Naval Research Laboratory

Washington, DC 20375-5320

NRL/MR/5547--20-10,158

NISE Annual Report: Quantum Information in Dynamic Environments

Daniel Bonior

Center for High Assurance Computer Systems Branch
Information Technology Division

September 29, 2020

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

UNCLASSIFIED//DISTRIBUTION A

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
29-09-2020	NRL Memorandum Report	

4. TITLE AND SUBTITLE

NISE Annual Report: Quantum Information in Dynamic Environments

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Daniel Bonior

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
1X12

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Research Laboratory
4555 Overlook Avenue, SW
Washington, DC 20375-5320

8. PERFORMING ORGANIZATION REPORT NUMBER

NRL/MR/5547--20-10,158

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
One Liberty Center
875 N. Randolph Street, Suite 1425
Arlington, VA 22203-1995

10. SPONSOR / MONITOR'S ACRONYM(S)

ONR

11. SPONSOR / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this document is to report all findings and their significance in the NISE project "Quantum Information in Dynamic Environments".

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Daniel Bonior
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	Unclassified Unlimited	30	**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified Unlimited	Unclassified Unlimited	Unclassified Unlimited			(202) 404-1202

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

This page intentionally left blank.

Contents

EXECUTIVE SUMMARY E-1

1. BACKGROUND RESEARCH 1
   1.1 Quantum Information Theory 1
   1.2 Domain Theory 4

2. THE DOMAIN OF UNITAL CHANNELS 5
   2.1 A Partial Order on the Symmetric Unitals 5
   2.2 The Approximation Relation 9
   2.3 A Measurement on the Symmetric Unital Channels 16

3. DYNAMIC ENVIRONMENTS 19
   3.1 Environment Operators and their Algebraic Properties 19
   3.2 Security Implications 22

4. OPEN QUESTIONS AND FUTURE RESEARCH 25

ACKNOWLEDGMENTS 25

Bibliography 26

This page intentionally left blank.

EXECUTIVE SUMMARY

The purpose of this document is to report all findings and their significance in the NISE project "Quantum Information in Dynamic Environments".

This page intentionally left blank.

NISE ANNUAL REPORT: QUANTUM INFORMATION IN DYNAMIC ENVIRONMENTS

1. BACKGROUND RESEARCH

Currently, *quantum channels* are used to model the interaction between a system and a *static environment*, i.e. one that does not evolve over time. However, the assumption of a static environment is not always practical. In this paper we show that not only are dynamic environments abundant, but they can result in reductions to protocol efficiency and security. In hopes of eventually arriving at a method to mitigate such risks, we close by laying the foundations for studying the effects of a dynamic environment on a quantum system.

1.1 Quantum Information Theory

Throughout this paper we limit ourselves to two-level quantum systems, or qubits, and let $\mathscr{H}$ denote a two-dimensional Hilbert space.

Definition 1.1.1. *The state of a qubit is a self-adjoint, positive semi-definite, trace one, linear operator $\rho : \mathscr{H} \to \mathscr{H}$, which we call a density operator. The set of qubits is denoted by Ω.*

Standard computations show that the identity and spin operators,

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

form a linearly independent set of self-adjoint matrices. Since every two-level quantum state is a 2×2 self-adjoint matrix, it then follows that $\{I, \sigma_1, \sigma_2, \sigma_3\}$ forms a linear basis for the set of qubits. Thus, any two-level state can be uniquely written in the following form:

$$\rho = r_0 I + r_1 \sigma_1 + r_2 \sigma_2 + r_3 \sigma_3,$$

where r_0, r_1, r_2, and r_3 are real numbers. Because each ρ has unity trace and the spin operators are traceless, we are forced to conclude that $r_0 = \frac{1}{2}$. For brevity, it is common practice to factor $\frac{1}{2}$ out of each r_i, rename the result r_i, and let $\boldsymbol{\sigma} = [\sigma_1 \ \sigma_2 \ \sigma_3]^t$ be a vector of matrices. We then have that every state can be uniquely written as

$$\rho = \tfrac{1}{2}\big(I + \langle r, \boldsymbol{\sigma} \rangle\big),$$

where $\langle \cdot, \cdot \rangle$ is the standard Euclidean inner product and $r \in \mathbb{R}^3$ is called the *Bloch vector*. It can further be shown that ρ is positive-semidefinite if and only if $r \in \mathbb{B}^3$; where $||r|| = 1$ is equivalent to $\rho^2 = \rho$. Moreover, when using Bloch vectors, distinguishable states are given by antipodal points; i.e. x and $-x$ in $\mathbb{B}^3$. For this reason, we refer to a pair of antipodal points as a *communication basis* since they provide a means of representing binary classical information. The following definition results from a commonly cited list of assumptions whose justifications are outside the scope of this paper:

Manuscript approved September 27, 2020.

