PRIVATE ALGEBRAS IN QUANTUM INFORMATION AND INFINITE-DIMENSIONAL COMPLEMENTARITY

JASON CRANN, DAVID W. KRIBS, RUPERT H. LEVENE,
AND IVAN G. TODOROV

Abstract. We introduce a generalized framework for private quantum codes using von Neumann algebras and the structure of commutants. This leads naturally to a more general notion of complementary channel, which we use to establish a generalized complementarity theorem between private and correctable subalgebras that applies to both the finite and infinite-dimensional settings. Linear bosonic channels are considered and specific examples of Gaussian quantum channels are given to illustrate the new framework together with the complementarity theorem.

1. Introduction

One of the most basic notions in quantum privacy is the private quantum code. Arising initially as the quantum analogue of the classical one-time pad, they were first called private quantum channels and investigated for optimal encryption schemes [1, 9]. The subject has grown considerably over the past decade and a half, with related applications in quantum secret sharing [12, 13] and the terminology "private quantum subsystems" taking hold as part of work on the theory of private shared reference frames [3, 4]. In recent years, focus in the subject has turned to investigating relevant properties of completely positive maps. This has led to connections established with quantum error correction [21], discussed in more detail below, as well as algebraic conditions characterizing private subsystems and new, surprisingly simple examples that suggest private subsystems are more ubiquitous than previously thought [18, 19]. These more recent works, along with [11], have also suggested deeper connections with the theory of operator algebras, opening up the possibility of extending the subject to infinite-dimensional Hilbert spaces.

Date: 15 August 2015.

2010 *Mathematics Subject Classification.* 47L90, 46L10, 81P45, 81P94, 94A40.

Key words and phrases. private algebra, private quantum subsystem, private quantum channel, von Neumann algebra, commutant, completely positive map, complementary channel, Gaussian quantum channel.

From a different but related direction, throughout the development of quantum theory, the notion of complementarity has played a fundamental role in the interpretation of quantum measurements, providing, for instance, the theoretical basis behind quantum state tomography. At the level of quantum channels, an appropriate notion of complementarity has been formulated and shown to be vital for understanding their overall structure [14, 22]. An underlying feature of complementarity is the trade-off between information and disturbance. For finite-dimensional quantum channels, this trade-off was quantified in [24], and was used to establish a complementarity theorem between private and correctable subsystems for a channel and its complementary channel [21].

As there is a more general framework for (infinite-dimensional) quantum error correction at the level of von Neumann algebras [5, 6, 7, 8], a natural question is to seek a generalized notion of private quantum codes that is also viable in the infinite-dimensional setting, and for which a suitable complementarity theorem holds. Using von Neumann algebras and the structure of commutants, in this paper we introduce a generalized framework for private quantum codes which may be seen as the complementary analogue of so-called operator algebra error correction, resulting in a natural notion of "private algebras". This in turn leads to a more general notion of complementary channel, and we establish a generalized complementarity theorem for arbitrary dimensions in the new framework. As a corollary, we also obtain a structure theorem for correctable subalgebras that generalizes a finite-dimensional result [20]. We finish by illustrating the framework and concepts for infinite-dimensional linear bosonic channels and a specific class of Gaussian quantum channels [15, 17].

The outline of the paper is as follows. In Section 2, we discuss the necessary preliminaries on infinite-dimensional channels and von Neumann algebras. We then introduce our generalized framework for private quantum codes in Section 3, and discuss their basic properties and examples. Section 4 contains the generalized complementarity theorem and its aforementioned application. In Section 5, we study explicit examples of linear bosonic and Gaussian quantum channels which illustrate the new framework along with the complementarity theorem. We end with a conclusion summarizing the results of the paper and an outlook on future work.

2. Preliminaries

Let S be a (not necessarily finite-dimensional) Hilbert space. We assume that the inner product is linear in the second variable and denote by $\mathcal{B}(S)$ (resp. $\mathcal{T}(S)$) the space of all bounded linear (resp. trace class) operators on S. There is a canonical isometric isomorphism between the Banach space dual $\mathcal{T}(S)^*$ of $\mathcal{T}(S)$ and $\mathcal{B}(S)$ via the trace:

$$\langle T, \rho \rangle := \mathrm{Tr}(T\rho), \quad T \in \mathcal{B}(S), \rho \in \mathcal{T}(S).$$

Thus, $\mathcal{T}(S)$ can be identified with the space of normal (*i.e.* weak* continuous) linear functionals on $\mathcal{B}(S)$, where, if $|\eta\rangle \in S$ and $\langle\xi|$ belongs to the dual S^* of S, the rank one operator $|\eta\rangle\langle\xi| \in \mathcal{T}(S)$ corresponds to the vector functional given by $\omega_{\xi,\eta}(X) = \langle\xi|X|\eta\rangle$, $X \in \mathcal{B}(S)$.

We denote by $\mathcal{S}(S)$ the set of all *states* on S; thus, an element $\rho \in \mathcal{T}(S)$ belongs to $\mathcal{S}(S)$ precisely when ρ is positive (that is, $\langle X, \rho\rangle = \mathrm{Tr}(X\rho) \geq 0$ whenever $X \geq 0$) and $\langle I, \rho\rangle = \mathrm{Tr}(\rho) = 1$.

If S and S' denote the respective input and output systems of a dynamical quantum process, then, in the Schrödinger picture, states in $\mathcal{T}(S)$ evolve under a completely positive trace preserving (CPTP) map to states in $\mathcal{T}(S')$. In the Heisenberg picture, which will be adopted in this paper, observables in $\mathcal{B}(S')$ evolve under a normal (*i.e.* weak*-weak* continuous) unital completely positive (NUCP) map $\mathcal{E}$ to observables in $\mathcal{B}(S)$. As a normal map, $\mathcal{E}$ has a unique pre-adjoint $\mathcal{E}_* : \mathcal{T}(S) \to \mathcal{T}(S')$ which is a CPTP map describing the corresponding evolution of states.

Suppose that in the above scenario, one wished, or had the ability, to measure only a certain subset $\mathcal{O}$ of observables on the output space S'. The results of the measurements will then be governed by the spectral projections of the corresponding elements in $\mathcal{O}$, which, by general spectral theory, lie in the von Neumann algebra M generated by $\mathcal{O}$. Thus, the relevant dynamics is encoded in the restriction of $\mathcal{E}$ to M, that is, in a NUCP map $\mathcal{E} : M \to \mathcal{B}(S)$. As such mappings are natural objects of study in operator algebra theory, and include the class of classical information channels, we will adopt this more general framework in this paper. The remainder of this section will be devoted to a brief overview of the relevant concepts; for details, we refer the reader to [26, 27].

A *von Neumann algebra* on a Hilbert space S is a $*$-subalgebra M of $\mathcal{B}(S)$ with unit $1_M = I_S \in M$ which is closed in the strong operator topology. For a subset $L \subseteq \mathcal{B}(S)$, its *commutant* is the subspace

$$L' := \{X \in \mathcal{B}(S) \mid XT = TX, \ \text{ for all } T \in L\}.$$

Von Neumann's bicommutant theorem states that a unital $*$-subalgebra M of $\mathcal{B}(S)$ is a von Neumann algebra if and only if $M'' := (M')'$ coincides with M. As $(L')'' = L'$ for any subset $L \subseteq \mathcal{B}(S)$, the commutant M' of a von Neumann algebra M is again a von Neumann algebra on S.

Another distinguishing feature of a von Neumann algebra M is that it is (isometrically isomorphic to) the dual of a unique Banach space M_*, called the *predual* of M, which consists of all weak* continuous linear functionals on M. For example, $M = \mathcal{B}(S)$ is a von Neumann algebra with $M_* = \mathcal{T}(S)$. We will denote by $\mathcal{S}(M)$ the set of normal states on M, that is, the positive elements ρ of M_* satisfying $\langle I_S, \rho\rangle = 1$. If M and N are von Neumann algebras, a bounded linear map $\mathcal{E} : M \to N$ is said to be *normal* if it is weak*-weak* continuous. In this case, $\mathcal{E}$ has a unique pre-adjoint $\mathcal{E}_* : N_* \to M_*$ satisfying

$$\langle X, \mathcal{E}_*(\rho)\rangle = \langle \mathcal{E}(X), \rho\rangle, \quad X \in M, \ \rho \in N_*.$$

Moreover, $\mathcal{E}$ is a NUCP map if and only if $\mathcal{E}_*$ is completely positive and $\mathcal{E}_*(\mathcal{S}(N)) \subseteq \mathcal{S}(M)$.

Given two Hilbert spaces S and S', we denote by $S \otimes S'$ their Hilbertian tensor product. For operators $X \in \mathcal{B}(S)$ and $Y \in \mathcal{B}(S')$, as usual we denote by $X \otimes Y$ the (unique) operator in $\mathcal{B}(S \otimes S')$ with $(X \otimes Y)(\xi \otimes \eta) = X\xi \otimes Y\eta$, $\xi \in S$, $\eta \in S'$. If $M \subseteq \mathcal{B}(S)$ and $N \subseteq \mathcal{B}(S')$ are von Neumann algebras, the weak* closed linear span $M \bar{\otimes} N$ of $\{X \otimes Y \mid X \in M,\ Y \in N\}$ is a von Neumann subalgebra of $\mathcal{B}(S \otimes S')$. In particular, $\mathcal{B}(S) \bar{\otimes} \mathcal{B}(S') = \mathcal{B}(S \otimes S')$. If $\rho \in M_*$ and $\omega \in N_*$, then there exists a (unique) element $\rho \otimes \omega \in (M \bar{\otimes} N)_*$ such that

$$\langle X \otimes Y, \rho \otimes \omega \rangle = \langle X, \rho \rangle \langle Y, \omega \rangle, \quad X \in M,\ Y \in N.$$

Thus, we have a natural embedding of the algebraic tensor product $M_* \odot N_*$ into $(M \bar{\otimes} N)_*$; its image is norm dense in $(M \bar{\otimes} N)_*$.

