Privacy and Correctability

Jack Wile

Definition 1. *Let $\mathscr{A}$ and $\mathscr{B}$ be Op^*-algebras over pre-Hilbert spaces $\mathcal{S}_1$ and $\mathcal{S}_2$ and let $\mathcal{E} : \mathscr{A} \mapsto \mathscr{B}$ be a quantum channel. If p is a projection on $\mathcal{S}_2$, an Op^*-algebra $\mathscr{N} \subseteq \mathscr{L}^\dagger(p(\mathcal{S}_2))$ is said to be private for $\mathcal{E}$ with respect to p if*

$$\mathcal{C}_p(\mathcal{E}(\mathscr{A})) \subseteq \mathscr{N}_c'.$$

If $p = I$, then we say that $\mathscr{N}$ is private for $\mathcal{E}$.

Definition 2. *Let $\mathscr{A}_1$ and $\mathscr{A}_2$ be Op^*-algebras over S_1, S_2, respectively and $\mathcal{E} : \mathscr{A}_1 \mapsto \mathscr{A}_2$ a quantum channel. Given a projection p over S_2, an Op^*-algebra $\mathscr{N} \subseteq \mathscr{L}^\dagger(p(S_2))$ is said to be correctable for $\mathcal{E}$ with respect to p if there exists a quantum channel $\mathcal{R} : \mathscr{N} \mapsto \mathscr{A}_1$ such that*

$$\mathcal{C}_p(\mathcal{E}(\mathcal{R})) = I_{\mathscr{N}}.$$

Definition 3. *Let $\mathscr{A}$ and $\mathscr{B}$ be Op^*-algebras over $\mathcal{S}_1$ and $\mathcal{S}_2$, and $\mathcal{E} : \mathscr{A} \mapsto \mathscr{B}$ a quantum channel between them. Given a Stinespring triple $(\pi, v, \mathcal{D})$ for $\mathcal{E}$, we define the complementary channel $\mathcal{E}^c : \pi(\mathscr{A})_c' \mapsto \mathscr{L}^\dagger(\mathcal{S}_2)$ by*

$$\mathcal{E}^c(x) = v^* x v, \quad \forall x \in (\mathscr{A})_c'.$$

Remark 1. *Let $(\pi_1, v_1, \mathcal{D}_1)$ and $(\pi_2, v_2, \mathcal{D}_2)$ be two Stinespring triples for $\mathcal{E}$ in the above definition and $\mathcal{F}_1$, $\mathcal{F}_2$ their respective complementary channels. By the uniqueness of the Stinespring representation we have a partial isometry, $u : \mathcal{D}_1 \mapsto \mathcal{D}_2$, satisfying*

$$uv_1 = v_2, \quad u^* v_2 = v_1 \text{ and } u\pi_1(a) = \pi_2(a)u,$$

for any $a \in \mathscr{A}$. Given $a \in \mathscr{A}$, $x \in \pi_1(\mathscr{A})'_c$ and $\psi, \xi \in \mathcal{D}_1$

$$\begin{aligned}
\langle \pi_2(a)\psi, \mathcal{C}_u(x)\xi \rangle &= \langle \pi_2(a)\psi, uxu^*\xi \rangle \\
&= \langle u^*\pi_2(a)\psi, xu^*\xi \rangle \\
&= \langle \pi_1(a)u^*\psi, xu^*\xi \rangle \\
&= \langle x^\dagger u^*\psi, \pi_1(a^\dagger)u^*\xi \rangle \\
&= \langle x^\dagger u^*\psi, u^*\pi_2(a^\dagger)\xi \rangle \\
&= \langle \mathcal{C}_u(x^\dagger)\psi, \pi_2(a^\dagger)\xi \rangle \\
&= \langle \mathcal{C}_u(x)^\dagger\psi, \pi_2(a)^\dagger\xi \rangle.
\end{aligned}$$

Hence, $\mathcal{C}_u(\pi_1(\mathscr{A})'_c) \subseteq \pi_2(\mathscr{A})'_c$ and by the same argument, $\mathcal{C}_{u^*}(\pi_2(\mathscr{A})'_c) \subseteq \pi_1(\mathscr{A})'_c$. Thus $\mathcal{F}_1(\mathcal{C}_{u^*})$ and $\mathcal{F}_2(\mathcal{C}_u)$ are well-defined and, by the relations u satisfies with respect to v_1 and v_2, $\mathcal{F}_1(\mathcal{C}_{u^*}) = \mathcal{F}_2$ and $\mathcal{F}_2(\mathcal{C}_u) = \mathcal{F}_1$.

