Quantum Information and Computation, Vol. 11, No. 9&10 (2011) 0774–0783

PRIVATE QUANTUM CHANNELS, CONDITIONAL EXPECTATIONS, AND TRACE VECTORS

AMBER CHURCH
Department of Mathematics & Statistics, University of Guelph
Guelph, ON, N1G 2W1, Canada

DAVID W. KRIBS
Department of Mathematics & Statistics, University of Guelph
Guelph, ON, N1G 2W1, Canada

Institute for Quantum Computing, University of Waterloo
Waterloo, ON, N2L 3G1, Canada

RAJESH PEREIRA
Department of Mathematics & Statistics, University of Guelph
Guelph, ON, N1G 2W1, Canada

SARAH PLOSKER
Department of Mathematics & Statistics, University of Guelph
Guelph, ON, N1G 2W1, Canada

Received May 26, 2011
Revised July 4, 2011

Private quantum channels are the quantum analogue of the classical one-time pad. Conditional expectations and trace vectors are notions that have been part of operator algebra theory for several decades. We show that the theory of conditional expectations and trace vectors is intimately related to that of private quantum channels. Specifically we give a new geometric characterization of single qubit private quantum channels that relies on trace vectors. We further show that trace vectors completely describe the private states for quantum channels that are themselves conditional expectations. We also discuss several examples.

Keywords: private quantum channels, private states, trace vectors, conditional expectations, completely positive maps, C*-algebras.
Communicated by: R Jozsa & M Mosca

1 Introduction

Private quantum channels are a basic tool in quantum cryptography [1]. Conditional expectations and trace vectors are notions that have played a role in the theory of operator algebras for more than half a century [2, 3]. In this paper we show that there is an intimate relationship between the two subjects. Specifically we give a new geometric characterization of single qubit private quantum channels via the Bloch sphere representation for qubit states that relies on trace vectors. We further show that trace vectors completely describe the private states for quantum channels that are themselves conditional expectations.

In the next two sections we introduce private quantum channels, conditional expectations, and trace vectors. We discuss basic properties and include simple examples of each. We then consider the single qubit case in detail, giving a trace vector characterization of private states for unital quantum channels. We finish with a complete characterization of the private states for channels that are themselves conditional expectations in terms of trace vectors.

2 Private Quantum Channels

We will use $\mathcal{H}$ or $\mathcal{K}$ to denote Hilbert spaces (which are assumed to be finite dimensional in this paper) and denote a d-dimensional Hilbert space by $\mathcal{H}_d$. We denote the set of linear operators on $\mathcal{H}$ by $\mathcal{L}(\mathcal{H})$, and we use $\mathbb{M}_d$ to denote the algebra of $d \times d$ complex matrices, which when convenient will be regarded as the matrix representations of operators in $\mathcal{L}(\mathcal{H}_d)$ with respect to a given orthonormal basis for $\mathcal{H}_d$. The identity element of an operator space X will be denoted by $\mathbb{1}_X$, or simply by $\mathbb{1}$ if the space is implied by the context, and we will write $\mathbb{1}_d$ for the identity of $\mathbb{M}_d$.

We will use Dirac notation for vectors $|\phi\rangle$ and vector duals $\langle\phi|$. Thus pure states are represented as $|\phi\rangle\langle\phi|$. General quantum states are represented by density operators (nonnegative operators with trace equal to 1), and we will use notation such as ρ, σ in that case. The adjoint of an operator A will be written $A^\dagger$, and we will reserve the asterisk notation when discussing abstract C*-algebras.

A quantum channel is a linear, completely positive, trace preserving map $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$. (Channels are generally defined on the set of trace class operators, with their dual maps defined on the set of bounded operators, but the sets coincide in the finite dimensional case.) Every channel can be written as

$$\mathcal{E}(\rho) = \sum_{i=1}^{n} K_i \rho K_i^\dagger, \tag{1}$$

for some operators $K_i : \mathcal{H} \to \mathcal{K}$ with $\sum_{i=1}^{n} K_i^\dagger K_i = \mathbb{1}$, for any density operator ρ. We call a representation of $\mathcal{E}$ as in equation (1) a *Kraus decomposition* of $\mathcal{E}$. A channel $\mathcal{E}$ is called a *random unitary channel* if it admits a decomposition

$$\mathcal{E}(\rho) = \sum_i p_i U_i \rho U_i^\dagger \qquad \forall \rho, \tag{2}$$

where $\{p_i\}$ form a probability distribution and U_i are unitary operators.