Given a Hilbert space S and a von Neumann algebra M, a *quantum channel* is a NUCP map $\mathcal{E} : M \to \mathcal{B}(S)$. (This is the dual viewpoint of how channels are typically presented in quantum information theory as CP trace-preserving maps, but is more natural in the operator algebra setting.) Note that a quantum channel $\mathcal{E}$ is automatically completely bounded (see *e.g.* [26]). We denote by $\|\Phi\|_{\mathrm{cb}}$ the c.b. norm of a completely bounded map Φ. In the case $M = \mathbb{C}$, an important example is the depolarizing channel $\mathcal{D} : \mathbb{C} \to \mathcal{B}(S)$ given by $\mathcal{D}(\lambda) = \lambda I$. It is straightforward to check that $\mathcal{D}_* : \mathcal{T}(S) \to \mathbb{C}$ coincides with the trace. If $\mathcal{F} : N \to \mathcal{B}(S')$ is another quantum channel on the von Neumann algebra N, then there exists a (unique) quantum channel $\mathcal{E} \otimes \mathcal{F} : M \bar{\otimes} N \to \mathcal{B}(S \otimes S')$ such that

$$(\mathcal{E} \otimes \mathcal{F})(X \otimes Y) = \mathcal{E}(X) \otimes \mathcal{F}(Y), \quad X \in M,\ Y \in N.$$

Channels can similarly be tensored in the Schrödinger picture, and $(\mathcal{E} \otimes \mathcal{F})_* = \mathcal{E}_* \otimes \mathcal{F}_*$.

Stinespring's theorem for normal maps asserts that if $\mathcal{E} : M \to \mathcal{B}(S)$ is a quantum channel, then there exist a Hilbert space H, a normal unital $*$-homomorphism $\pi : M \to \mathcal{B}(H)$ and an isometry $V : S \to H$ such that

$$\mathcal{E}(X) = V^* \pi(X) V, \quad X \in M. \tag{1}$$

We refer to the triple (π, V, H) as a *Stinespring triple* for $\mathcal{E}$, and to identity (1) as a *Stinespring representation* of $\mathcal{E}$. Such a Stinespring representation is unique up to a conjugation by a partial isometry in the following sense: if (π_1, V_1, H_1) and (π_2, V_2, H_2) are Stinespring triples for $\mathcal{E}$, then there is a partial isometry $U : H_1 \to H_2$ such that

$$UV_1 = V_2, \quad U^*V_2 = V_1 \ \text{ and } \ U\pi_1(X) = \pi_2(X)U \tag{2}$$

for all $X \in M$. If (π_1, V_1, H_1) yields a *minimal* Stinespring representation, meaning that the linear span of $\pi_1(M)V_1S$ is a dense subspace of H_1, then we will call (π_1, V_1, H_1) a *minimal Stinespring triple* for $\mathcal{E}$. In this case, the map U above is necessarily an isometry, and any two minimal Stinespring representations for $\mathcal{E}$ are unitarily equivalent.

3. Private Quantum Codes via Commutant Structures

We now introduce our generalized notion of privacy for quantum channels. Given Hilbert spaces S and S' and a bounded operator $T : S' \to S$, we write $\mathcal{C}_T : \mathcal{B}(S') \to \mathcal{B}(S)$, $\mathcal{C}_T(X) = TXT^*$ for conjugation by T. Clearly, if T is a partial isometry then $\mathcal{C}_T$ is a quantum channel from $\mathcal{B}(S')$ into $\mathcal{B}(TT^*S)$. For a Hilbert space S, we let $\mathcal{P}(S)$ denote the set of projections in $\mathcal{B}(S)$.

Definition 3.1. Let S be a Hilbert space, let M be a von Neumann algebra, and let $\mathcal{E} : M \to \mathcal{B}(S)$ be a quantum channel. If $P \in \mathcal{P}(S)$, a von Neumann subalgebra $N \subseteq \mathcal{B}(PS)$ is called *private for $\mathcal{E}$ with respect to P* if

$$\mathcal{C}_P \circ \mathcal{E}(M) \subseteq N'.$$

Given $\varepsilon > 0$, we say that N is *ε-private for $\mathcal{E}$ with respect to P* if there exists a quantum channel $\mathcal{F} : M \to \mathcal{B}(S)$ such that

$$\|\mathcal{E} - \mathcal{F}\|_{\mathrm{cb}} < \varepsilon$$

and N is private for $\mathcal{F}$ with respect to P. If $P = I$, we simply say that $N \subseteq \mathcal{B}(S)$ is *private* (resp. *ε-private*) for $\mathcal{E}$.

Remark. The definition of a private subalgebra is motivated by the notion of an operator private subsystem [3, 4, 18, 19, 21]. Recall that, if S, A, B and S' are finite-dimensional Hilbert spaces with $S = (A \otimes B) \oplus (A \otimes B)^{\perp}$ and $\mathcal{E} : \mathcal{B}(S') \to \mathcal{B}(S)$ is a UCP map with pre-adjoint $\mathcal{E}_* : \mathcal{T}(S) \to \mathcal{T}(S')$, then B is called an operator private subsystem for $\mathcal{E}$ if $\mathcal{E}_* \circ (\mathcal{C}_P)_* = \mathcal{F}_* \otimes \mathrm{Tr}$ for some quantum channel $\mathcal{F} : \mathcal{B}(S') \to \mathcal{B}(A)$, where P is the projection from S onto $A \otimes B$ [21]. Assuming $P\rho P = \sum_{i=1}^n \rho_i^A \otimes \rho_i^B$, where ρ_i^A (resp. ρ_i^B) are elements of $\mathcal{T}(A)$ (resp. $\mathcal{T}(B)$), we have

$$\begin{aligned}
\langle \mathcal{C}_P \circ \mathcal{E}(T), \rho \rangle &= \langle T, \mathcal{E}_* \circ (\mathcal{C}_P)_*(\rho) \rangle = \langle T, \mathcal{E}_*(P\rho P) \rangle \\
&= \sum_{i=1}^n \langle T, \mathcal{E}_*(\rho_i^A \otimes \rho_i^B) \rangle = \sum_{i=1}^n \langle T, (\mathcal{F}_* \otimes \mathrm{Tr})(\rho_i^A \otimes \rho_i^B) \rangle \\
&= \sum_{i=1}^n \langle T, \mathcal{F}_*(\rho_i^A) \rangle \langle I_B, \rho_i^B \rangle = \sum_{i=1}^n \langle \mathcal{F}(T) \otimes I_B, \rho_i^A \otimes \rho_i^B \rangle \\
&= \langle \mathcal{F}(T) \otimes I_B, P\rho P \rangle = \langle P(\mathcal{F}(T) \otimes I_B)P, \rho \rangle.
\end{aligned}$$

Thus,

$$\mathcal{C}_P \circ \mathcal{E}(\mathcal{B}(S')) \subseteq \mathcal{B}(A) \otimes I_B = (I_A \otimes \mathcal{B}(B))' = N',$$

where $N := I_A \otimes \mathcal{B}(B) = \{I_A \otimes Y : Y \in \mathcal{B}(B)\}$, a von Neumann subalgebra of $\mathcal{B}(PS)$.

Conversely, if $\mathcal{C}_P \circ \mathcal{E}(\mathcal{B}(S')) \subseteq N' = \mathcal{B}(A) \otimes I_B$, then for every $T \in \mathcal{B}(S')$ there exists $X_T \in \mathcal{B}(A)$ such that $\mathcal{C}_P \circ \mathcal{E}(T) = X_T \otimes I_B$. Set $\mathcal{F}(T) = X_T$. It is easy to check that this defines a UCP map $\mathcal{F}\colon \mathcal{B}(S') \to \mathcal{B}(A)$ and that its pre-adjoint $\mathcal{F}_* : \mathcal{T}(A) \to T(S')$ satisfies $\mathcal{E}_* \circ (\mathcal{C}_P)_* = \mathcal{F}_* \otimes \mathrm{Tr}$. Thus, B is an operator private subsystem if and only if $N \cong \mathcal{B}(B)$ is a private subalgebra for $\mathcal{E}$ with respect to P.

The choice of the term "private" is justified by the fact that any information stored in the operator private subsystem B completely decoheres under the action of $\mathcal{E}_*$ [1, 4]. From the Heisenberg perspective, observables on the output system evolve under $\mathcal{E}$ to observables having uniform statistics with respect to the subsystem B in the sense that the expected value of a measurement of $\mathcal{E}(T)$ in the state $\rho \in \mathcal{T}(A \otimes B)$ solely depends on the marginal state $\mathrm{Tr}_B(\rho) \in \mathcal{T}(A)$.

In the more general setting of private subalgebras, not all information about observables in the subalgebra $N \subseteq \mathcal{B}(PS)$ is lost under the action of $\mathcal{E} : M \to \mathcal{B}(S)$, just the *quantum* information. Indeed, the only obtainable information about N after an application of the channel is the classical information contained in its center $\mathcal{Z}(N) = N \cap N'$. Thus, we recover the usual sense of privacy when N is a *factor*, meaning $\mathcal{Z}(N) = \mathbb{C}I$. If N is a factor of type I, then $N \cong I_A \otimes \mathcal{B}(B)$ for some Hilbert spaces A and B [27]. This induces a decomposition $S = (A \otimes B) \oplus (A \otimes B)^\perp$ and it follows that B is an operator private subsystem for $\mathcal{E}$. Hence, operator private subsystems are precisely the private type I factors.

Examples. An immediate class of examples of private subalgebras arises from normal conditional expectations. If S is a Hilbert space and $\mathcal{E} : \mathcal{B}(S) \to N'$ is a normal conditional expectation, that is, a weak*-weak* continuous projection of norm one, where $N \subseteq \mathcal{B}(S)$ is a von Neumann subalgebra, then trivially, N is private for the quantum channel $\mathcal{E}$. Some concrete examples are the following.

