{N}(\Phi, \omega) &= \{a \in \mathcal{N}(\Phi), \Phi^n(\sigma_t^\omega(a)) = \sigma_t^\omega(\Phi^n(a)),\ t \in \mathbb{R}\}\\ &= \{a \in \mathcal{N}(\Phi),\ \sigma_t(a) \in \mathcal{N}(\Phi),\ t \in \mathbb{R}\} = \cap_n \mathcal{M}_{\Phi^n,\omega}\\ &= \cap_n \mathcal{F}_{(\Phi^n)^*_\omega \circ \Phi^n} = \cap_n \mathcal{F}_{\Phi^n \circ (\Phi^n)^*_\omega}\end{aligned}$$

in particular, $\mathcal{N}(\Phi, \omega)$ is the largest subalgebra in $\mathcal{N}(\Phi)$ invariant under the modular group σ^ω. Indeed, the first equality is clear from definition of $\tilde{\mathcal{M}}_{\Phi^n,\omega}$ and the fact that ω is an invariant state. Further, it is easy to see that $\mathcal{N}(\Phi, \omega)$ is invariant under Φ and since $\Phi^n(\tilde{\mathcal{M}}_{\Phi^n,\omega}) = \mathcal{M}_{\Phi^n,\omega}$, we have

$$\mathcal{N}(\Phi, \omega) = \Phi^n(\mathcal{N}(\Phi, \omega)) \subseteq \Phi^n(\tilde{\mathcal{M}}_{\Phi^n,\omega}) = \mathcal{M}_{\Phi^n,\omega}, \qquad n \in \mathbb{N}.$$

It follows that $\mathcal{N}(\Phi, \omega) \subseteq \cap_n \mathcal{M}_{\Phi^n,\omega}$. For the converse, let us denote $\mathcal{M}_1 := \cap_n \mathcal{M}_{\Phi^n,\omega}$. Note that since $\mathcal{M}_1 \subseteq \mathcal{M}_{\Phi^n,\omega}$ for all n, we have $(\Phi|_{\mathcal{M}_1})^{-1} = \Phi^*_\omega|_{\mathcal{M}_1}$ and

$$(\Phi^*_\omega|_{\mathcal{M}_1})^n = (\Phi^n|_{\mathcal{M}_1})^{-1} = (\Phi^n)^*_\omega|_{\mathcal{M}_1}, \quad \forall n.$$

Since $\mathcal{M}_1$ is invariant under σ_t and its preimage under Φ^n is a subalgebra in $\mathcal{M}_{\Phi^n}$, it follows by Lemma 3 (iii) that $(\Phi^n)^{-1}(\mathcal{M}_1) \subseteq \tilde{\mathcal{M}}_{\Phi^n,\omega}$. Moreover, since $\Phi^{-1}(\mathcal{M}_1)$ is a subalgebra in $\mathcal{N}(\Phi)$ invariant under σ_t^ω (again by Lemma 3 (iii)), it follows that $\mathcal{M}_1$ is invariant under $(\Phi|_{\mathcal{M}_1})^{-1} = \Phi^*_\omega|_{\mathcal{M}_1}$. We now have for each n,

$$\mathcal{M}_1 = (\Phi^*_\omega)^n(\mathcal{M}_1) = (\Phi^n)^{-1}(\mathcal{M}_1) \subseteq \tilde{\mathcal{M}}_{\Phi^n,\omega},$$

which shows the opposite inclusion. The last two equalities follow by Lemma 5.

References

[1] B. Kümmerer, R. Nagel, Mean ergodic semigroups on W*-algebras, Acta Sci. Math. 41 (1979), 151-155

[2] A. Luczak, Quantum sufficiency in the operator algebra framework, Int. J. Theor. Phys. 53 (2014), 3423-3433

[3] D. Petz, Sufficient subalgebras and the relative entropy of states of a von Neumann algebra, Commun. Math. Phys. 105 (1986), 123-131

[4] D. Petz, Sufficiency of channels over von Neumann algebras, Quart. J Math. Oxford 39 (1988), 97-108

[5] M. Takesaki, Theory of operator algebras II, Springer-Verlag Berlin Heidelberg, 2003

[6] M. Takesaki, Conditional expectations in von Neumann algebras, J. Funct. Anal. **9** (1972), 306-321

[7] J. Tomiyama, On the projection of norm one in W*-algebras III., Tohoku Math. J. 11 (1959), 125-129