A Domain of Unital Channels

Johnny Feng*

Naval Research Laboratory / Tulane University

Abstract

The common practice of slightly rewording the first paragraph or two of the introduction and calling it an abstract has always seemed a colossal waste of space to the author. Here, we will try to be as brief and to the point as possible. In this paper we prove the space of unital qubit channels is a Scott domain. We also provide a simple protocol to achieve Holevo capacity for these channels.

1 Intro

Domain theoretic techniques have been put to surprising use by Keye Martin in quantum information theory, showing how to find the optimal time to measure in Grover's algorithm [11], and deriving entropy as the least fixed point of a Scott continuous operator [12]. The discovery of the spectral order by Coecke and Martin [3] showed that the connection with domain theory is even deeper, by proving that the space of quantum states actually forms a domain. In [13] Martin analyzes qubit channels as self-maps on Ω^2 , the domain of two-level quantum states, and proves that Holevo capacity can be calculated from the informatic derivative.

In this paper, we more thoroughly examine the space of qubit channels. We completely characterize the Scott continuous qubit channels, complementing a result of Martin's [13]. We then explore the order on qubit channels given pointwise by the spectral order on Ω^2 . We prove that the unital qubit channels in this order form a Scott domain on their own right. Holevo capacity turns out to be a domain theoretic measurement, and we find the natural measurement, which allows us to calculate the unique channel with greatest capacity above any non-trivial unital channel.

In order to do this, we start by explicitly defining the decomposition of channels described by King and Ruskai in [9], based on the singular value decomposition. Along the way, we use it to provide a simple and experimentally realizable protocol that achieves Holevo capacity for any unital channel.

The proofs, which are in the final version, are omitted in this short version.

^{*} johnny.feng@nrl.navy.mil

2 **Qubit Channels and the Bloch Representation**

First we make sure we are all on the same page with terminology. Let \mathcal{H}^2 be a twodimensional complex Hilbert space. We denote the inner product by $\langle \cdot | \cdot \rangle$, and denote the trace of a matrix ρ by Tr ρ .

Definition 2.1. A quantum state is a self-adjoint, positive semidefinite operator $\rho : \mathcal{H}^2 \to \mathcal{H}^2$ with $\operatorname{Tr} \rho = 1$. If the eigenvalues of ρ are $\{0, 1\}$ we call ρ a pure state, or a qubit. We denote the set of all quantum states as Ω^2 .

Definition 2.2. Let $\rho \in \Omega^2$, and suppose $\sum p_i \rho_i = \rho$ for a finite collection of $\rho_i \in \Omega^2$, where $p_i \in [0, 1]$ and $\sum p_i = 1$. Then we call $\sum_i p_i \rho_i$ an **ensemble** for ρ .

Definition 2.3. A qubit channel is a completely positive, trace preserving map $\varepsilon : \Omega^2 \to \Omega^2$. If $\varepsilon(I/2) = I/2$, then ε is unital.

The qubit channels are closed under composition and convex sum, that is, if $\varepsilon_1, \varepsilon_2$ are channels, then so are $\varepsilon_1 \circ \varepsilon_2$ and $p\varepsilon_1 + (1-p)\varepsilon_2$ for any $p \in [0,1]$.

Throughout the paper, we will be using the Bloch representation of quantum states and qubit channels. This representation comes from the fact that every quantum state can be written uniquely as

$$\rho = \frac{1}{2}I + \frac{1}{2}(r_x\sigma_x + r_y\sigma_y + r_z\sigma_z)$$

where $r_x^2 + r_y^2 + r_z^2 \le 1$ and $\sigma_x, \sigma_y, \sigma_z$ are the Pauli spin matrices. The vector (r_x, r_y, r_z) in the unit ball \mathbb{B}^3 is called the **Bloch vector** associated with ρ . Conversely, every vector in the unit ball maps in this way to a quantum state. We call \mathbb{B}^3 the **Bloch ball**.

Every qubit channel $\varepsilon : \Omega^2 \to \Omega^2$ induces a map $f_{\varepsilon} : \mathbb{B}^3 \to \mathbb{B}^3$, which is called the Bloch representation of ε . The following is proven in [14].