In quantum cryptography, a private quantum channel (PQC) is the quantum analogue to the classical one-time pad. The following definition gives the mathematical framework for the notion in quantum information.

Definition 1 *Let $\mathcal{S} \subseteq \mathcal{H}$ be a set of pure states and let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ be a channel. Let ρ_0 be a density operator acting on $\mathcal{H}$. Then $[\mathcal{S}, \mathcal{E}, \rho_0]$ is a* private quantum channel *(PQC) if for any state $|\phi\rangle \in \mathcal{S}$, we have*

$$\mathcal{E}(|\phi\rangle\langle\phi|) = \rho_0.$$

PQCs were first considered in [1], where the authors consider a particular class of random unitary channels. The most basic example is the following.

Definition 2 *A map* $\mathcal{E} : \mathfrak{B}(\mathcal{H}_{2^n}) \to \mathfrak{B}(\mathcal{H}_{2^n})$ *is called a* depolarizing channel *if, for any density matrix* $\rho \in \mathfrak{B}(\mathcal{H}_{2^n})$*, we have*

$$\mathcal{E}(\rho) = \frac{p}{n}\mathbb{1} + (1-p)\rho,$$

where $0 < p \leq 1$ *is a probability. When* $p = 1$ *the* completely depolarizing channel *is obtained, which gives the simplest example of a PQC, where every pure state is a private state. We denote the completely depolarizing channel by* $\mathcal{E}_{\mathbb{C}}$*.*

3 Conditional Expectations and Trace Vectors

We recall a basic definition from operator algebras. Suppose there exists an orthogonal direct sum decomposition of a Hilbert space as $\mathcal{H} = \bigoplus_i (M_i \otimes N_i) \oplus K$. Let $\mathcal{A}$ be an algebra of operators in $\mathcal{L}(\mathcal{H})$ consisting of all operators that belong to the set $\mathcal{A} = \bigoplus_i (\mathbb{1}_{M_i} \otimes \mathcal{L}(N_i)) \oplus 0_K$, where 0_K is the zero operator on K. We call $\mathcal{A}$ a *(concrete finite dimensional) C*-algebra*. $\mathcal{A}$ is unital if $\mathbb{1}_{\mathcal{H}} \in \mathcal{A}$; i.e., $\mathcal{K}$ is the zero subspace. A $*$-subalgebra $\mathcal{B}$ of $\mathcal{A}$ is a subset that is also a C*-algebra. See [4] for basic C*-algebra theory.

Definition 3 *Let* $\mathcal{A}$ *be a C*-algebra and let* $\mathcal{B} \subseteq \mathcal{A}$ *be a unital *-subalgebra. We call a linear map* $\mathcal{E}_{\mathcal{B}} : \mathcal{A} \to \mathcal{B}$ *a* conditional expectation *of* $\mathcal{A}$ *onto* $\mathcal{B}$ *if*

(i) $\mathcal{E}_{\mathcal{B}}(b) = b$ *for all* $b \in \mathcal{B}$*;*

(ii) $\mathcal{E}_{\mathcal{B}}(b_1 a b_2) = b_1 \mathcal{E}_{\mathcal{B}}(a) b_2$ *for all* $b_1, b_2 \in \mathcal{B}$ *and for all* $a \in \mathcal{A}$*;*

(iii) $a \in \mathcal{A}$, $a \geq 0$ *implies* $\mathcal{E}_{\mathcal{B}}(a) \geq 0$*.*

Conditional expectations were first considered in [2]. We are interested in conditional expectations from $\mathbb{M}_n$ onto a subalgebra that are also quantum channels and hence trace preserving. We will therefore restrict ourselves to trace preserving conditional expectations. We will call such maps *conditional expectation channels*.