(i) *Deletion channels:* $\mathcal{E}(T) = \langle T, \rho \rangle I$, for some $\rho \in \mathcal{S}(S)$; in this case $N = \mathcal{B}(S)$.

(ii) *Uniform phase-flips on n-qubits:*

$$\mathcal{E}(T) = \frac{1}{2^n} \sum_{(s_1,\cdots,s_n) \in \mathbb{Z}_2^n} Z_{(s_1,\cdots,s_n)} T Z^*_{(s_1,\cdots,s_n)},$$

where $Z_{(s_1,\cdots,s_n)} = \otimes_{i=1}^n Z_{s_i}$ where $Z_0 = I$ and $Z_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$; in this case, $N = N' = \otimes_{i=1}^n \Delta_2$, where Δ_2 is the diagonal subalgebra of $M_2(\mathbb{C})$.

(iii) *Uniform bit-flips on n-qubits:*

$$\mathcal{E}(T) = \frac{1}{2^n} \sum_{(s_1,\cdots,s_n) \in \mathbb{Z}_2^n} X_{(s_1,\cdots,s_n)} T X^*_{(s_1,\cdots,s_n)},$$

where $X_{(s_1,\cdots,s_n)} = \otimes_{i=1}^n X_{s_i}$ with $X_0 = I$ and $X_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$; in this case, $N = N' = \otimes_{i=1}^n \mathcal{C}_2$, where $\mathcal{C}_2$ is the subalgebra of circulant matrices in $M_2(\mathbb{C})$.

The latter two examples fall under a general class of conditional expectations arising from compact group representations: if $\pi : G \to \mathcal{B}(H_\pi)$ is a unitary representation of a compact group, then $\mathcal{E} : \mathcal{B}(H_\pi) \to \mathcal{B}(H_\pi)$ defined

by

$$\mathcal{E}(T) = \int_G \pi(s) T \pi(s)^* \, dh(s)$$

where h is a normalized Haar measure on G, is a conditional expectation onto $\pi(G)'$, so that $N = \pi(G)''$ in this case. A similar class of examples was considered in [4].

4. Complementarity with Correctable Subalgebras

In finite dimensions, a perfect duality exists between operator private and correctable subsystems: a subsystem is correctable for a channel $\mathcal{E}$ if and only if it is private for any complementary channel $\mathcal{E}^c$ [21]. Using the continuity of the Stinespring representation [24], an approximate version of the complementarity theorem was also established [21]. In this section, we generalize the notion of complementarity to quantum channels of the form $\mathcal{E} : M \to \mathcal{B}(S)$, and in this new framework, extend the complementarity theorem and its approximate version.

Definition 4.1. Let S be a Hilbert space, let M be a von Neumann algebra, and let $\mathcal{E} : M \to \mathcal{B}(S)$ be a quantum channel. Given a Stinespring triple (π, V, H) for $\mathcal{E}$, we define the *complementary channel* of $\mathcal{E}$ with respect to (π, V, H) to be the NUCP map $\mathcal{E}^c_{\pi,V,H} : \pi(M)' \to \mathcal{B}(S)$ given by

$$\mathcal{E}^c_{\pi,V,H}(X) = V^* X V, \quad X \in \pi(M)'.$$

We also say that $\mathcal{E}^c_{\pi,V,H}$ is *a complementary channel of* $\mathcal{E}$.

Remark 4.2. Suppose that (π_1, V_1, H_1) and (π_2, V_2, H_2) are Stinespring triples for $\mathcal{E}$, and let $\mathcal{F}_1 = \mathcal{E}^c_{\pi_1,V_1,H_1}$ and $\mathcal{F}_2 = \mathcal{E}^c_{\pi_2,V_2,H_2}$. By the uniqueness of the Stinespring representation, there exists a partial isometry $U : H_1 \to H_2$ satisfying identities (2). It follows that, if $Y \in \pi_1(M)'$ and $X \in M$ then

$$\begin{aligned} \mathcal{C}_U(Y)\pi_2(X) = UYU^*\pi_2(X) = UY\pi_1(X)U^* = U\pi_1(X)YU^* \\ = \pi_1(X)UYU^* = \pi_2(X)\mathcal{C}_U(Y); \end{aligned}$$

thus, $\mathcal{C}_U(\pi_1(M)') \subseteq \pi_2(M)'$ and, similarly, $\mathcal{C}_{U^*}(\pi_2(M)') \subseteq \pi_1(M)'$. Hence the maps $\mathcal{F}_2 \circ \mathcal{C}_U$ and $\mathcal{F}_1 \circ \mathcal{C}_{U^*}$ are well-defined; by (2), $\mathcal{F}_1 = \mathcal{F}_2 \circ \mathcal{C}_U$ and $\mathcal{F}_2 = \mathcal{F}_1 \circ \mathcal{C}_{U^*}$.

Let $\mathcal{E} : M \to \mathcal{B}(S)$ be a quantum channel and suppose that (π, V, H) is a Stinespring triple for $\mathcal{E}$ with π faithful. Let $\mathcal{E}^c = \mathcal{E}^c_{\pi,V,H}$, and note that $(\mathrm{id}_{\pi(M)'}, V, H)$ is a Stinespring triple for $\mathcal{E}^c$ (here $\mathrm{id}_{\pi(M)'} : \pi(M)' \to \pi(M)'$ is the identity map). Letting $\mathcal{E}^{cc} : \pi(M) \to \mathcal{B}(S)$ be the complement of $\mathcal{E}^c$ with respect to this Stinespring triple, we have that

$$\mathcal{E}^c(\pi(X)) = \mathcal{E}(X), \quad X \in M.$$

Identifying M with $\pi(M)$, we see that $\mathcal{E}^{cc} = \mathcal{E}$; thus, the generalized notion of complementarity is involutive, as expected.

A specific example of a Stinespring triple for $\mathcal{E}$ whose corresponding normal representation is faithful can be obtained as follows. Let $M_1 \subseteq \mathcal{B}(H_1)$ and $M_2 \subseteq \mathcal{B}(H_2)$ be von Neumann algebras. The amplification-induction theorem [27, Theorem IV.5.5] states that for every normal $*$-homomorphism π from M_1 onto M_2, there exists a Hilbert space H_3, a projection $P \in M_1' \bar{\otimes} \mathcal{B}(H_3)$ and a unitary $U : H_2 \to P(H_1 \otimes H_3)$ such that

$$\pi(X) = U^* P(X \otimes I_{H_3}) P U, \quad X \in M_1.$$

Viewing PU as an isometry $W : H_2 \to H_1 \otimes H_3$, we have

$$\pi(X) = W^*(X \otimes I_{H_3})W, \quad X \in M_1. \tag{3}$$

Now suppose that $M \subseteq \mathcal{B}(S')$ is a von Neumann algebra, $\mathcal{E} : M \to \mathcal{B}(S)$ is a quantum channel and (π, V, H) is a Stinespring triple for $\mathcal{E}$ (with π not necessarily faithful). Since the image $\pi(M)$ is a von Neumann algebra on H [27], the amplification-induction theorem allows us to write

$$\mathcal{E}(X) = \widetilde{V}^*(X \otimes I_{H_3})\widetilde{V}, \quad X \in M, \tag{4}$$

where $\widetilde{V} = WV$ is the composition of the Stinespring isometry $V : S \to H$ and the isometry $W : H \to S' \otimes H_3$ from the representation of π as in equation (3).

Note that if $M = \mathcal{B}(S')$, then $M' = \mathbb{C} I_{S'}$ and $P = I_{S'} \otimes P' \in I_{S'} \bar{\otimes} \mathcal{B}(H_3)$ for some $P' \in \mathcal{P}(H_3)$, so we may view W as a unitary from H onto $S' \otimes P' H_3$. Equation (4) then becomes the usual Stinespring representation of a quantum channel $\mathcal{E} : \mathcal{B}(S') \to \mathcal{B}(S)$, and its corresponding complement $\mathcal{E}^c : I_{S'} \bar{\otimes} \mathcal{B}(P' H_3) \to \mathcal{B}(S)$ is the usual complementary channel as studied in the literature.

Lemma 4.3. *Let S and S' be Hilbert spaces, $M \subseteq \mathcal{B}(S')$ be a von Neumann algebra, $\mathcal{E} : M \to \mathcal{B}(S)$ be a quantum channel and $W : S \to S$ be a partial isometry. If $\mathcal{E}^c$ is a complementary channel of $\mathcal{E}$, then $\mathcal{C}_W \circ \mathcal{E}^c$ is a complementary channel of $\mathcal{C}_W \circ \mathcal{E}$.*

Proof. Suppose that $\mathcal{E}^c$ is associated with the Stinespring triple (π, V, H) of $\mathcal{E}$. Then

$$\mathcal{E}(X) = V^* \pi(X) V, \quad X \in M$$

and

$$\mathcal{E}^c(Y) = V^* Y V, \quad Y \in \pi(M)'.$$

Thus,

$$\mathcal{C}_W \circ \mathcal{E}(X) = W V^* \pi(X) V W^*, \quad X \in M,$$

and hence (π, VW^*, H) is a Stinespring triple for $\mathcal{C}_W \circ \mathcal{E}$. The claim is now immediate. □

Before proceeding to the complementarity theorem, we recall the operator algebra formalism of quantum error correction [6, 7, 8].