Proposition 2.4. Let f_{ε} be the map induced on the Bloch ball by a qubit channel ε . Then

- (1) f_{ε} is convex linear, i.e. $f_{\varepsilon}(px_1+(1-p)x_2) = pf_{\varepsilon}(x_1)+(1-p)f_{\varepsilon}(x_2)$ for $p \in [0,1]$, $x_1, x_2 \in \mathbb{B}^3$.
- (2) $f_{\varepsilon_1 \circ \varepsilon_2} = f_{\varepsilon_1} \circ f_{\varepsilon_2}$.
- (3) $f_{p\varepsilon_1+(1-p)\varepsilon_2} = pf_{\varepsilon_1} + (1-p)f_{\varepsilon_2}.$

From this, we see the Bloch representations of qubit channels are also closed under composition and convex sum. Further, since f_{ε} is convex linear it can be written as $f_{\varepsilon}(x) = Mx + b$ for some real 3×3 matrix $M \in M_3(\mathbb{R})$ and $b \in \mathbb{B}^3$. Since the state I/2 has Bloch vector 0, we see ε is unital iff $f_{\varepsilon}(0) = 0$, i.e. if b = 0. We denote the set of Bloch representations of qubit channels by Q and of unital channels by U.

3 Diagonalization of Unital Qubit Channels

It is known that the singular value decomposition can be used to diagonalize the Bloch representation of a unital qubit channel [2] [9]. First we describe this diagonalization precisely, and then we will use it throughout the next several sections to prove some interesting results.

For a given 3×3 real matrix M, the singular value decomposition allows us to decompose M as

$$M = \Theta_1 \Sigma \Theta_2$$

where $\Theta_1, \Theta_2 \in O(3)$, i.e. are 3×3 orthogonal matrices, and

$$\Sigma = \begin{pmatrix} \sigma_1 & 0 & 0\\ 0 & \sigma_2 & 0\\ 0 & 0 & \sigma_3 \end{pmatrix}$$

where $\sigma_1, \sigma_2, \sigma_3$ are the positive square roots of the eigenvalues of $M^t M$, called the *sin-gular values* of M.

This representation is not unique. The reader interested in the full characterization of different singular value decompositions can consult Theorem 3.1.1' of [8]. It is standard practice when using the singular value decomposition to assume the entries on the diagonal are in decreasing order, because if they are not we can simply swap rows of Θ_1 and columns of Θ_2 until they are. We will make this assumption on Σ .

Since the only members of O(3) which are qubit channels are those in SO(3) we would like to modify Θ_1, Θ_2 to be in SO(3). We do this by checking the determinants and multiplying by -1 when necessary. If det $\Theta_1 = -1$, then we multiply Θ_1 and Σ by -1, and if det $\Theta_2 = -1$, then we multiply Θ_2 and Σ by -1. Let

$$R_1 = \det(\Theta_1)\Theta_1, \quad R_2 = \det(\Theta_2)\Theta_2, \quad D = \det(\Theta_1)\det(\Theta_2)\Sigma$$

to get

$$M = R_1 D R_2.$$

Now it is easy to see the following:

Proposition 3.1. Let M be a 3×3 real matrix. Then M can be decomposed as $M = R_1DR_2$, where $R_1, R_2 \in SO(3)$ and D is a diagonal matrix with either all nonnegative entries in decreasing order or all nonpositive entries in increasing order. Furthermore, M is a qubit channel iff D is a qubit channel.

We can do the same thing with the Bloch representation of an arbitrary qubit channel.

Corollary 3.2. Let M be a 3×3 real matrix and $b \in \mathbb{R}^3$, and let fx = Mx + b. Then $f = R_1 \circ \Delta \circ R_2$, where $\Delta x = Dx + R_1^{-1}b$, with $M = R_1DR_2$ as in Proposition 3.1. We call $f = R_1 \circ \Delta \circ R_2$ a spin diagonalization of f. Furthermore, f is a qubit channel iff Δ is a qubit channel.

Now, given an arbitrary 3×3 matrix M we would like to be able to identify when it is the Bloch representation of a channel. Conditions are known for when M is a diagonal matrix [9], a clear and elementary proof of which is given in [14].