More examples of conditional expectation channels will be discussed below, but for the reader familiar with quantum information, we note here that the n-qubit completely depolarizing channel $\mathcal{E}_{\mathbb{C}}$ is the conditional expectation onto the trivial scalar algebra $\mathbb{C} \cdot \mathbb{1}_{2^n}$. One way to see how conditional expectations inevitably arise in the theory is through trace inner products.

Definition 4 *A linear functional* $\tau : \mathcal{A} \to \mathbb{C}$ *is a* faithful trace *if*

(i) $\tau(a_1 a_2) = \tau(a_2 a_1)$

(ii) $\tau(a^\dagger a) > 0$ *for all* $a \in \mathcal{A}$ *with* $a \neq 0$*.*

Given a faithful trace τ on $\mathcal{A}$ we can define an inner product $\langle a_1, a_2 \rangle = \tau(a_1^\dagger a_2)$. We note that if $\mathcal{A}$ has a faithful trace τ, the orthogonal projection onto $\mathcal{B}$ with respect to this inner product is the unique τ-preserving conditional expectation from $\mathcal{A}$ to $\mathcal{B}$. The essential structure of this argument can be found in [2]. The most well-known example is the so-called Hilbert-Schmidt inner product $\langle A, B \rangle = \mathrm{Tr}(A^\dagger B)$ on $\mathcal{M}_n$.

3.1 Trace vectors

We now consider trace vectors, a notion that initially arose in work of Murray and von Neumann [3], and has more recently been studied in the field of matrix theory.

Definition 5 *Let $\mathcal{A}$ be a $*$-subalgebra of $\mathcal{L}(\mathcal{H}_n)$. A vector $|v\rangle$ is a* trace vector *of $\mathcal{A}$ if*

$$\langle v|a|v\rangle = \frac{1}{n}\operatorname{Tr} a \quad \forall a \in \mathcal{A}.$$

More generally, given a density operator ρ_0, we say $|v\rangle$ is a trace vector with respect to ρ_0 *of $\mathcal{A}$ if*

$$\langle v|a|v\rangle = \operatorname{Tr}(\rho_0 a) \quad \forall a \in \mathcal{A}. \tag{3}$$

Thus by "trace vector", we really mean "trace vector with respect to $\frac{1}{n}\mathbb{1}_n$".

By letting $a = \mathbb{1}$ in the definition of a trace vector, we find $\langle v|v\rangle = 1$; a trace vector has unit length. It is easy to build a trace vector from other trace vectors in order to create a more general class of examples. Indeed, if $|v_i\rangle$ is a trace vector of the algebra $\mathcal{A}_i = (\mathbb{1}_{M_i} \otimes \mathcal{L}(N_i)) \oplus 0_K$ for $i \in \{1, \ldots, q\}$, then $|v\rangle = \bigoplus_{i=1}^q |v_i\rangle$ is a trace vector of the algebra $\mathcal{A} = \bigoplus_{i=1}^q \mathcal{A}_i$. In this way, trace vectors behave predictably. This also allows us to consider each summand separately, as we will do later.

Example 1 *As a fundamental example for quantum information, consider a maximally entangled state $|\varphi_e\rangle \in \mathcal{H}_m \otimes \mathcal{H}_n$. That is, a state $|\varphi_e\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |e_i\rangle \otimes |f_i\rangle$, where $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ form orthonormal sets in $\mathcal{H}_m$ and $\mathcal{H}_n$ respectively, and $d = \min\{m, n\}$. If $m \geq n$, then one can check via direct calculation that $|\varphi_e\rangle$ is a trace vector for the algebra $\mathbb{1}_m \otimes \mathcal{L}(\mathcal{H}_n)$. And if $m = n$ an analogous calculation works for $\mathcal{L}(\mathcal{H}_m) \otimes \mathbb{1}_n$.*

The general case is clarified by the following theorem of the third author. We recall that a vector $|v\rangle$ is a *separating vector* of an algebra $\mathcal{A}$ if $a|v\rangle = 0$ for some $a \in \mathcal{A}$ implies $a = 0$.