Definition 4.4. Let S be a Hilbert space, M be a von Neumann algebra, and $\mathcal{E} : M \to \mathcal{B}(S)$ be a quantum channel. If $P \in \mathcal{P}(S)$, a von Neumann subalgebra $N \subseteq \mathcal{B}(PS)$ is said to be *correctable for $\mathcal{E}$ with respect to P* if there exists a quantum channel $\mathcal{R} : N \to M$ such that

$$\mathcal{C}_P \circ \mathcal{E} \circ \mathcal{R} = \mathrm{id}_N .$$

Given $\varepsilon > 0$, we say that N is *ε-correctable for $\mathcal{E}$ with respect to P* if there exists a quantum channel $\mathcal{R} : N \to M$ such that

$$\|\mathcal{C}_P \circ \mathcal{E} \circ \mathcal{R} - \mathrm{id}_N\|_{\mathrm{cb}} < \varepsilon.$$

If $P = I$, we simply say that $N \subseteq \mathcal{B}(S)$ is *correctable* (resp. *ε-correctable*) for $\mathcal{E}$.

The above definition unifies the notions of correctable and noiseless (meaning correctable, but with no active correction required) subspaces and subsystems under one umbrella, allowing for a general treatment of quantum error correction using the language of operator algebras. As mentioned in [8], correctable subsystems correspond to correctable von Neumann algebras of type I, analogous to the situation above for operator private subsystems.

Note that the channel $\mathcal{R}$ in Definition 4.4 (called the *recovery channel*) has a slightly more general form than the one usually studied in the literature, (namely, a NUCP map $\mathcal{R} : \mathcal{B}(S') \to \mathcal{B}(S)$ satisfying $\mathcal{C}_P \circ \mathcal{E} \circ \mathcal{R} = \mathcal{C}_P|_N$). The reason is to keep in line with our general picture of quantum channels as NUCP maps whose domain can be a general von Neumann algebra.

Lemma 4.5. *Let M be a von Neumann algebra and let $\mathcal{E} : M \to B(S)$ be a quantum channel. If $\varepsilon > 0$ and $N \subseteq \mathcal{B}(S)$ is a von Neumann algebra which is ε-correctable (respectively, correctable) for some particular complement of $\mathcal{E}$, then N is ε-correctable (respectively, correctable) for every complement of $\mathcal{E}$.*

Proof. Let (π_0, V_0, H_0) and (π, V, H) be Stinespring triples for $\mathcal{E}$, and denote the corresponding complements by $\mathcal{E}_0^c$ and $\mathcal{E}^c$. Suppose that N is ε-correctable for $\mathcal{E}_0^c$; we will show that the same is true of $\mathcal{E}^c$. There is a quantum channel $\mathcal{R}_0 : N \to \pi_0(M)'$ with $\|\mathcal{E}_0 \circ \mathcal{R}_0 - \mathrm{id}_N\|_{\mathrm{cb}} < \varepsilon$. By Remark 4.2, there is a partial isometry $U : H_0 \to H$ so that

$$U\pi_0(M)'U^* \subseteq \pi(M)', \quad \mathcal{E}_0^c = \mathcal{E}^c \circ \mathcal{C}_U \quad \text{and} \quad \mathcal{E}^c = \mathcal{E}_0^c \circ \mathcal{C}_{U^*}. \tag{5}$$

Fix a normal state $\omega \in N_*$ and define a quantum channel $\mathcal{R} : N \to \pi(M)'$ by

$$\mathcal{R}(T) = U\mathcal{R}_0(T)U^* + \langle T, \omega\rangle(1 - UU^*), \quad T \in N.$$

(The second term is required to ensure that $\mathcal{R}$ is unital.) Since U^*U is a projection, we have $\mathcal{C}_{U^*} \circ \mathcal{R} = \mathcal{C}_{U^*} \circ \mathcal{C}_U \circ \mathcal{R}_0$ and so, by (5),

$$\mathcal{E}^c \circ \mathcal{R} = \mathcal{E}_0^c \circ \mathcal{C}_{U^*} \circ \mathcal{R} = \mathcal{E}_0^c \circ \mathcal{C}_{U^*} \circ \mathcal{C}_U \circ \mathcal{R}_0 = \mathcal{E}_0^c \circ \mathcal{R}_0.$$

Hence $\|\mathcal{E}^c \circ \mathcal{R} - \mathrm{id}_N\|_{\mathrm{cb}} = \|\mathcal{E}_0^c \circ \mathcal{R}_0 - \mathrm{id}_N\|_{\mathrm{cb}} < \varepsilon$ and so N is ε-correctable for $\mathcal{E}^c$. The assertion with correctability in place of ε-correctability is proven by replacing "less than ε" with "equal to zero" in the preceding. □

The following elementary lemma will be used to obtain quantum channels from (not necessarily unital) normal completely positive maps.

Lemma 4.6. *Let S be a Hilbert space and let M and N be von Neumann algebras with $N \subseteq \mathcal{B}(S)$. If $\mathcal{F} : M \to N$ is a normal completely positive contractive map, then there is a quantum channel $\widetilde{\mathcal{F}} : M \to N$ with $\|\widetilde{\mathcal{F}} - \mathcal{E}\|_{\mathrm{cb}} \leq 2\|\mathcal{F} - \mathcal{E}\|_{\mathrm{cb}}$ for any quantum channel $\mathcal{E} : M \to \mathcal{B}(S)$.*

Proof. Let $\omega \in M_*$ be a normal state and set $A = 1_N - \mathcal{F}(1_M)$. Since $\mathcal{F}$ is contractive and positive, $\mathcal{F}(1_M)$ is a positive contraction and so $A \geq 0$. Let $\widetilde{\mathcal{F}}$ be the map defined by $\widetilde{\mathcal{F}}(X) = \mathcal{F}(X) + \langle X, \omega\rangle A$, $X \in M$. Then $\widetilde{\mathcal{F}}$ is unital by construction, and as it is the sum of two normal completely positive maps into N, we see that $\widetilde{\mathcal{F}}$ is a quantum channel from M into N. The map $\widetilde{\mathcal{F}} - \mathcal{F}$ is completely positive, so it attains its (completely bounded) norm at 1_M [26]; hence,

$$\|\widetilde{\mathcal{F}} - \mathcal{F}\|_{\mathrm{cb}} = \|\langle 1_M, \omega\rangle A\| = \|A\| = \|(\mathcal{E} - \mathcal{F})(1_M)\| \leq \|\mathcal{F} - \mathcal{E}\|_{\mathrm{cb}}.$$

Thus $\|\widetilde{\mathcal{F}} - \mathcal{E}\|_{\mathrm{cb}} \leq \|\widetilde{\mathcal{F}} - \mathcal{F}\|_{\mathrm{cb}} + \|\mathcal{F} - \mathcal{E}\|_{\mathrm{cb}} \leq 2\|\mathcal{F} - \mathcal{E}\|_{\mathrm{cb}}$. □

The next theorem is one of the central results of the paper. It generalizes the main results of both [21] and [5], which correspond to the special case that S' is finite dimensional and $M = \mathcal{B}(S')$. In the proof, we will use results from [23]; the latter paper is concerned with the continuity of the Stinespring representation for completely positive maps defined on C*-algebras. By Stinespring's theorem for normal maps, it is straightforward to verify that the results we will need remain valid in the case of normal completely positive maps defined on von Neumann algebras.

Theorem 4.7. *Let S and S' be Hilbert spaces, $M \subseteq \mathcal{B}(S')$ be a von Neumann algebra, $\mathcal{E} : M \to \mathcal{B}(S)$ be a quantum channel and $P \in \mathcal{P}(S)$. If a von Neumann subalgebra $N \subseteq \mathcal{B}(PS)$ is ε-private (respectively, ε-correctable) for $\mathcal{E}$ with respect to P then it is $2\sqrt{\varepsilon}$-correctable (respectively, $8\sqrt{\varepsilon}$-private) for any complement of $\mathcal{E}$ with respect to P. In particular, N is private (respectively, correctable) for $\mathcal{E}$ with respect to P if and only if it is correctable (respectively, private) for any complement of $\mathcal{E}$ with respect to P.*

Proof. Without loss of generality we may suppose that $P = I$; indeed, $N \subseteq \mathcal{B}(PS)$ is ε-private (respectively, ε-correctable) for $\mathcal{E}$ with respect to P if and only it is ε-private (respectively, ε-correctable) for $\mathcal{C}_P \circ \mathcal{E}$. The general statement now follows from Lemma 4.3, according to which $\mathcal{C}_P \circ \mathcal{E}^c$ is complementary to $\mathcal{C}_P \circ \mathcal{E}$.

We first consider one of the implications in the case $\varepsilon = 0$. Namely, suppose that N is private for $\mathcal{E}$, so that $\mathcal{E}(M) \subseteq N'$, and hence $N = N'' \subseteq \mathcal{E}(M)'$. Let $\mathcal{E}^c$ be the complement of $\mathcal{E}$ with respect to a minimal Stinespring triple (π, V, H) for $\mathcal{E}$. It follows from Arveson's commutant lifting theorem [2, Theorem 1.3.1] that there exists a normal *-homomorphism $\rho : \mathcal{E}(M)' \to \pi(M)'$ such that $\rho(X)V = VX$ for all $X \in \mathcal{E}(M)'$ (see also [27,

IV.3.6]). Consider the quantum channel $\mathcal{R} := \rho|_N : N \to \pi(M)'$. Since $\mathcal{E}$ is unital, V is an isometry and hence

$$\mathcal{E}^c(\mathcal{R}(T)) = V^*\rho(T)V = V^*VT = T$$

for all $T \in N$. Thus, N is correctable for $\mathcal{E}^c$. By Lemma 4.5, N is correctable for any complement of $\mathcal{E}$.