Theorem 1 (Arveson's Commutant Lifting Theorem)**.** *Let $\mathcal{E} : \mathscr{A}_1 \mapsto \mathscr{A}_2$ be a quantum channel between Op*-algebras. There exists a Stinespring triple $(\pi, v, \mathcal{D})$ and a normal $*$-homomorphism $\rho : \mathcal{E}(\mathscr{A}_1)'_c \mapsto \pi(\mathscr{A}_1)'_c$ satisfying $\rho(x)v = vx$ for all $x \in \mathcal{E}(\mathscr{A}_1)'_c$.*

Proof. Given $x \in \mathcal{E}(\mathscr{A}_1)'_c$, define $\rho(x)$ on $\mathscr{A}_1 \otimes S_2$ by $\rho(x)(a \otimes \psi) = a \otimes x\psi$ and extending linearly. Let π be the usual Stinespring representation on $\mathscr{A}_1 \otimes S_2$ and note that as defined ρ and π commute. We claim that ρ induces a well-defined map on the quotient, $\mathcal{D}$ of $\mathscr{A}_1 \otimes S_2$ by the kernel N of the usual Stinespring inner product;

$$\langle a \otimes \psi, b \otimes \xi \rangle := \langle \mathcal{E}(a^\dagger b)\psi, \xi \rangle.$$

Suppose that $\xi = \sum_{k=1}^n a_k \otimes \xi_k$ is in N and observe

$$\begin{aligned}
0 &= \sum_{i,j=1}^n \langle \mathcal{E}(a_i^\dagger a_j)\xi_i, \xi_j \rangle \\
&= \langle [\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n [\xi]_i^n, [\xi]_i^n \rangle,
\end{aligned}$$

where $[\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n$ is the matrix in $M_n(\mathscr{A}_2)$ and $[\xi]_i^n$ a vector in $S_2 \otimes \mathbb{C}^n$. $[\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n$ is symmetric, and by complete positivity, $[\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n \geq 0$. Let A be its Friedrichs extension. By the previous lemma, $S_2 \otimes \mathbb{C}^n \subseteq \mathcal{D}(A) \subseteq \mathcal{D}(\sqrt{A})$ and hence

$$0 = \langle [\xi_i]_i^n, A[\xi_i]_i^n \rangle = \langle \sqrt{A}[\xi_i]_i^n, \sqrt{A}[\xi_i]_i^n \rangle = \left\| \sqrt{A}[\xi_i]_i^n \right\|^2,$$

implying $\sqrt{A}[\xi_i]_i^n = [\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n[\xi_i]_i^n = 0$. Since $1 \otimes \mathcal{E}(\mathscr{A}_1)'_c \subseteq M_n(\mathcal{E}(\mathscr{A}_1))'_c$, for any $x \in \mathcal{E}(\mathscr{A}_1)'_c$;

$$\begin{aligned}
\langle \rho(x)\xi, \rho(x)\xi \rangle &= \sum_{i,j}^n \langle \mathcal{E}(a_i^\dagger a_j)x\xi_i, \xi_j \rangle \\
&= \langle [\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n (1 \otimes x)[\xi_i]_i^n, (1 \otimes x)[\xi_i]_i^n \rangle \\
&= \langle (1 \otimes x^\dagger)(1 \otimes x)[\xi_i]_i^n, ([\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n)^\dagger [\xi_i]_i^n \rangle \\
&= \langle (1 \otimes x^\dagger)(1 \otimes x)[\xi_i]_i^n, [\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n [\xi_i]_i^n \rangle \\
&= 0,
\end{aligned}$$

where the second to last line is by the symmetry of $[\mathcal{E}(a_i^\dagger a_j)]_{i,j}^n$. Hence ρ is well-defined on the quotient. Next we show that ρ is a $*$-representation. For $x \in \mathcal{E}(\mathscr{A}_1)'_c$ we have

$$\begin{aligned}
\langle \rho(x^\dagger)\xi, \psi \rangle &= \sum_{i=1}^n \sum_{j=1}^m \langle \mathcal{E}(a_i^\dagger b_j)x^\dagger \xi_i, \psi_j \rangle \\
&= \sum_{i=1}^n \sum_{j=1}^m \langle x^\dagger \xi_i, \mathcal{E}(b_j^\dagger a_i)\psi_j \rangle \\
&= \sum_{i=1}^n \sum_{j=1}^m \langle \mathcal{E}(a_i^\dagger b_j)\xi_i, x\psi_j \rangle \\
&= \langle \xi, \rho(x)\psi \rangle,
\end{aligned}$$

where $\psi = \sum_{j=1}^m b_j \otimes \psi_j$. That ρ is multiplicative is seen easily by definition, and thus is inherited by the function defined on the quotient by N. Let $\{x_\alpha\}_{\alpha \in I}$ be a net in $\mathcal{E}(\mathscr{A}_1)'_c$ converging to zero ultraweakly. Given $\{\xi_k\}_{k\in\mathbb{N}}, \{\psi_k\}_{k\in\mathbb{N}} \in \mathcal{D}^\infty(\pi(\mathscr{A}_1)'_c)$, where $\xi_k = \sum_{i=1}^{n_k} a_{k,i} \otimes \xi_k(i)$ and $\psi_k = \sum_{j=1}^{m_k} b_{k,j} \otimes \psi_k(j)$, we have