Theorem 2 *If $\mathcal{A}$ is a unital $*$-subalgebra of $\mathbb{M}_n$, then the following conditions are equivalent:*

1. *$\mathcal{A}$ is unitarily equivalent to $\oplus_{i=1}^q \left(\mathbb{1}_{m_i} \otimes \mathbb{M}_{n_i}\right)$, where $m_i \geq n_i$ for all i and $\sum_{i=1}^q m_i n_i = n$.*

2. *$\mathcal{A}$ has a separating vector.*

3. *$\mathcal{A}$ has a trace vector.*

4. *There exists a set of trace vectors of $\mathcal{A}$ that form an orthonormal basis of $\mathbb{C}^n$.*

This result is proved in [5]. A related infinite dimensional open problem goes all the way back to von Neumann [6]. Consider two simple cases. It is clear that $\mathbb{M}_n$ has no trace vectors – from both the theorem and the definition of trace vectors. On the other hand, let Δ_2 be the algebra of 2×2 diagonal matrices with respect to a basis $\{|0\rangle, |1\rangle\}$. One can readily check that the trace vectors for Δ_2 are (up to complex phase) all vectors of the form $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$, for $0 \leq \theta < 2\pi$; in other words, the set of all states that lie on the equator in the Bloch sphere representation for qubits (this point is further elucidated in the next section).

4 Private Quantum Channels on the Bloch Sphere

In this section we give a geometric characterization of single qubit unital PQCs in terms of the Bloch sphere representation [7] for single qubit states. We also show how the private states for such PQCs are determined by trace vectors. An alternative description was discussed in [8], where the entropy of sets of such private states was considered.

Every unital quantum channel is a random unitary channel in the single qubit case [9]. Thus, our private quantum channel $[\mathcal{S}, \mathcal{E}, \rho_0]$ in this case is given by a random unitary channel $\mathcal{E} : \mathbb{M}_2 \to \mathbb{M}_2$, a set of pure states $\mathcal{S}$, and an output density matrix ρ_0. More precisely, we have $\mathcal{E}(|v\rangle\langle v|) = \rho_0$ for all $|v\rangle \in \mathcal{S}$. We would like to allow for the possibility of orthonormal vectors in $\mathcal{S}$. As the channel is unital this can only occur if $\rho_0 = \frac{1}{n}\mathbb{1}$, and hence we shall focus on this case here.

Using the Bloch sphere representation, we can associate to any density matrix $\rho \in \mathbb{M}_2$ a Bloch vector $\vec{r} \in \mathbb{R}^3$ satisfying $\|\vec{r}\| \leq 1$, where

$$\rho = \frac{\mathbb{1} + \vec{r} \cdot \vec{\sigma}}{2}. \tag{4}$$

We use $\vec{\sigma}$ to denote the *Pauli vector*, that is, $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)^T$. Note that the set $\{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ forms a basis for the *real* vector space of Hermitian matrices in $\mathbb{M}_2$. We recall that a state is pure if and only if $\|\vec{r}\| = 1$ and that the maximally mixed state $\frac{\mathbb{1}}{n}$ has Bloch vector $\vec{r} = \vec{0}$.

As discussed in [10], every linear map $\Phi : \mathbb{M}_2 \to \mathbb{M}_2$ can be represented in the basis $\{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ by a 4×4 matrix $\mathbb{T}$, and Φ preserves the trace if and only if the first row of the matrix $\mathbb{T}$ satisfies $t_{1k} = \delta_{1k}$; i.e.,

$$\mathbb{T} = \begin{pmatrix} 1 & \mathbf{0} \\ \vec{t} & T \end{pmatrix} \tag{5}$$

where T is a 3×3 matrix, $\mathbf{0}$ is a row vector, and $\vec{t}$ is a column vector. The transformation Φ maps the subspace of Hermitian matrices into itself *iff* $\mathbb{T}$ is real; finally, the map Φ is unital *iff* $\vec{t} = \vec{0}$.

Thus, every unital qubit channel $\mathcal{E}$ can be represented as

$$\mathcal{E}\left(\frac{1}{2}\left[\mathbb{1} + \vec{r} \cdot \vec{\sigma}\right]\right) = \frac{1}{2}\left[\mathbb{1} + (T\vec{r}) \cdot \vec{\sigma}\right], \tag{6}$$

where T and $\vec{t}$ are real, and we recall any density matrix can be written as in equation (4). Here, the submatrix T represents a deformation of the Bloch sphere, while the vector $\vec{t}$ represents a translation. This affine mapping of the Bloch sphere into itself is also discussed in section 8.3.2 of [7].