Now suppose that N is ε-private for $\mathcal{E}$, so that N is private for some channel $\mathcal{F} : M \to \mathcal{B}(S)$ with $\|\mathcal{E} - \mathcal{F}\|_{\mathrm{cb}} < \varepsilon$. By [23, Proposition 6], there is a common normal representation $\pi : M \to \mathcal{B}(H)$ with Stinespring triples $(\pi, V_{\mathcal{E}}, H)$ and $(\pi, V_{\mathcal{F}}, H)$ for $\mathcal{E}$ and $\mathcal{F}$, respectively, so that

$$\|V_{\mathcal{E}} - V_{\mathcal{F}}\| \leq \sqrt{\|\mathcal{E} - \mathcal{F}\|_{\mathrm{cb}}} < \sqrt{\varepsilon}.$$

Let $\mathcal{E}^c : \pi(M)' \to \mathcal{B}(S)$ and $\mathcal{F}^c : \pi(M)' \to \mathcal{B}(S)$ be the corresponding complementary channels. It follows from [23, Proposition 3] that

$$\|\mathcal{E}^c - \mathcal{F}^c\|_{\mathrm{cb}} \leq 2\|V_{\mathcal{E}} - V_{\mathcal{F}}\| < 2\sqrt{\varepsilon}.$$

Since N is private for $\mathcal{F}$, it is correctable for $\mathcal{F}^c$ by the previous paragraphs, so there exists a channel $\mathcal{R} : N \to \pi(M)'$ such that $\mathcal{F}^c \circ \mathcal{R} = \mathrm{id}_N$. Hence,

$$\|\mathcal{E}^c \circ \mathcal{R} - \mathrm{id}_N\|_{\mathrm{cb}} = \|(\mathcal{E}^c - \mathcal{F}^c) \circ \mathcal{R}\|_{\mathrm{cb}} < 2\sqrt{\varepsilon}$$

as $\|\mathcal{R}\|_{\mathrm{cb}} = 1$. Thus, N is $2\sqrt{\varepsilon}$-correctable for $\mathcal{E}^c$. By Lemma 4.5, the same is true of any other complement of $\mathcal{E}$.

Conversely, suppose that N is ε-correctable for $\mathcal{E}$, so that $\|\mathcal{E}\circ\mathcal{R} - \mathrm{id}_N\| < \varepsilon$ for some quantum channel $\mathcal{R} : N \to M$. Again by [23, Proposition 6], there exists a common normal representation $\pi : M \to \mathcal{B}(H)$ and Stinespring triples $(\pi, V_{\mathcal{E}\mathcal{R}}, H)$ and $(\pi, V_{\mathrm{id}}, H)$ for $\mathcal{E} \circ \mathcal{R}$ and id_N, respectively, so that

$$\|V_{\mathcal{E}\mathcal{R}} - V_{\mathrm{id}}\| \leq \sqrt{\|\mathcal{E} \circ \mathcal{R} - \mathrm{id}_N\|_{\mathrm{cb}}} < \sqrt{\varepsilon}.$$

By the amplification-induction theorem, there exist Hilbert spaces $H_{\mathcal{E}}, H_{\mathcal{R}}$ and isometries $V_{\mathcal{E}} : S \to S' \otimes H_{\mathcal{E}}$ and $V_{\mathcal{R}} : S' \to S \otimes H_{\mathcal{R}}$ such that

$$\mathcal{E}(X) = V_{\mathcal{E}}^*(X \otimes I_{H_{\mathcal{E}}})V_{\mathcal{E}}, \quad X \in M,$$

and

$$\mathcal{R}(T) = V_{\mathcal{R}}^*(T \otimes I_{H_{\mathcal{R}}})V_{\mathcal{R}}, \quad T \in N.$$

Thus,

$$\mathcal{E} \circ \mathcal{R}(T) = V_{\mathcal{E}}^*(V_{\mathcal{R}}^* \otimes I_{H_{\mathcal{E}}})(T \otimes I_{H_{\mathcal{R}}} \otimes I_{H_{\mathcal{E}}})(V_{\mathcal{R}} \otimes I_{H_{\mathcal{E}}})V_{\mathcal{E}}, \quad T \in N,$$

and, by Remark 4.2, there exists a partial isometry $U : H \to S \otimes H_{\mathcal{R}} \otimes H_{\mathcal{E}}$ such that $UV_{\mathcal{E}\mathcal{R}} = (V_{\mathcal{R}} \otimes I_{H_{\mathcal{E}}})V_{\mathcal{E}}$, $U\pi(T) = (T \otimes I_{H_{\mathcal{R}}} \otimes I_{H_{\mathcal{E}}})U$ for all $T \in N$, and

$$\mathcal{C}_{U^*}(N'\bar{\otimes}\mathcal{B}(H_{\mathcal{R}})\bar{\otimes}\mathcal{B}(H_{\mathcal{E}})) \subseteq \pi(N)'. \tag{6}$$

Moreover,

$$\|(V_{\mathcal{R}} \otimes I_{H_{\mathcal{E}}})V_{\mathcal{E}} - UV_{\mathrm{id}}\| = \|UV_{\mathcal{E}\mathcal{R}} - UV_{\mathrm{id}}\| \leq \|V_{\mathcal{E}\mathcal{R}} - V_{\mathrm{id}}\| < \sqrt{\varepsilon}. \tag{7}$$

Let $\mathcal{R}^c : N'\bar{\otimes}\mathcal{B}(H_{\mathcal{R}}) \to \mathcal{B}(S')$ be the complement of $\mathcal{R}$ with respect to the Stinespring triple $(T \mapsto T\otimes I_{H_{\mathcal{R}}}, V_{\mathcal{R}}, S\otimes H_{\mathcal{R}})$, and define normal completely

positive maps $\mathcal{F}, \mathcal{R}^\flat : N' \bar{\otimes} \mathcal{B}(H_\mathcal{R}) \bar{\otimes} \mathcal{B}(H_\mathcal{E}) \to \mathcal{B}(S)$ by $\mathcal{F} = \mathcal{C}_{V_{\mathrm{id}}^*} \circ \mathcal{C}_{U^*}$ and $\mathcal{R}^\flat = \mathcal{C}_{V_\mathcal{E}^*} \circ (\mathcal{R}^c \otimes \mathrm{id}_{\mathcal{B}(H_\mathcal{E})})$. By (7) and [23, Proposition 3], $\|\mathcal{F} - \mathcal{R}^\flat\|_{\mathrm{cb}} < 2\sqrt{\varepsilon}$. Since $(\pi, V_{\mathrm{id}}, H)$ is a Stinespring triple for id_N, the uniqueness of the Stinespring representation (see (2)) implies that there exists a partial isometry $W : H \to S$ satisfying $WV_{\mathrm{id}} = I_S$, $V_{\mathrm{id}} = W^*$ and $W\pi(T) = TW$, for $T \in N$. Thus, $V_{\mathrm{id}}^* \pi(N)' V_{\mathrm{id}} \subseteq N'$ (see Remark 4.2) and (6) shows that the image of $\mathcal{F}$ lies in N'. By Lemma 4.6, there is a quantum channel

$$\widetilde{\mathcal{F}} : N' \bar{\otimes} \mathcal{B}(H_\mathcal{R}) \bar{\otimes} \mathcal{B}(H_\mathcal{E}) \to N' \quad \text{with} \quad \|\widetilde{\mathcal{F}} - \mathcal{R}^\flat\|_{\mathrm{cb}} < 4\sqrt{\varepsilon}.$$

Since the range of $\mathcal{R}$ lies in M, we trivially have that M' is private for $\mathcal{R}$. By the first part of the proof, M' is correctable for $\mathcal{R}^c$, so there is a quantum channel $\mathcal{G} : M' \to N' \bar{\otimes} \mathcal{B}(H_\mathcal{R})$ satisfying $\mathcal{R}^c \circ \mathcal{G} = \mathrm{id}_{M'}$. We have

$$\mathcal{R}^\flat \circ (\mathcal{G} \otimes \mathrm{id}_{\mathcal{B}(H_\mathcal{E})}) = \mathcal{C}_{V_\mathcal{E}^*}|_{M' \bar{\otimes} \mathcal{B}(H_\mathcal{E})} = \mathcal{E}^c, \tag{8}$$

where $\mathcal{E}^c : M' \bar{\otimes} \mathcal{B}(H_\mathcal{E}) \to \mathcal{B}(S)$ is the complement of $\mathcal{E}$ with respect to the Stinespring triple $(T \mapsto T \otimes I_{H_\mathcal{E}}, V_\mathcal{E}, S' \otimes H_\mathcal{E})$. By (8) and the fact that $\mathcal{G} \otimes \mathrm{id}_{\mathcal{B}(H_\mathcal{E})}$ is a complete contraction,

$$\|\widetilde{\mathcal{F}} \circ (\mathcal{G} \otimes \mathrm{id}_{\mathcal{B}(H_\mathcal{E})}) - \mathcal{E}^c\|_{\mathrm{cb}} \leq \|\widetilde{\mathcal{F}} - \mathcal{R}^\flat\|_{\mathrm{cb}} < 4\sqrt{\varepsilon}.$$

Since the range of $\widetilde{\mathcal{F}}$ is contained in N', the von Neumann algebra N is $4\sqrt{\varepsilon}$-private for $\mathcal{E}^c$.

Finally, if $\mathcal{E}^\sharp : \pi^\sharp(M)' \to \mathcal{B}(S)$ is another complement to $\mathcal{E}$, then there exists a partial isometry $U^\sharp : H^\sharp \to S' \otimes H_\mathcal{E}$ satisfying $\mathcal{E}^\sharp = \mathcal{E}^c \circ \mathcal{C}_{U^\sharp}$. Then

$$\|\widetilde{\mathcal{F}} \circ (\mathcal{G} \otimes \mathrm{id}_{\mathcal{B}(H_\mathcal{E})}) \circ \mathcal{C}_{U^\sharp} - \mathcal{E}^\sharp\| < 4\sqrt{\varepsilon}.$$

Applying Lemma 4.6 to the normal completely positive contraction $\mathcal{Q} = \widetilde{\mathcal{F}} \circ (\mathcal{G} \otimes \mathrm{id}_{\mathcal{B}(H_\mathcal{E})}) \circ \mathcal{C}_{U^\sharp}$, we obtain a quantum channel $\widetilde{\mathcal{Q}} : \pi^\sharp(M)' \to N'$ satisfying $\|\widetilde{\mathcal{Q}} - \mathcal{E}^\sharp\|_{\mathrm{cb}} < 8\sqrt{\varepsilon}$, so N is $8\sqrt{\varepsilon}$-private for $\mathcal{E}^\sharp$. □

Applications of Theorem 4.7 to Gaussian quantum channels will be given in the next section. In the remainder of the present section, we give two illustrations of this result. The first one relates to discrete Schur multipliers; we refer the reader to [26] for the relevant background.