Proposition 3.3. A diagonal matrix

$$D = \begin{pmatrix} d_1 & 0 & 0\\ 0 & d_2 & 0\\ 0 & 0 & d_3 \end{pmatrix}$$

is the Bloch representation of a unital qubit channel iff the following four inequalities are satisfied:

- (1) $1 + d_1 + d_2 + d_3 \ge 0$
- (2) $1 + d_1 d_2 d_3 \ge 0$
- (3) $1 d_1 + d_2 d_3 \ge 0$
- (4) $1 d_1 d_2 + d_3 \ge 0$

This allows us to test if an arbitrary matrix is a channel.

Corollary 3.4. Let M be a 3×3 real matrix, and let $M = R_1 D R_2$,

$$D = \begin{pmatrix} d_1 & 0 & 0\\ 0 & d_2 & 0\\ 0 & 0 & d_3 \end{pmatrix}$$

be a spin diagonalization of M. Then M is the Bloch representation of a unital channel iff

$$\min\{1 - d_1 - d_2 + d_3, 1 + d_1 + d_2 + d_3\} \ge 0.$$

4 A Protocol to Achieve Holevo Capacity

One of the remarkable things about unital channels is that very hard problems, such as calculating capacity and devising methods to send information at capacity, can be solved.

The Holevo capacity of a channel tells us how much classical information we can transmit through a quantum channel. If the signal states are not entangled across multiple uses of the channel, we have the following theorem, proven in [7]

Theorem 4.1. *The Holevo capacity of a channel* $f \in Q$ *is given by*

$$C(f) = \max_{p_i,\rho_i} \left\{ H(f(\rho)) - \sum_i p_i H(f(\rho_i)) \right\}$$

over all ensembles $\sum_{i} p_i \rho_i = \rho$, where $H(\rho) = -\text{Tr}\rho \log \rho$ is Von Neumann entropy.

It is known that for unital qubit channels that there is a simple formula for the Holevo capacity [5][9][13].

Theorem 4.2. *The Holevo capacity of a unital qubit channel* $f \in U$ *is given by*

$$C(f) = \log 2 - h\left(\frac{1 + \|f\|}{2}\right)$$

where ||f|| is the spectral norm and $h(x) = -x \log x - (1-x) \log(1-x)$ is Shannon entropy.

52

A serious drawback in the proofs of Theorem 4.2 is that they are non-constructive, hence even though we know there is some optimal input ensemble, we do not in general know what that ensemble is. To make things worse, even if we are given an ensemble that achieves capacity, we still have no idea what measurement to use to communicate at capacity. In the case of unital channels, however, the spin diagonalization shows us exactly what we should do.

- 1. Calculate a spin diagonalization of the channel, $f = R_1 D R_2$. Note that $R_2^{-1} e_1$ and $-R_2^{-1} e_1$ correspond to an orthogonal basis $\{|\Psi_0\rangle, |\Psi_1\rangle\}$, while $R_1 e_1$ and $-R_1 e_1$ correspond another orthogonal basis $\{|\Phi_0\rangle, |\Phi_1\rangle\}$.
- 2. Alice encodes "0" and "1" as $|\Psi_0\rangle$ and $|\Psi_1\rangle$ to send them through the channel.
- 3. Bob measures in the $\{|\Phi_0\rangle, |\Phi_1\rangle\}$ basis for each state received.

It is easy to show that this protocol describes a classical channel whose classical capacity is equal to the Holevo capacity.

5 Domain Theory

We review the basic definitions from domain theory [1] [6].

Definition 5.1. Let (P, \sqsubseteq) be a partially ordered set. A subset $C \subseteq P$ is **directed** if $\forall x, y \in C \exists z \in C$ such that $x, y \sqsubseteq z$. If the least upper bound for C exists, it is called the **supremum** of C and is denoted by $\sup C$. If every directed subset $C \subseteq P$ has a supremum, then P is called a **dcpo**.

We think of the order as an information order: $x \sqsubseteq y$ if the information in x is carried by y. Directed sets can intuitively be thought of as steps along a computation, and the supremum as the answer to which the computation converges. The definition of approximation we are about to make can be read as: x approximates y if any computation that gives us y has to compute x at some point along the way. Continuity means any piece of information can be completely recovered from the things that approximate it.