We are of course interested in cases where $\mathcal{S}$ is nonempty. This is easily seen to occur precisely when T in equation (6) has non-trivial nullspace.

Thus we consider the cases in which T has non-trivial nullspace; that is, the subspace of vectors $\vec{r}$ such that $T\vec{r} = 0$ is one, two, or three-dimensional.

Finally, we note that in the single qubit case the unital subalgebras of the algebra $\mathcal{A} = \mathbb{M}_2$ can be easily classified. They are $\mathbb{M}_2$, $\mathbb{C} \cdot \mathbb{1}_2$ (the two trivial cases), and, up to unitary conjugation, Δ_2, the subalgebra of all diagonal matrices in $\mathbb{M}_2$. To be precise, this third case refers to the subalgebras $\mathcal{B}$ of the form $U^\dagger \Delta_2 U$, where $U \in \mathcal{A}$ is unitary.

Theorem 3 *Let $\mathcal{E} : \mathbb{M}_2 \to \mathbb{M}_2$ be a unital qubit channel, with T the mapping induced by $\mathcal{E}$ as in equation (6). Then there are three possibilities for a private quantum channel $[\mathcal{S}, \mathcal{E}, \frac{1}{2}\mathbb{1}]$ with $\mathcal{S}$ nonempty:*

1. *If the nullspace of T is 1-dimensional, then $\mathcal{S}$ consists of a pair of orthonormal states.*
2. *If the nullspace of T is 2-dimensional, then the set $\mathcal{S}$ is the set of all trace vectors of the subalgebra $U^\dagger \Delta_2 U$ of 2×2 diagonal matrices up to a unitary equivalence.*
3. *If the nullspace of T is 3-dimensional, then $\mathcal{E}$ is the completely depolarizing channel and $\mathcal{S}$ is the set of all unit vectors. In other words, $\mathcal{S}$ is the set of all trace vectors of $\mathbb{C} \cdot \mathbb{1}_2$.*

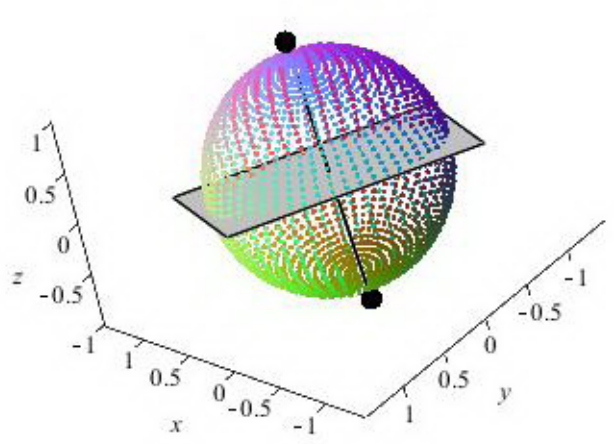

Fig. 1. Case (1)

Proof: We shall write $\vec{r}_\phi$ for the Bloch sphere vector representation of a single qubit state $|\phi\rangle$. It is clear from equation (6) that $\mathcal{E}(|\phi\rangle\langle\phi|) = \frac{1}{2}\mathbb{1}$ if and only if $T\vec{r}_\phi = 0$. Hence the relevant set that yields private states here is the intersection of the nullspace of T and the surface of the Bloch sphere.

Case (1): The nullspace of T is 1-dimensional. In this case, the nullspace is a single line through the origin of the Bloch sphere and the range of T is a plane through the origin. Obviously this line meets the surface of the Bloch sphere in two antipodal points. These two antipodal points correspond to a pair of orthonormal single qubit states. Figure 1 gives an example.

Case (2): The nullspace of T is 2-dimensional. In this case, the nullspace is a plane through the origin of the Bloch sphere. This plane meets the surface of the sphere in a great circle.