Example 4.8. Let X be a non-empty countable set and $(\delta_x)_{x \in X}$ be the standard orthonormal basis of $\ell_2(X)$. We identify every element of $\mathcal{B}(\ell^2(X))$ with its corresponding (possibly infinite) matrix $[T_{x,y}]_{x,y \in X}$, where $T_{x,y} = \langle T\delta_y, \delta_x \rangle$, $x, y \in X$. Any collection of unit vectors $(|\psi_x\rangle)_{x \in X}$ in the Hilbert space $H = \ell_2(X)$ defines a correlation matrix $C := [\langle \psi_y | \psi_x \rangle]_{x,y \in X}$, which in turn yields a NUCP map $\Phi : \mathcal{B}(\ell_2(X)) \to \mathcal{B}(\ell_2(X))$ via *Schur multiplication*:

$$\Phi(T) = [\langle \psi_y | \psi_x \rangle T_{x,y}]_{x,y \in X}, \quad T \in \mathcal{B}(\ell_2(X)).$$

By abuse of notation, we denote by $\ell_\infty(X)$ the von Neumann subalgebra of diagonal matrices in $\mathcal{B}(\ell_2(X))$. It is straightforward to verify that $\Phi(D_1 T D_2) = D_1 \Phi(T) D_2$ for all $D_1, D_2 \in \ell_\infty(X)$ and all $T \in \mathcal{B}(\ell_2(X))$, *i.e.*, that Φ is an $\ell_\infty(X)$-bimodule map. Thus, $\ell_\infty(X)$ is correctable for Φ and,

by Theorem 4.7, it is private for any complement Φ^c of Φ. In particular, the range of any complement of Φ is contained in a commutative von Neumann algebra, reflecting the well-known fact that complements of discrete Schur multipliers are entanglement breaking (see [22]).

We next present an application of Theorem 4.7 by generalizing the main result in [20] concerning the structure of correctable subsystems for finite-dimensional channels as generalized multiplicative domains. In [20, Theorem 11], a one-to-one correspondence was established between correctable subsystems B of a finite-dimensional channel $\mathcal{E} : \mathcal{B}(S) \to \mathcal{B}(S)$ and generalized multiplicative domains $\mathrm{MD}_\pi(\mathcal{E})$, where the latter is defined relative to a projection $P \in \mathcal{P}(S)$, a C*-subalgebra $N \subseteq \mathcal{B}(PS)$ and a representation $\pi : N \to \mathcal{B}(S)$, to be

$$\begin{aligned}\mathrm{MD}_\pi(\mathcal{E}) := \big\{T \in N \mid \pi(T)(\mathcal{E}_* \circ (\mathcal{C}_P)_*(R)) = \mathcal{E}_* \circ (\mathcal{C}_P)_*(TR) \\ \text{and } (\mathcal{E}_* \circ (\mathcal{C}_P)_*(R))\pi(T) = \mathcal{E}_* \circ (\mathcal{C}_P)_*(RT), \text{ for all } R \in N\big\}.\end{aligned}$$

Specifically, if $S = (A \otimes B) \oplus (A \otimes B)^\perp$, then B is correctable if and only if $I_A \otimes \mathcal{B}(B) = \mathrm{MD}_\pi(\mathcal{E})$ for some representation $\pi\colon I_A \otimes \mathcal{B}(B) \to \mathcal{B}(S)$. In the Heisenberg picture, $T \in \mathrm{MD}_\pi(\mathcal{E})$ if and only if

$$\langle(\mathcal{C}_P \circ \mathcal{E}(X))T, R\rangle = \langle \mathcal{C}_P \circ \mathcal{E}(X\pi(T)), R\rangle$$

and

$$\langle T(\mathcal{C}_P \circ \mathcal{E}(X)), R\rangle = \langle \mathcal{C}_P \circ \mathcal{E}(\pi(T)X), R\rangle$$

for all $R \in N$ and $X \in \mathcal{B}(S)$.

Corollary 4.9. *Let S and S' be Hilbert spaces, $M \subseteq \mathcal{B}(S')$ be a von Neumann algebra, and $\mathcal{E} : M \to \mathcal{B}(S)$ be a quantum channel and $P \in \mathcal{P}(S)$. A von Neumann subalgebra $N \subseteq \mathcal{B}(PS)$ is correctable for $\mathcal{E}$ with respect to P if and only if there exists a normal representation $\pi : N \to M$ such that*

$$(9)\quad (\mathcal{C}_P \circ \mathcal{E}(X))T = \mathcal{C}_P \circ \mathcal{E}(X\pi(T)) \quad \textit{and} \quad T(\mathcal{C}_P \circ \mathcal{E}(X)) = \mathcal{C}_P \circ \mathcal{E}(\pi(T)X)$$

for all $T \in N$ and $X \in \mathcal{B}(S)$.

Proof. As in the proof of Theorem 4.7, it suffices to consider the case $P = I_S$. If there exists a normal representation $\pi : N \to M$ satisfying (9), then by taking $X = I$ in (9) and using the fact that $\mathcal{E}$ is unital, we see that N is correctable for $\mathcal{E}$.

Conversely, if N is correctable for $\mathcal{E}$, then by Theorem 4.7, N is private for any complement $\mathcal{E}^c$ of $\mathcal{E}$. Taking a Stinespring representation for $\mathcal{E}$ of the form $\mathcal{E}(X) = V^*(X \otimes I_H)V$, $X \in M$ (see (4)), the corresponding complement $\mathcal{E}^c : M' \bar{\otimes} \mathcal{B}(H) \to \mathcal{B}(S)$ has range in N', so N is a von Neumann subalgebra of $\mathcal{E}^c(M' \bar{\otimes} \mathcal{B}(H))'$. Taking a minimal Stinespring triple (π^c, V^c, H^c) for $\mathcal{E}^c$, it follows by Arveson's commutant lifting theorem [2, Theorem 1.3.1] that there exists a normal representation $\pi' : \mathcal{E}^c(M' \bar{\otimes} \mathcal{B}(H))' \to \pi^c(M' \bar{\otimes} \mathcal{B}(H))'$ satisfying $\pi'(Y)V^c = V^cY$ for all $Y \in \mathcal{E}^c(M' \bar{\otimes} \mathcal{B}(H))'$. By the uniqueness of the Stinespring representation, there exists an isometry $W : H^c \to S' \otimes H$

such that $WV^c = V$, $V^c = W^*V$, $W\pi^c(X') = X'W$ for all $X' \in M'\bar{\otimes}\mathcal{B}(H)$, and

$$W\pi^c(M'\bar{\otimes}\mathcal{B}(H))'W^* \subseteq (M'\bar{\otimes}\mathcal{B}(H))' = M \otimes I_H.$$

Let $\pi'' : M \otimes I_H \to M$ be the *-isomorphism defined by $\pi''(X \otimes 1) = X$ and note that, since W is an isometry, $\mathcal{C}_W \circ \pi'$ is a normal *-homomorphism. Thus, $\pi := \pi'' \circ \mathcal{C}_W \circ \pi'|_N : N \to M$ is a normal representation satisfying

$$\begin{aligned}\mathcal{E}(X\pi(T)) &= V^*((X\pi(T)) \otimes I_H)V = V^*(X \otimes I_H)(\pi(T) \otimes I_H)V \\ &= V^*(X \otimes I_H)W\pi'(T)W^*V = V^*(X \otimes I_H)W\pi'(T)V^c \\ &= V^*(X \otimes I_H)WV^cT = V^*(X \otimes I_H)VT = \mathcal{E}(X)T\end{aligned}$$

for all $X \in M$ and $T \in N$. Similarly, $T\mathcal{E}(X) = \mathcal{E}(\pi(T)X)$ for all $X \in M$ and $T \in N$. □

Remark 4.10. Corollary 4.9 implies that the correction channel $\mathcal{R}$ may always be taken to be *-homomorphism, a fact previously observed in the case $M = \mathcal{B}(S')$ for a separable Hilbert space S' [8, Proposition 4.4].

5. Private Algebras for Linear Bosonic Quantum Channels

In this section we begin our analysis of private algebras and generalized complementarity for linear bosonic quantum channels, focusing mainly on the subclass of Gaussian channels. Such channels arise naturally in the dynamics of open bosonic systems described by quadratic Hamiltonians (see [28] and the references therein). We begin with a short review of the relevant machinery, adopting the notation of [17], to which we refer the reader for details.