Definition 1.1.2. *A qubit channel is a completely positive, trace preserving, convex-linear map $\varepsilon : \Omega \to \Omega$.*

For a more detailed discussion on the assumptions of Definition 1.1.2, see [5]. In the same publication, the set of qubit channels are shown to be closed under composition and convex sums. Furthermore, every quantum channel ε induces a map f_ε on the Bloch vector. In particular,

$$\varepsilon\left(\frac{I+\langle r,\boldsymbol{\sigma}\rangle}{2}\right)=\frac{I+\langle f_\varepsilon(r),\boldsymbol{\sigma}\rangle}{2}.$$

Definition 1.1.3. *Each quantum channel f_ε is an affine map on the set of Bloch vectors $\mathbb{B}^3$. Furthermore, f_ε is linear if and only if $f_\varepsilon(I)=I$, in which case we say f_ε is unital.*

For the remainder of this paper we restrict ourselves to the set of unital channels, $\mathscr{U}$, as these channels ensure the entropy of the system is non-decreasing, and thus provide a conservative model for environmental noise as shown in [1]. We conclude our brief introduction to quantum information with the following results, which are also found in [1].

Theorem 1.1.4. *The set of unital qubit channels is a convex, compact set whose set of extreme points is $SO(3)$; i.e. $\mathscr{U}=\langle SO(3)\rangle$.*

Proposition 1.1.5. *Let f_ε be the Bloch representation of a qubit channel ε.*

(i) *The function f_ε is convex linear.*

(ii) *The composition of qubit channels corresponds to the composition of Bloch representations.*

(iii) *Convex sums of qubit channels correspond to convex sums of Bloch representations.*

Proposition 1.1.6. *A unital qubit channel f is symmetric if and only if it is a convex sum of involutive rotations that form a copy of the Klein four group. Explicitly,*

$$f=\sum_{i=0}^{4}p_i r^t s_i r,$$

where $p\in\Delta^4$, r is a member of $SO(3)$, and the s_i's are the Bloch representations of the identity and spin operators given by:

$$s_0=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\quad s_1=\begin{bmatrix}1&0&0\\0&-1&0\\0&0&-1\end{bmatrix}\quad s_2=\begin{bmatrix}-1&0&0\\0&1&0\\0&0&-1\end{bmatrix}\quad s_3=\begin{bmatrix}-1&0&0\\0&-1&0\\0&0&1\end{bmatrix}.$$

Note, Proposition 1.1.6 applies only to the set of symmetric unital channels, $\mathscr{U}_s$. While this restriction may appear arbitrary, $\mathscr{U}_s$ will be the subject of all results contained in this paper. Let us take a moment to explain why. Suppose one party, call them Alice, sends a qubit to another party, Bob, through the unital qubit channel f. As seen in [4], when using the Bloch representation, the probability of the state x resulting in some other state y, is given by

$$p(y|fx)=\frac{1+\langle y,fx\rangle}{2},$$

where $x, y \in S^2$. It then follows that the probability of receiving a flipped qubit, i.e. an error, is

$$p(-x|fx) = \frac{1 - \langle x, fx \rangle}{2}.$$

This, together with the following theorem shown in [4], we see that in the Bloch representation $p(-x|fx)$ can be calculated using a systematically constructed symmetric channel which we denote by $\varphi(f)$.

Theorem 1.1.7. *For any unital channel f,*

$$\langle x, fx \rangle = \langle x, \varphi(f)x \rangle,$$

where $\varphi(f) = \frac{1}{2}(f + f^t)$ and f^t is the transpose of f.