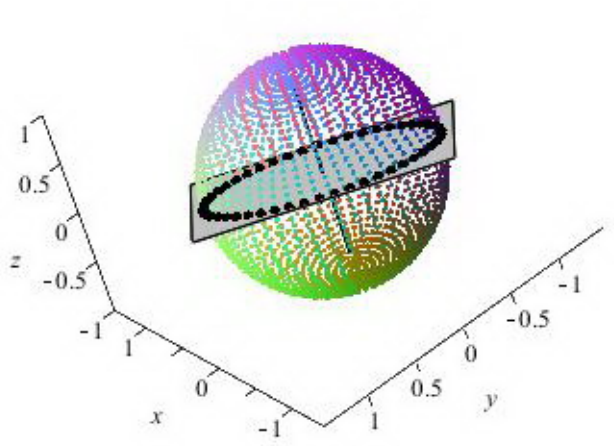

Fig. 2. Case (2)

The pure states corresponding to the points on this circle are precisely the private states for the channel. See an illustration in Figure 2.

To see how these private states arise from the trace vector perspective, let us consider the action of the channel more directly. As the nullspace of T is 2-dimensional, its range is a line through the origin. For simplicity we shall assume this line is the z-axis; other cases are unitarily equivalent to this case. Thus, the range of T intersects the sphere in the north and south poles, corresponding to the pure states $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ respectively. The action of T here will be a possible rotation of the Bloch sphere followed by a projection of the sphere onto the z-axis, followed by a possible contraction. By unitary equivalence, we only need consider the case where there is no initial rotation of the Bloch sphere. In terms of the Pauli matrices $\sigma_x, \sigma_y, \sigma_z$, this means the action of the channel is given by $\mathcal{E}(\sigma_x) = 0$, $\mathcal{E}(\sigma_y) = 0$ and $\mathcal{E}(\sigma_z) = p\sigma_z$ for some $0 < p \leq 1$.

Now Δ_2 is the algebra of all diagonal matrices with respect to the ordered basis $\{|0\rangle, |1\rangle\}$; explicitly, Δ_2 is the set of all operators of the form $a|0\rangle\langle 0| + b|1\rangle\langle 1|$ for arbitrary scalars a, b. Then the projection onto the z-axis is a conditional expectation onto the subalgebra Δ_2; call it $\mathcal{E}_\Delta$. Explicitly,

$$\mathcal{E}_\Delta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}, \text{ for any matrix } \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

One can check directly that $\mathcal{E} = p\mathcal{E}_\Delta + (1-p)\mathcal{E}_{\mathbb{C}}$, where $\mathcal{E}_{\mathbb{C}}$ is the completely depolarizing channel.

As $\mathcal{E}_{\mathbb{C}}$ adds no restrictions to the private states for $\mathcal{E}$, it suffices to show that the trace vectors for Δ_2 are precisely the pure states that lie on the equator of the Bloch sphere. But the equator states are precisely the states that satisfy $|\langle\phi||0\rangle| = \frac{1}{\sqrt{2}} = |\langle\phi||1\rangle|$. And it is easy to see that these are the states which do indeed satisfy the trace vector condition for the algebra Δ_2.

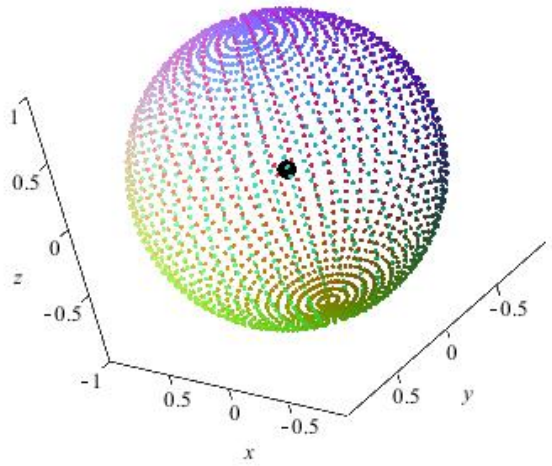

Fig. 3. Case (3)

Case (3): The nullspace of T is 3-dimensional, in other words T is the zero operator. In this case T maps the entire Bloch sphere to its origin, which corresponds to the maximally mixed state $\frac{1}{2}\mathbb{1}$, as shown in Figure 3. It is clear in this case that $\mathcal{E}$ is the completely depolarizing channel $\mathcal{E}_{\mathbb{C}}$. Moreover, the set $\mathcal{S}$ has no restrictions; that is, $\mathcal{S}$ is the set of all unit vectors. In other words, $\mathcal{S}$ is the set of all trace vectors of $\mathbb{C} \cdot \mathbb{1}_2$. □

5 Private States for Conditional Expectation Channels

The following result clarifies the general connection between conditional expectation channels, trace vectors and private states.