Let $\mathbb{R}^{2n}$ represent the phase space of a system of n bosonic modes. We will write vectors in $\mathbb{R}^{2n}$ as $z = (x_1, y_1, x_2, y_2, \cdots, x_n, y_n)$, where $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ are vectors in $\mathbb{R}^n$ describing the positions and momenta of the n modes. Let $U, V : \mathbb{R}^n \to \mathcal{B}(L_2(\mathbb{R}^n))$ be the strongly continuous unitary representations given by

$$V_x\psi(s) = e^{i\langle x,s\rangle}\psi(s) \quad \text{and} \quad U_y\psi(s) = \psi(s+y)$$

for $\psi \in L_2(\mathbb{R}^n)$ and $s \in \mathbb{R}^n$. These one parameter groups satisfy the Weyl form of the canonical commutation relations (CCR):

$$U_yV_x = e^{i\langle x,y\rangle}V_xU_y, \quad x, y \in \mathbb{R}^n.$$

Composing the two, we obtain the *Weyl representation* $W : \mathbb{R}^{2n} \to \mathcal{B}(L_2(\mathbb{R}^n))$ given by

$$W(z) = e^{\frac{i}{2}\langle x,y\rangle}V_xU_y, \quad z \in \mathbb{R}^{2n}.$$

Let

$$\Delta_n = \bigoplus_{i=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and, writing $z' = (x'_1, y'_1, \ldots, x'_n, y'_n)$, let

$$\Delta(z, z') = \langle z, \Delta_n(z') \rangle = \sum_{i=1}^{n} (x_i y'_i - x'_i y_i)$$

be the canonical *symplectic form* on $\mathbb{R}^{2n}$. The Weyl representation W satisfies the Weyl–Segal form of the CCR:

$$W(z + z') = e^{\frac{i}{2}\Delta(z,z')} W(z) W(z'), \quad z, z' \in \mathbb{R}^{2n}. \tag{10}$$

The linear transformations $T : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ which preserve the symplectic form Δ, in the sense that

$$\Delta(Tz, Tz') = \Delta(z, z'), \quad z, z' \in \mathbb{R}^{2n},$$

are called *symplectic transformations*. These form a subgroup of $\mathrm{GL}(2n, \mathbb{R})$ denoted by $\mathrm{Sp}(2n, \mathbb{R})$. Note that, by (10), $[W(z), W(z')] = 0$ if and only if $\Delta(z, z') \in 2\pi\mathbb{Z}$, where as usual $[X, Y] = XY - YX$ is the commutator of two operators X and Y. By (10) and the Stone-von Neumann theorem, given any $T \in \mathrm{Sp}(2n, \mathbb{R})$, there exists a unitary $U_T \in \mathcal{B}(L_2(\mathbb{R}^n))$ such that

$$W(Tz) = U_T^* W(z) U_T \tag{11}$$

for all $z \in \mathbb{R}^{2n}$.

An important feature of the Weyl representation W is that it allows one to study the statistical properties of quantum states via a "non-commutative characteristic function". Specifically, given a state $\rho \in \mathcal{T}(L_2(\mathbb{R}^n))$, we let $\varphi_\rho(z) = \mathrm{Tr}(\rho W(z))$, for $z \in \mathbb{R}^{2n}$. This characteristic function φ_ρ determines the operator ρ via the following inversion formula:

$$\rho = \frac{1}{(2\pi)^n} \int_{\mathbb{R}^{2n}} \varphi_\rho(z) W(-z)\, dz,$$

where the integral converges to ρ in the weak operator topology by [16, Corollary 5.3.5]. A state $\rho \in \mathcal{T}(L_2(\mathbb{R}^n))$ is said to be *Gaussian* if its characteristic function is of the form

$$\varphi_\rho(z) = \exp\left(i\langle m, z\rangle - \tfrac{1}{2}\alpha(z, z)\right)$$

where $m \in \mathbb{R}^{2n}$ is a vector, called the *mean of* ρ, and α is a symmetric bilinear form on $\mathbb{R}^{2n}$ known as the *covariance matrix of* ρ.

A *linear bosonic channel* is a quantum channel $\mathcal{E} : \mathcal{B}(L_2(\mathbb{R}^n)) \to \mathcal{B}(L_2(\mathbb{R}^n))$ for which there exists $\ell \in \mathbb{N}$, a state $\rho_E \in \mathcal{T}(L_2(\mathbb{R}^\ell))$ in an ℓ-mode bosonic environment and a symplectic block matrix

$$T = \begin{pmatrix} K & L \\ K_E & L_E \end{pmatrix} \in \mathrm{Sp}(2(n + \ell), \mathbb{R})$$

where K is $2n \times 2n$ and L_E is $2\ell \times 2\ell$, so that if $U_T \in \mathcal{B}(L_2(\mathbb{R}^{n+\ell}))$ is the unitary associated by (11) with T, then the pre-adjoint of $\mathcal{E}$ has the form

$$\mathcal{E}_*(\rho) = \mathrm{Tr}_E(U_T(\rho \otimes \rho_E)U_T^*), \quad \rho \in \mathcal{T}(L_2(\mathbb{R}^n))$$

where the partial trace is taken over the tensor factor $E = L_2(\mathbb{R}^\ell)$ of $L_2(\mathbb{R}^{n+\ell}) = L_2(\mathbb{R}^n) \otimes L_2(\mathbb{R}^\ell)$. Using the block decomposition of T, one may easily verify (see [17, §12.4.1]) that

$$\mathcal{E}(W(z)) = f(z)W(Kz), \quad \text{where} \quad f(z) = \varphi_{\rho_E}(K_E z), \quad z \in \mathbb{R}^{2n}.$$

If f is the characteristic function of a Gaussian state, then $\mathcal{E}$ is called a *Gaussian channel*. In this case, the environment state ρ_E in the representation of $\mathcal{E}_*$ is a Gaussian state.

One immediately obtains private subalgebras if $K : \mathbb{R}^n \to \mathbb{R}^n$ does not have full rank. Indeed, if $R \subseteq \mathbb{R}^n$ denotes the image of K, then it is clear that $\mathcal{E}(\mathcal{B}(L_2(\mathbb{R}^n))) \subseteq W(R)''$, where the double commutant $W(R)''$ coincides with the von Neumann subalgebra of $\mathcal{B}(L_2(\mathbb{R}^n))$ generated by $\{W(z) \mid z \in R\}$. Let

$$R^\Delta := \{z \in \mathbb{R}^{2n} \mid \Delta(z, z') = 0 \text{ for all } z' \in R\}$$

be the *symplectic complement* of R. By the CCR (10), $[W(z), W(z')] = 0$ if $\Delta(z, z') = 0$, and it follows that $W(R^\Delta) \subseteq W(R)'$. Hence,

$$\mathcal{E}(\mathcal{B}(L_2(\mathbb{R}^n))) \subseteq W(R^\Delta)' = (W(R^\Delta)'')',$$

and we have the following result.

Proposition 5.1. *Let $\mathcal{E} : \mathcal{B}(L_2(\mathbb{R}^n)) \to \mathcal{B}(L_2(\mathbb{R}^n))$ be a linear bosonic channel, and let R be the range of the matrix K with symplectic complement R^Δ. Then the von Neumann algebra $W(R^\Delta)''$ is private for $\mathcal{E}$.*

Example 5.2. For a simple example with $n = 1$, let $S = L_2(\mathbb{R})$ and consider the class of single mode Gaussian channels $\mathcal{E} : \mathcal{B}(S) \to \mathcal{B}(S)$ satisfying

$$\mathcal{E}(W(z)) = f(z)W(Kz), \quad z = (x, y) \in \mathbb{R}^2$$

where

$$K = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad f(z) = \exp\big(-\tfrac{1}{2}\alpha(x^2 + y^2)\big),$$

with $\alpha = N_0 + \frac{1}{2}$ for some non-negative integer N_0. This class is known as A_2 in Holevo's classification of single mode Gaussian channels [15]. In this case, the range of K is $R = \mathbb{R} \times \{0\}$ and $R^\Delta = R$, so

$$W(R)'' = \{V_x \mid x \in \mathbb{R}\}'' = L_\infty(\mathbb{R})$$

is private for $\mathcal{E}$, where we canonically identify $L_\infty(\mathbb{R})$ with the (abelian) von Neumann subalgebra of $\mathcal{B}(S)$ consisting of multiplication operators by essentially bounded functions.

By Theorem 4.7, $L_\infty(\mathbb{R})$ is a correctable subalgebra for any complementary channel $\mathcal{E}^c$ of $\mathcal{E}$. Let us show this explicitly by computing a correction channel $\mathcal{R}$ for one particular complement $\mathcal{E}^c$. First, one may easily verify that the pre-adjoint $\mathcal{E}_* : \mathcal{T}(S) \to \mathcal{T}(S)$ can be represented as

$$\mathcal{E}_*(\rho) = \mathrm{Tr}_E(U_T(\rho \otimes \rho_E)U_T^*), \quad \rho \in \mathcal{T}(S),$$

where E is a copy of $L_2(\mathbb{R})$ and $\rho_E \in \mathcal{T}(E)$ is the Gaussian state with characteristic function $\varphi_{\rho_E} = f$, and $T \in \mathrm{Sp}(4,\mathbb{R})$ is given by the block matrix

$$T = \begin{pmatrix} K & -I \\ I & K' \end{pmatrix}$$

where I is the 2×2 identity matrix and $K' = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

The state ρ_E is the Gibbs thermal state with mean photon number N_0, and is pure if and only if $N_0 = 0$. Thus, let E' be another copy of $L_2(\mathbb{R})$, and let $|\psi\rangle \in E \otimes E'$ be a canonical purification of ρ_E, that is, $\rho_E = \mathrm{Tr}_{E'}(|\psi\rangle\langle\psi|)$. Then

$$\mathcal{E}_*(\rho) = \mathrm{Tr}_{E\otimes E'}((U_T \otimes I_{E'})(\rho \otimes |\psi\rangle\langle\psi|)(U_T^* \otimes I_{E'})), \quad \rho \in \mathcal{T}(S),$$

so we can obtain a complement $\mathcal{E}^c : \mathcal{B}(E \otimes E') \to \mathcal{B}(S)$ whose pre-adjoint $\mathcal{E}^c_*$ is given by

$$\mathcal{E}^c_*(\rho) = \mathrm{Tr}_S((U_T \otimes I_{E'})(\rho \otimes |\psi\rangle\langle\psi|)(U_T^* \otimes I_{E'})), \quad \rho \in \mathcal{T}(S).$$