Definition 5.2. Let (D, \sqsubseteq) be a dcpo, and let $x, y \in D$. If for every directed set $C \subseteq D$ where $y \sqsubseteq \sup C$, we have $x \sqsubseteq c$ for some $c \in C$, then we say **x approximates y**, and we write $x \ll y$. For a point $x \in D$, if $\{y \in D | y \ll x\}$ is a directed set with supremum x we say D is continuous at x. If D is continuous for all $x \in D$ we call D a **domain**. If, in addition, any two elements with an upper bound have a supremum, we call D a **Scott domain**.

Example 5.3. One of the most basic examples of a domain is the closed interval [0,1] with the usual \leq order. All subsets of [0,1] are directed, and approximation is given by $x \ll y \Leftrightarrow x < y$. Given any two $x, y \in [0,1]$, $x, y \sqsubseteq \max\{x, y\}$, so it is in fact a Scott domain.

There are many ways to construct new domains from given ones, and we will be making use of one of these.

Definition 5.4. Let D_i be a collection of domains, where each D_i has a least element \perp_i . Then their **coalesced sum** $\prod \{D_i\}$ is the disjoint union of the D_i with the equivalence relation identifying all \perp_i 's.

The coalesced sum simply joins domains together by their least elements. The coalesced sum of (Scott) domains is a (Scott) domain.

Example 5.5. The coalesced sum of arbitrarily many copies of [0, 1] is a Scott domain.

Definition 5.6. Let $f : D \to E$ be a function between domains. f is called **monotone** if for every $x, y \in D$, if $x \sqsubseteq y$ then $f(x) \sqsubseteq f(y)$. f **preserves directed suprema** if for every directed $C \subseteq D$, $f(\sup C) = \sup f(C)$. If f is both monotone and preserves directed suprema, we say f is **Scott continuous**.

An important type of Scott continuous function is a measurement. The order tells us qualitatively when y is "better information" than x, but a measurement provides a quantitative idea of how much better [10].

Definition 5.7. Let $\mu : D \to E$ be a Scott continuous function between domains. For $\varepsilon \in E$, the set $\mu_{\varepsilon}(x) = \{y \sqsubseteq x | \epsilon \ll \mu y\}$ are called the ε -approximations of x. For a point $x \in D$, if given any $y \ll x$ we can find some ε such that y approximates everything in $\mu_{\varepsilon}(x)$, we say μ measures the content of x. If μ measures the content of ker $\mu = \{x \in D | \mu x \in \max E\}$, then we say μ is a measurement.

6 The Spectral Order

In [3] Bob Coecke and Keye Martin describe an order on quantum states called the *spectral order*, which makes the space of quantum states a Scott domain. This order extends to a pointwise order on quantum channels, which we will also call the *spectral order*. First, we define the Bayesian order on classical states.

Definition 6.1. Let $\Delta^2 = \{(p_1, p_2) \in [0, 1]^2 | p_1 + p_2 = 1\}$ be the classical 2-states. Then for $x, y \in \Delta^2$,

 $x \sqsubseteq_b y \equiv (y_1 \le x_1 \le 1/2)$ or $(1/2 \le x_1 \le y_1)$.

This is called the **Bayesian order** on Δ^2 .

Definition 6.2. A quantum observable is a self-adjoint linear operator $e : \mathcal{H}^2 \to \mathcal{H}^2$.

Given a quantum observable e, let λ_1 , λ_2 be its eigenvalues, with corresponding eigenvectors e_1 , e_2 , and let π_1 , π_2 be the projection operators onto their respective eigenspaces. Then quantum mechanics tells us that an experiment to measure the observable e on a system whose state is given by ρ will give the value λ_1 with probability $\text{Tr}(\pi_1(\rho))$ and value λ_2 with probability $\text{Tr}(\pi_2(\rho))$. We write

$$\operatorname{spec}(\rho|e) = (\operatorname{Tr}(\pi_1(\rho)), \operatorname{Tr}(\pi_2(\rho)))$$

and notice that if e has two distinct eigenspaces, $\operatorname{spec}(\rho|e) \in \Delta^2$. If the eigenspaces are distinct, then since $\operatorname{spec}(\rho|e)$ is independent of the eigenvalues, we relabel the eigenvalues as $\{1, 2\}$. Conversely, if the eigenvalues of e are $\{1, 2\}$, then e has two distinct eigenspaces.