Theorem 4 *Let $\mathcal{E} : \mathbb{M}_n \to \mathcal{A}$ be a conditional expectation channel. Then $[\mathcal{S}, \mathcal{E}, \rho_0]$ is a private quantum channel if and only if $\mathcal{S}$ is a set of trace vectors of $\mathcal{A}$ with respect to $\rho_0 \in \mathcal{A}$.*

Proof: Let us first assume that $[\mathcal{S}, \mathcal{E}, \rho_0]$ is a PQC. Then $\mathcal{E}(|v\rangle\langle v|) = \rho_0$ for all $|v\rangle \in \mathcal{S}$, and in particular note that ρ_0 belongs to $\mathcal{A}$. Thus for all $|v\rangle \in \mathcal{S}$ and for all $a \in \mathcal{A}$, we have

$$\begin{aligned} \langle v|a|v\rangle &= \mathrm{Tr}(|v\rangle\langle v|a) \\ &= \mathrm{Tr}(\mathcal{E}(|v\rangle\langle v|a)) \\ &= \mathrm{Tr}(\mathcal{E}(|v\rangle\langle v|)a) = \mathrm{Tr}(\rho_0 a), \end{aligned}$$

where the second and third identities follow from the trace preservation and conditional expectation properties of $\mathcal{E}$ respectively. It follows that the states of $\mathcal{S}$ are trace vectors of $\mathcal{A}$ with respect to ρ_0.

For the converse, observe that when the vector states of $\mathcal{S}$ are trace vectors of $\mathcal{A}$ with respect to ρ_0, a similar calculation shows for all $|v\rangle \in \mathcal{S}$ and for all $a \in \mathcal{A}$ that

$$\begin{aligned} \mathrm{Tr}(\rho_0 a) &= \langle v|a|v\rangle \\ &= \mathrm{Tr}(|v\rangle\langle v|a) \\ &= \mathrm{Tr}(\mathcal{E}(|v\rangle\langle v|a)) = \mathrm{Tr}(\mathcal{E}(|v\rangle\langle v|)a). \end{aligned}$$

As ρ_0 belongs to $\mathcal{A}$, it follows that $[\mathcal{S}, \mathcal{E}, \rho_0]$ forms a private quantum channel. □

Example 5 *Of course the three cases of Theorem 3 when applied to a unital single qubit conditional expectation channel $\mathcal{E}_\mathcal{A} : \mathbb{M}_2 \to \mathcal{A}$ are covered by this theorem. Indeed, applying Theorem 4 to $\mathcal{E}_\mathcal{A}$ and letting $\rho_0 = \frac{1}{2}\mathbb{1}$ yields $[\mathcal{S}, \mathcal{E}_\mathcal{A}, \frac{1}{2}\mathbb{1}]$ is a PQC if and only if $\mathcal{A} = U^\dagger \Delta_2 U$ or $\mathcal{A} = \mathbb{C} \cdot \mathbb{1}_2$ and $\mathcal{S}$ is a set of trace vectors of $\mathcal{A}$. Case 1 of Theorem 3 is an example of when $\mathcal{S}$ is a proper subset of the set of all trace vectors of $U^\dagger \Delta_2 U$, whereas Case 2 occurs when $\mathcal{S}$ is the entire set. Case 3 occurs when $\mathcal{S}$ is the set of all trace vectors of $\mathbb{C} \cdot \mathbb{1}_2$.*