For H a Hilbert space of the form $L^2(\mathbb{R}^n)$, let us denote the corresponding Weyl representation $W\colon \mathbb{R}^{2n} \to \mathcal{B}(H)$ by W_H. For $z, z' \in \mathbb{R}^2$ and $\rho \in \mathcal{T}(S)$, we have

$$\begin{aligned}
&\langle \mathcal{E}^c(W_{E\otimes E'}(z,z')), \rho\rangle \\
&\quad = \mathrm{Tr}\left((U_T \otimes I_{E'})(\rho \otimes |\psi\rangle\langle\psi|)(U_T^* \otimes I_{E'})(I_S \otimes W_{E\otimes E'}(z,z'))\right) \\
&\quad = \mathrm{Tr}\left((\rho \otimes |\psi\rangle\langle\psi|)(U_T^* \otimes I_{E'})W_{S\otimes E\otimes E'}(0,z,z')(U_T \otimes I_{E'})\right) \\
&\quad = \mathrm{Tr}\left((\rho \otimes |\psi\rangle\langle\psi|)W_{S\otimes E\otimes E'}(T(0,z),z')\right) \\
&\quad = \mathrm{Tr}\left((\rho \otimes |\psi\rangle\langle\psi|)W_{S\otimes E\otimes E'}(-z,(0,y),z')\right) \\
&\quad = \mathrm{Tr}\left(|\psi\rangle\langle\psi| W_{E\otimes E'}((0,y),z')\right) \cdot \langle W_S(-z), \rho\rangle.
\end{aligned}$$

Since $\rho \in \mathcal{T}(S)$ was arbitrary, it follows that

$$\mathcal{E}^c(W_{E\otimes E'}(z,z')) = \mathrm{Tr}(|\psi\rangle\langle\psi| W_{E\otimes E'}((0,y),z'))W_S(-z), \quad z, z' \in \mathbb{R}^2.$$

Given the above structure of $\mathcal{E}^c$, it is clear that the map

$$\mathcal{R} : L_\infty(\mathbb{R}) \to \mathcal{B}(E \otimes E'), \quad \mathcal{R}(W_S(x,0)) = W_{E\otimes E'}((-x,0),0), \quad x \in \mathbb{R}$$

defines a quantum channel satisfying $\mathcal{E}^c \circ \mathcal{R} = \mathrm{id}_{L_\infty(\mathbb{R})}$.

Remark 5.3. The symplectic matrix T in the preceding example is not unique. Indeed, any symplectic block matrix of the form

$$\begin{pmatrix} K & * \\ I & * \end{pmatrix}$$

will do, as only the first column is relevant for the description of $\mathcal{E}$. In general, if $A, B : \mathbb{R}^n \to \mathbb{R}^n$ satisfy $\Delta = A^t \Delta A + B^t \Delta B$ (so that the map $z \mapsto Az \oplus Bz$ is a symplectic embedding), then the matrix

$$\begin{pmatrix} A & * \\ B & * \end{pmatrix}$$

can be completed to an element of $\mathrm{Sp}(2n, \mathbb{R})$ (see [17, Theorem 12.30]). In particular, when $[A, B] = 0$, which is the case in the above example, there is a canonical choice for matrices $C, D \in M_n(\mathbb{R})$ turning

$$\begin{pmatrix} A & C \\ B & D \end{pmatrix}$$

into a symplectic matrix, namely $C = -B'$ and $D = A'$, where $B' = \Delta^{-1} B^t \Delta$ and $A' = \Delta^{-1} A^t \Delta$ are the *symplectic adjoints* of A and B, respectively. This is precisely how we chose T above, and since the structure of $K' = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ was crucial in determining the recovery channel $\mathcal{R}$ (and the overall structure of $\mathcal{E}^c$), the above example may be a glimpse of a deeper connection between complementarity and symplectic duality.

6. Conclusion

In this paper, we generalized the formalism of private subspaces and private subsystems to the setting of von Neumann algebras using commutant structures, introduced a generalized framework for studying complementarity of quantum channels, and established a general complementarity theorem between operator private and correctable subalgebras that applies to both the finite and infinite dimensional settings. This new framework is particularly amenable to the important class of linear bosonic channels, and our preliminary investigations suggests a deeper connection between complementarity and symplectic duality. Moreover, since symplectic geometry has played a decisive role in the development of quantum error correcting codes [10], it is natural to develop such a formalism for private quantum codes via complementarity in both the finite and infinite-dimensional settings. This, and related questions are currently being pursued and will appear in future work.

References

[1] Ambainis, A., Mosca, M., Tapp, A., de Wolf, R., *Private quantum channels*, 41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000), 547-553, IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.

[2] Arveson, W. B., *Subalgebras of C^*-algebras*, Acta Math. **123** (1969), 141-224.

[3] Bartlett, S. D., Hayden, P., Spekkens, R. W., *Random subspaces for encryption based on a private shared Cartesian frame*, Phys. Rev. A **72** (5), (2005) 052329.

[4] Bartlett, S. D., Rudolph, T., Spekkens, R. W., *Decoherence-full subsystems and the cryptographic power of a private shared reference frame*, Phys. Rev. A **70** (3), (2004) 032307.

[5] Bény, C., *Conditions for the approximate correction of algebras*, TQC 2009 LNCS 5906, (2009) pp. 6675.

[6] Bény, C., Kempf, A., Kribs, D. W., *Generalization of quantum error correction via the Heisenberg picture*, Phys. Rev. Lett. **98** (2007), 100502.

[7] Bény, C., Kempf, A., Kribs, D. W., *Quantum error correction of observables*, Phys. Rev. A **76** (2007), 042303.

[8] Bény, C., Kempf, A., Kribs, D. W., *Quantum error correction on infinite-dimensional Hilbert spaces*, J. Math. Phys. **50** (2009), no. 6, 062108, 24 pp.

[9] Boykin, P.O., Roychowdhury, V. *Optimal encryption of quantum bits*, Phys. Rev. A **67** (2003), 042317.
[10] Calderbank, A. R., Rains, E. M., Shor, P. W., Sloane, N. J. A., *Quantum error correction and orthogonal geometry*, Phys. Rev. Lett. **78** (1997), no. 3, 405-408.
[11] Church, A., Kribs, D.W., Pereira, R., Plosker, S., *Private quantum channels, conditional expectations, and trace vectors*, Quant. Inf. & Comp. **11** (2011), 774-783.
[12] Crepeau, C., Gottesman, D., Smith, A., *Secure multi-party quantum computing*, 34th Annual Symposium on Theory of Computing (ACM, Montreal) (2002), 643.
[13] Cleve, R., Gottesman, D., Lo, H.-L., *How to share a quantum secret*, Phys. Rev. Lett. **83** (1999), 648.
[14] Holevo, A.S., *On complementary channels and the additivity problem*, Probab. Theory and Appl. **51** (2005), 133-143.
[15] Holevo, A. S., *One-mode quantum Gaussian channels: structure and quantum capacity*, Prob. Inf. Trans. **43** (2007), no. 1, 1-11.
[16] Holevo, A. S., *Probabilistic and Statistical Aspects of Quantum Theory*, Scuola Normale Superiore Pisa, 2011.
[17] Holevo, A. S., *Quantum Systems, Channels, Information. A Mathematical Introduction*, De Gruyter Studies in Mathematical Physics, 16. De Gruyter, Berlin, 2012.
[18] Jochym-O'Conor, T., Kribs, D. W., Laflamme, R., Plosker, S., *Quantum subsystems: exploring complementarity of quantum privacy and error correction*, Phys. Rev. A **90**, (2014) 032305.
[19] Jochym-O'Conor, T., Kribs, D. W., Laflamme, R., Plosker, S., *Private quantum subsystems*, Phys. Rev. Lett. **111**, (2013) 030502.
[20] Johnston, N., Kribs, D. W., *Generalized multiplicative domains and quantum error correction*, Proc. Amer. Math. Soc. **139** (2011), 627-639.
[21] Kretschmann, D., Kribs, D. W., Spekkens, R. W., *Complementarity of private and correctable subsystems in quantum cryptography and error correction*, Phys. Rev. A **78** (3), (2008) 032330.
[22] King, C., Matsumoto, K., Nathanson, M., Ruskai, M. B., *Properties of conjugate channels with applications to additivity and multiplicativity*, Markov Process. Related Fields **13**, (2007) 391-423.
[23] Kretschmann, D., Schlingemann, D., Werner, R. F., *A continuity theorem for Stinespring's dilation*, J. Funct. Anal. **255** (2008) 1889-1904.
[24] Kretschmann, D., Schlingemann, D., Werner, R. F., *The information-disturbance tradeoff and the continuity of Stinespring's representation*, IEEE Trans. Inf. Theory, **54** (4), (2008) pp. 1708-1717.
[25] Linblad, G., *A general no-cloning theorem*, Lett. Math. Phys. **47** (1999), 189-196.
[26] Paulsen, V. I., *Completely bounded maps and operator algebras*, Cambridge University Press, 2002.
[27] Takesaki, M., *Theory of Operator Algebras I*, Encyclopedia of Mathematical Sciences 124, Springer-Verlag Berlin–Heidelberg–New York (2002).
[28] Weedbrook, C., *et al*, *Gaussian quantum information*, Rev. Mod. Phys. **84** (2012), 621-669.

[1]School of Mathematics & Statistics, Carleton University, Ottawa, ON, Canada H1S 5B6

[2]Université Lille 1 - Sciences et Technologies, UFR de Mathématiques, Laboratoire de Mathématiques Paul Painlevé - UMR CNRS 8524, 59655 Villeneuve d'Ascq Cédex, France
E-mail address: jason_crann@carleton.ca

[1]Department of Mathematics & Statistics, University of Guelph, Guelph, ON, Canada N1G 2W1

[2]Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada N2L 3G1
E-mail address: dkribs@uoguelph.ca

School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland
E-mail address: rupert.levene@ucd.ie

Pure Mathematics Research Centre, Queen's University Belfast, Belfast BT7 1NN, United Kingdom
E-mail address: i.todorov@qub.ac.uk