A domain of unital channels

Definition 6.3. For $\rho, \sigma \in \Omega^2$,

 $\rho \sqsubseteq \sigma \equiv \exists$ an observable *e* such that spec $(\rho|e) \sqsubseteq_b$ spec $(\sigma|e)$

where the eigenvalues of e are $\{1, 2\}$ and e commutes with ρ, σ . This is called the **spectral** order on Ω^2 .

Theorem 6.4. Ω^2 with the spectral order is a Scott domain.

This was proven in [3]. As noted in [13], and can be shown as a corollary to Theorem 4.5 in [3], the order has a much nicer description in the Bloch formalism.

Proposition 6.5. For $x, y \in \mathbb{B}^3$

 $x \sqsubseteq y \Leftrightarrow \exists p \in [0, 1]$ such that x = py

where the order on \mathbb{B}^3 is the order induced by the spectral order on Ω^2 .

7 Scott Continuous Channels

In [13] Martin proves that the unital channels are exactly the Scott continuous channels with a lower set of fixed points. Here we characterize all Scott continuous channels.

Theorem 7.1. $f \in Q$ is Scott continuous iff it is unital or constant.

Geometrically it is easy to see why this is true. Given any channel fx = Mx + b, the image of M is symmetric about the origin, and so the image of f is symmetric about b. If we require f to be monotone, since f(0) = b, then the image of f must be contained in $\uparrow b$. If $b \neq 0$ then this is simply the radial line segment going from b to the boundary of \mathbb{B}^3 , and if b = 0 this is all of \mathbb{B}^3 . This, however, makes it impossible for the image of f to be symmetric about b unless b = 0 or the image of f consists solely of b.



Figure 1. I-III show the possible non-trivial images of f for $b \neq 0$, which are either ellipsoids, ellipses, or line segments centered at b. IV shows the upper set of b.

8 Domain of Unital Qubit Channels

Since a channel is a function over Ω^2 the spectral order extends to a pointwise order on channels. In the Bloch formulation, we define it as follows.

Definition 8.1. *For* $f, g \in Q$ *,*

$$f \sqsubseteq g \equiv \forall x \in \mathbb{B}^3, \ fx \sqsubseteq gx$$

This is called the **spectral order** *on* Q*.*

First we make the simple observation that composition on the left or right by rotations is order preserving.

Proposition 8.2. Let $f, g \in Q$, and $R \in SO(3)$. If $f \sqsubseteq g$ then $f \circ R \sqsubseteq g \circ R$ and $R \circ f \sqsubseteq R \circ g$.

In order to understand what this order looks like on unital channels, we start by examining it when one of the channels has a diagonal Bloch representation.

Proposition 8.3. Let

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix} \qquad N = \begin{pmatrix} n_{11} & 0 & 0 \\ 0 & n_{22} & 0 \\ 0 & 0 & n_{33} \end{pmatrix}$$

be 3×3 real matrices. If $M \subseteq N$ then $\exists p \in [0, 1]$ such that M = pN.

Now we are ready to characterize the order on all unital channels.

Corollary 8.4. Let $f, g \in U$. Then $f \sqsubseteq g \Leftrightarrow \exists p \in [0, 1]$ such that f = pg.

We will need to be able to identify the maximal elements of this order.

Proposition 8.5. Define the function $\mu : \mathcal{U} \to [0, 1]$ by

$$\mu f = \min\{1 - d_1 - d_2 + d_3, 1 + d_1 + d_2 + d_3\}$$

where

$$f = R_1 \begin{pmatrix} d_1 & 0 & 0\\ 0 & d_2 & 0\\ 0 & 0 & d_3 \end{pmatrix} R_2$$

is any spin diagonalization of f. Then $f \in \max(\mathcal{U})$ iff $\mu f = 0$. Furthermore, if $f \neq 0$ then $(1/(1 - \mu f))f$ is the maximal unital channel above f.

At last, we can see the following:

Corollary 8.6. $(\mathcal{U}, \sqsubseteq)$, the set of unital qubit channels with the spectral order, is a Scott domain.

56

9 Scott Continuous Operators and Measurements on Channels

A number of functions on channels turn out to be Scott Continuous on the domain of unital channels.

Proposition 9.1. The following functions are Scott continuous on U.