Example 6 *Conditional expectations arise as the most basic non-trivial examples of private quantum communication using a private shared Cartesian frame [11]. Let $\mathcal{H} = (\mathbb{C}^2)^{\otimes N}$, and for simplicity suppose N is even. Decompose the space as*

$$(\mathbb{C}^2)^{\otimes N} = \bigoplus_{j=0}^{N/2} \mathbb{H}_j \otimes \mathbb{K}_j,$$

where the special unitary group $\mathrm{SU}(2)$ acts irreducibly on $\mathbb{H}_j$ and trivially on $\mathbb{K}_j$. As formulated in [11], if Alice and Bob share a reference frame to which Eve does not have access, and Alice prepares N qubits in a state ρ and sends them to Bob, Eve will see the resulting state simply as a mixture of all rotations $\Omega \in \mathrm{SU}(2)$. This situation can be summed up with the channel $\mathcal{E}$, defined by

$$\mathcal{E}(\rho) = \sum_{j=0}^{N/2} (\mathcal{E}_{\mathbb{C}j} \otimes id_{\mathbb{K}_j})(\Pi_j \rho \Pi_j),$$

where $\mathcal{E}_{\mathbb{C}j}$ is the completely depolarizing channel on $\mathbb{H}_j$ and Π_j is the projection onto $\mathbb{H}_j$. One can see immediately that $\mathcal{E}$ is in fact a conditional expectation channel that maps onto the algebra $\oplus_j (\mathbb{1}_{\mathbb{H}_j} \otimes \mathcal{L}(\mathbb{K}_j))$. Thus, as noted in Theorem 4, private states for $\mathcal{E}$ can be found using trace vectors, which in this case can be constructed on the summands of the direct sum in a manner analogous to Example 1.

6 Outlook

We see two main potential outcomes of the present work. Firstly, it is clear even just from the examples we have discussed here that there are numerous conditional expectation channels of relevance in quantum information, though they have not been viewed from this perspective before. It should be possible to use the conditional expectation and trace vector machinery to construct other new and useful examples of private quantum channels. Secondly, this

work raises the intriguing possibility that a much more extensive theory of private quantum channels and private states could be developed. With few exceptions, the work on private channels appearing in the literature has focused primarily on specific instances and channels, rather than an overarching theory. We intend to continue these investigations elsewhere.

Acknowledgements

We are grateful to Aron Pasieka for assistance with the Bloch sphere figures. D.W.K. was supported by Ontario Early Researcher Award 048142, NSERC Discovery Grant 400160 and NSERC Discovery Accelerator Supplement 400233. R.P. was supported by NSERC Discovery Grant 400096. S.P. was supported by an NSERC doctoral scholarship.

References

1. A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf (2000), *Private quantum channels,* IEEE Symposium on Foundations of Computer Science (FOCS), pp. 547-553.
2. H. Umegaki (1954), *Conditional expectation in an operator algebra,* Tohoku Math. J. II, vol. 6, pp. 177-181.
3. F. J. Murray and J. von Neumann (1937), *On rings of operators. II,* Trans. Amer. Math. Soc., vol. 41, pp. 208-248.
4. K. Davidson (1996), *C^*-algebras by example,* Fields Institute Monographs, 6. American Mathematical Society (Providence, RI).
5. R. Pereira (2003), *Trace vectors in matrix analysis.* PhD dissertation, p. 36.
6. L. Ge (2003), *On "Problems on von Neumann algebras by R. Kadison, 1967",* Acta Math. Sinica, English Series, vol. 19, no. 3, pp. 619-624.
7. M. Nielsen and I. Chuang (2000), *Quantum computation and quantum information,* Cambridge Univ. Press (New York).
8. J. Bouda and M. Ziman (2007), *Optimality of private quantum channels,* J. Phys. A: Math. Theor., vol. 40, pp. 5415-5426.
9. L. Landau and R. Streater (1993), *On Birkhoff's theorem for doubly stochastic completely positive maps of matrix algebras,* Linear Algebra Appl, vol. 193, pp. 107-127.
10. C. King and M. B. Ruskai (2001), *Minimal entropy of states emerging from noisy quantum channels,* IEEE Trans. on Inform. Theory, vol. 47, issue 1, pp. 192-209.
11. S. Bartlett, P. Hayden, and R. Spekkens (2005), *Random subspaces for encryption based on private shared cartesian frame.* Phys. Rev. A, vol. 72, 052329.