Proof. Since f is a matrix with real entries, then by the definition of adjoint we know that

$$\langle x, fx \rangle = \langle x, f^t x \rangle.$$

It then directly follows that

$$\begin{aligned} \langle x, fx \rangle &= \langle x, \tfrac{1}{2}(f+f)x \rangle \\ &= \tfrac{1}{2}\langle x, fx \rangle + \tfrac{1}{2}\langle x, fx \rangle \\ &= \tfrac{1}{2}\langle x, fx \rangle + \tfrac{1}{2}\langle x, f^t x \rangle \\ &= \langle x, \tfrac{1}{2}(f+f^t)x \rangle \\ &= \langle x, \varphi(f)x \rangle. \end{aligned}$$

Therefore, the probability of Bob receiving a flipped qubit due to the channel f is equal to that given by the symmetric channel $\varphi(f)$. □

In short, the probability of errors induced by any unital noise can be calculated using a symmetric channel. With this in mind, we restrict ourselves to the set of symmetric unital qubit channels, $\mathscr{U}_s$. Lastly, we have the following proposition which is a consequence of Proposition 1.1.6 and is proven in [1]:

Proposition 1.1.8. *Let λ be a diagonal matrix with entries λ_1, λ_2, and λ_3. Then λ is a unital channel if and only if the following inequalities are satisfied:*

(i) $(\forall i)\ \ 1 - |\lambda_i| \geq 0$

(ii) $1 + \lambda_1 + \lambda_2 + \lambda_3 \geq 0$

(iii) $1 + \lambda_1 - \lambda_2 - \lambda_3 \geq 0$

(iv) $1 - \lambda_1 + \lambda_2 - \lambda_3 \geq 0$

(v) $1 - \lambda_1 - \lambda_2 + \lambda_3 \geq 0$

1.2 Domain Theory

Definition 1.2.1. *Let X be an arbitrary set. A binary relation $\sqsubseteq$ is a subset of $X \times X$. We use the notation $x \sqsubseteq y$ to mean $(x,y) \in \sqsubseteq$ and call $(X, \sqsubseteq)$ a partially ordered set, or poset, if the following three properties hold for all $x,y,z \in X$:*

(i) $x \sqsubseteq x$.

(ii) *If $x \sqsubseteq y$ and $y \sqsubseteq z$, then $x \sqsubseteq z$.*

(iii) *If $x \sqsubseteq y$ and $y \sqsubseteq x$, then $x = y$.*

Definition 1.2.2. *Let $(X, \sqsubseteq)$ be a poset. For any subset $A \subseteq X$, if $y \sqsubseteq x$ for all $y \in A$, then x is called an upper bound of the set A. Furthermore, if $x \sqsubseteq z$ for any other upper bound z of A, then x is referred to as the supremum of A and is denoted by $sup(A)$, or $\bigsqcup A$.*

Definition 1.2.3. *Let x be an element in the poset $(X, \sqsubseteq)$. We say x is a maximal element of X if for all $y \in X$, $x \sqsubseteq y$ implies $x = y$. We denote the set of maximal elements for a set X by $max(X)$.*

Definition 1.2.4. *Let X be a poset. A nonempty subset $A \subseteq X$ is directed if for every $x,y \in A$ there exists $z \in X$ such that $x,y \sqsubseteq z$. If every directed subset of X has a supremum, then X is called a directed complete poset, or dcpo.*

Definition 1.2.5. *Let $(X, \sqsubseteq)$ be a dcpo with $x,y \in X$. If for every directed subset A where $y \sqsubseteq \bigsqcup A$, we have $x \sqsubseteq z$ for some $z \in A$, then we say that x approximates y, or $x \ll y$.*

Definition 1.2.6. *Let $(X, \sqsubseteq)$ be a dcpo.*
$\uparrow x \equiv \{y \in X \mid x \sqsubseteq y\}$ *(principal upper set of x).*
$\downarrow x \equiv \{y \in X \mid y \sqsubseteq x\}$ *(principal lower set of x).*
$\Uparrow x \equiv \{y \in X \mid x \ll y\}$ *(way above set of x).*
$\Downarrow x \equiv \{y \in X \mid y \ll x\}$ *(way below set of x).*