$$\begin{aligned}
\sum_k \langle p(x_\alpha)\xi_k, \psi_k \rangle &= \sum_k \sum_{i=1}^{n_k} \sum_{j=1}^{m_k} \langle \mathcal{E}(a_{i,k}^\dagger b_{j,k})x_\alpha \xi_k(i), \psi_k(j) \rangle \\
&= \sum_k \sum_{i=1}^{n_k} \sum_{j=1}^{m_k} \langle \mathcal{E}(a_{i,k}^\dagger b_{j,k})\xi_k(i), x_\alpha \psi_k(j) \rangle.
\end{aligned}$$

The final line is equal to a seminorm in the ultraweak topology on $\mathcal{E}(\mathscr{A}_1)'_c$, and thus converges to zero, showing that ρ is normal. Recall that the isometry in the usual Stinespring representation is given by $v(\phi) = 1 \otimes \phi$ from which the claimed identity easily follows.

$\square$

Theorem 2. *Let $\mathscr{A}_1$ and $\mathscr{A}_2$ be Op^*-algebras on pre-Hilbert spaces $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively, and $\mathcal{E} : \mathscr{A}_1 \mapsto \mathscr{A}_2$ a quantum channel. If an Op^*-algebra $\mathscr{N} \subseteq \mathscr{L}^\dagger(\mathcal{S}_2)$ is private (respectively, correctable) for $\mathcal{E}$ then it is correctable (respectively, private) for any complement of $\mathcal{E}$.*

Proof. Suppose that $\mathscr{N}$ is private for $\mathcal{E}$ and let $\mathcal{E}^c$ be the complement of $\mathcal{E}$ with respect to the Stinespring representation from the proof of the theorem, and $\rho : \mathcal{E}(\mathscr{A}_1)'_c \mapsto \pi(\mathscr{A}_1)'_c$ the $*$-homomorphism from Arveson's commutant lifting theorem satisfying $\rho(x)v = vx$. $\mathcal{R} := \rho|_{\mathscr{N}}$ corrects $\mathcal{E}^c$;

$$\mathcal{E}^c(\mathcal{R}(x)) = v^\dagger \rho(x) v = v^\dagger v x = x.$$

The result follows for general complementary channels by Remark 1.

Now suppose that $\mathscr{N}$ is correctable for $\mathcal{E}$ and let $\mathcal{R} : \mathscr{N} \mapsto \mathscr{A}_1$ be the correcting channel so that $\mathcal{E}\mathcal{R} = I_{\mathscr{N}}$. By the amplification induction theorem, there exist isometries

$\square$

Corollary 1. *Let $\mathscr{A}_1$ and $\mathscr{A}_2$ be Op^*-algebras on pre-Hilbert spaces S_1, S_2, respectively, and p a projection on S_2. If an Op^*-algebra $\mathscr{N} \subseteq \mathscr{L}^\dagger(p(S_2))$ is private (respectively, correctable) for $\mathcal{E}$ with respect to p then it is correctable (respectively, private) for any complement of $\mathcal{E}$ with respect to p.*

Proof. First observe that, by definition, $\mathscr{N} \subseteq \mathscr{L}^\dagger(p(S_2))$ is private (respectively, correctable) for $\mathcal{E}$ with respect to p if and only if it is private (respectively, correctable) for $\mathcal{C}_p(\mathcal{E})$. Given a complementary channel $\mathcal{E}^c$ with respect to a Stinespring dilation $(\pi, v, \mathcal{D})$, $\mathcal{C}_p(\mathcal{E}^c)$ is a complementary channel for $\mathcal{C}_p(\mathcal{E})$ with respect to $(\pi, vp, \mathcal{D})$. This follows immediately; on the one hand

$$\mathcal{C}_p(\mathcal{E}(a)) = pv^\dagger \pi(a) vp,$$

showing that $(\pi, vp, \mathcal{D})$ is a Stinespring triple for $\mathcal{C}_p(\mathcal{E})$ and then if $\mathcal{E}^c_p$ is the induced complementary channel, for any $x \in \pi(\mathscr{A}_1)'_c$ we have

$$\mathcal{E}^c_p(x) = pv^\dagger x vp = \mathcal{C}_p(\mathcal{E}^c(x)).$$

The corollary follows by applying the previous theorem to the channels $\mathcal{C}_p(\mathcal{E})$ and $\mathcal{C}_p(\mathcal{E}^c)$.

$\square$