- (1) $\Phi(f) = f^t$
- (2) $\Phi(f) = pf + (1-p)f^t$ for $p \in [0,1]$
- (3) $\Phi(f) = D$, where $R_1 D R_2$ is any spin diagonalization of f, with $D \ge 0$ if det f = 0
- (4) $\Phi(f) = \begin{cases} 0 & \text{if } f = 0; \\ (1/(1-\mu f))f & \text{otherwise, with } \mu \text{ as defined in Proposition 8.5.} \end{cases}$
- (5) Holevo capacity
- (6) $\mu f = \min\{1 d_1 d_2 + d_3, 1 + d_1 + d_2 + d_3\}$

In the case of (5) and (6), these are, in fact, both measurements. The reader might recall that the function μ was used in Section 3 to characterize when a matrix represents a unital channel, and in Section 8 to find the maximal channel over a given channel. It is, in fact, the natural measurement on Ω^2 . In particular, ker $\mu = \max \mathcal{U}$.

We can restate the characterization in Section 3 as follows: if you extend μ to a function from $M_3(\mathbb{R}) \to \mathbb{R}$, then $\mu^{-1}([0,1])$ is the set of unital channels. So the space of unital channels is exactly captured by μ , its natural measurement.

10 Outro

The day is short and there is still much to do. In this paper, we focused on the unital qubit channels, a setting where a number of results work out very nicely. When we extend the order to all qubit channels, however, things are not as nice. In fact, capacity fails to be monotone in this order! [4]

There are many other orders that can be put on qubit channels, and this begs the question of whether we can find one for which qubit channels form a domain with capacity its natural measurement. In addition, the question of whether higher dimensional quantum channels possess domain theoretic structure remains open.

11 Acknowledgements

The author would like to thank Keye Martin for asking the question of whether unital channels formed a domain, and for being so excited when the answer turned out to be yes.

References

58

- S. Abramsky and A. Jung. Domain Theory. In S. Abramsky, D. Gabbay and T.S.E. Maibaum, Editors, Handbook of Logic in Computer Science vol. 3, Clarendon Press (1994).
- [2] P.S. Bourdon and H.T. Williams. Unital quantum operations on the Bloch ball and Bloch region, Physical Review A, Vol. 69, Article 022314, 2004.
- [3] B. Coecke, K. Martin. A Partial Order on Classical and Quantum States. Technical Report PRG-RR-02-07, Oxford University, 2002. http://web.comlab.ox.ac.uk/oucl/publications/tr/rr-02-07.html
- [4] J. Feng. A Domain of Quantum Channels. In preparation.
- [5] A. Fujivara and H. Nagaoka. Operational capacity and semi-classicality of quantum channels, IEEE Trans. Inform. Theory 44 (1998) 10711086.
- [6] G. Gierz, K.H. Hofmann, K. Keimel, J.D. Lawson, M. Mislove and D.S. Scott, Continuous Lattices and Domains, Cambridge Press (2003).
- [7] A. S. Holevo, The capacity of the quantum channel with general signal states, IEEE Trans. Info. Theory, vol. 44, pp. 269273, 1998.
- [8] R.A. Horn and C.R. Johnson, Topics in Matrix Analysis, Cambridge University Press, Cambridge, 1991.
- [9] C. King, M.B. Ruskai. Minimal entropy of states emerging from noisy quantum channels, IEEE Trans. Inform. Theory 47 (2001) 192209.
- [10] K. Martin. A foundation for computation. Ph.D. Thesis, Tulane University, Department of Mathematics (2000)
- K. Martin. Epistemic motion in quantum searching. Technical Report PRG-RR-03-06, Oxford University, 2003. http://web.comlab.ox.ac.uk/oucl/publications/tr/rr-03-06.html
- [12] K. Martin. Entropy as a fixed point. Theoretical Computer Science, 350(23):292324, 2006.
- [13] K. Martin. 2008. A Domain Theoretic Model of Qubit Channels. In Proceedings of the 35th international Colloquium on Automata, Languages and Programming, Part II (Reykjavik, Iceland, July 07 - 11, 2008). Lecture Notes In Computer Science, vol. 5126. Springer-Verlag, Berlin, Heidelberg, 283-297.
- [14] K. Martin. The scope of a quantum channel, Mathematical Structures in Computer Science, Cambridge University Press, to appear.