Definition 1.2.7. *Let $(X, \sqsubseteq)$ be a poset. We say that X is continuous at $x \in X$ if $\Downarrow x$ is directed with $\bigsqcup \Downarrow x = x$. If X is a dcpo that is continuous at all $x \in X$, then we call $(X, \sqsubseteq)$ a domain.*

Definition 1.2.8. *Let $\phi : X \to Y$ be a function between posets. Then ϕ is monotone if for all $x,y \in X$, $x \sqsubseteq y$ implies $\phi(x) \sqsubseteq \phi(y)$. Furthermore, we say a monotone function ϕ is strictly monotone if $\phi(x) = \phi(y)$ and $x \sqsubseteq y$ implies $x = y$. We say ϕ preserves suprema if for every directed subset $A \subseteq X$ such that $\bigsqcup A$ exists, then $\bigsqcup \phi(A)$ exists and $\bigsqcup \phi(A) = \phi(\bigsqcup A)$. A function is Scott continuous if it is monotone and preserves suprema.*

Definition 1.2.9. *Let X, Y be sets, each with its own binary relation. We then call an invertible function $\phi : X \to Y$ an order isomorphism if both it and its inverse are monotone.*

Definition 1.2.10. *Let $\mu : X \to Y$ be a Scott continuous function between domains. Then the ε-approximations of x are given by $\mu_\varepsilon(x) = \{y \sqsubseteq x \mid \varepsilon \ll \mu y\}$ where $\varepsilon \in Y$. If $y \ll x$ and we can find some ε such that $z \in \mu_\varepsilon(x)$ implies $y \ll z$, then we say μ measures the content of x. If μ measures the content of $ker\mu = \{x \in X \mid \mu x \in \max Y\}$, then μ is a measurement.*

2. THE DOMAIN OF UNITAL CHANNELS

In this section we further our understanding of the set of symmetric unital qubit channels by studying its order theoretic structure under a physically meaningful partial order. The contents of this chapter come directly from the author's thesis [4].

2.1 A Partial Order on the Symmetric Unitals

We say that for any $f, g \in \mathscr{U}_s$

$$f \sqsubseteq g \quad \Longleftrightarrow \quad \langle x, \big[f-g\big]x\rangle \geq 0,$$

for all $x \in S^2$.

Recalling that the probability of error when sending a qubit through a channel is $p(-x|fx) = \frac{1}{2}\big(1 - \langle x, fx\rangle\big)$, it then follows that $f \sqsubseteq g$ if and only if $p(-x|fx) \leq p(-x|fx)$ for all $x \in S^2$. In other words, "*f is below g*" is equivalent to saying that "*f has a smaller probability of causing error than g for all representations of information*". For the sake of brevity we will in some cases denote $\langle x, \big[f-g\big]x\rangle \geq 0$ for all $x \in S^2$ with $f - g \geq 0$ and any ambiguity will be resolved by context.

Theorem 2.1.1. *The binary relation $\sqsubseteq$ is a partial order on the set of symmetric unital channels.*

Proof. For every symmetric unital channel f

$$\langle x, \big[f-f\big]x\rangle = 0 \geq 0, \tag{1}$$

for all $x \in S^2$. Therefore, $\sqsubseteq$ is reflexive. Furthermore, if $f \sqsubseteq g$ and $g \sqsubseteq h$, then for all $x \in S^2$

$$\langle x, \big[f-h\big]x\rangle = \langle x, \big[f-g\big]x\rangle + \langle x, \big[g-h\big]x\rangle \geq 0. \tag{2}$$

Consequently, $\sqsubseteq$ is also transitive. Finally, we show that our order is antisymmetric by considering the case in which $f \sqsubseteq g$ and $g \sqsubseteq f$. Under this assumption,

$$\langle x, \big[f-g\big]x\rangle \leq 0 \leq \langle x, \big[f-g\big]x\rangle, \tag{3}$$

which is true if and only if

$$\langle x, \big[f-g\big]x\rangle = 0. \tag{4}$$

Then, we must have that $f - g$ is both symmetric and skew-symmetric. This directly implies that $f - g = 0$; or equivalently $f = g$. $\square$

With a partial order, let us take a moment to establish an order isomorphism which we will prove useful throughout the remainder of this paper.

Theorem 2.1.2. *Conjugation by a rotation is an order isomorphism on $(\mathscr{U}_s, \sqsubseteq)$.*

Proof. By definition of our order relation, $f \sqsubseteq g$ if and only if

$$\langle x, [f-g]x\rangle \geq 0 \tag{5}$$

for all $x \in S^2$. It then follows that since every $r \in SO(3)$ maps S^2 bijectively onto itself, f is below g if and only if

$$\langle r^t x, [f-g] r^t x \rangle \geq 0 \tag{6}$$

for all $x \in S^2$ and $r \in SO(3)$. Therefore, by the definition of an adjoint operator we have that $f \sqsubseteq g$ if and only if

$$\langle x, r[f-g] r^t x \rangle \geq 0; \tag{7}$$

or equivalently, $rfr^t \sqsubseteq rgr^t$. $\square$

In order to explore the order theoretic structure of $(\mathscr{U}_s, \sqsubseteq)$, we will first establish some of the more useful properties of each symmetric unital channel.

Properties of Symmetric Unital Channels

Theorem 2.1.3. *The identity matrix I is the least element in $(\mathscr{U}_s, \sqsubseteq)$.*

Proof. If f is a symmetric unital channel, then there exists some rotation r such that $f = r\lambda r^t$, where $\lambda \in \mathscr{U}_s$ is the diagonal matrix whose entries are the eigenvalues of f. It then follows from Proposition 1.1.8, that $\lambda_i \leq 1$ for all i. Note, it is well-documented in the literature that for any symmetric matrix A, the inner product $\langle x, Ax \rangle \leq \lambda_{max}$ for all $x \in S^2$, where λ_{max} is the largest eigenvalue of A. In other words,

$$\langle x, fx \rangle \leq \lambda_{max} \leq 1 \tag{8}$$

for all i and unit vectors x. Additionally, since $\langle x, Ix \rangle = 1$ for all $x \in S^2$, we have that

$$\langle x, \big[I - f\big] x \rangle = \langle x, Ix \rangle - \langle x, fx \rangle = 1 - \langle x, fx \rangle \geq 0. \tag{9}$$

$\square$

Theorem 2.1.4. *For every symmetric unital channel $f \neq I$, there exists a unique $p \in [0,1)$ and a unique $m \in \mathscr{U}_s$ with $tr(m) = -1$ such that $f = pI + (1-p)m$.*

Proof. Note that the identity can be written in this form where the choice of m does not matter and p is 1. If we assume $f \neq I$, then from Proposition 1.1.6 there exists some $r \in SO(3)$ and $q \in \Delta^4$ such that

$$f = \sum_{i=0}^{3} q_i r^t s_i r, \tag{10}$$

where the s_i's are the Bloch representations of the identity and spin channels. Therefore, we may write

$$f = q_0 I + (1-q_0) \sum_{i=1}^{3} \frac{q_i}{1-q_0} r^t s_i r. \tag{11}$$

Checking that the following coefficients sum to 1

$$\sum_{i=1}^{3} \frac{q_i}{1-q_0} = 1, \tag{12}$$

we then have that the summation on the righthand side of Eq. 11 is a convex sum. That is, our sum forms a symmetric unital channel with

$$\mathrm{tr}\left(\sum_{i=1}^{3}\frac{q_i}{1-q_0}r^t s_i r\right) = -\sum_{i=1}^{3}\frac{q_i}{1-q_0} = -1. \tag{13}$$

Letting $p = q_0$ and $m = \sum_{i=1}^{3}\frac{q_i}{1-q_0}r^t s_i r$, each symmetric unital channel f may then be written in the following form:

$$f = pI + (1-p)m, \tag{14}$$

where $p \in [0,1)$ and $m \in \mathscr{U}_s$ with $\mathrm{tr}(m) = -1$. To show the uniqueness of m and p, we assume there exist distinct pairs (m_1, p_1) and (m_2, p_2) that satisfy Eq. 14. Explicitly,

$$p_1 I + (1-p_1)m_1 = f = p_2 I + (1-p_2)m_2. \tag{15}$$

We then have that the following statements are equivalent:

$$\begin{aligned} \mathrm{tr}\big(p_1 I + (1-p_1)m_1\big) &= \mathrm{tr}\big(p_2 I + (1-p_2)m_2\big) \\ p_1\,\mathrm{tr}(I) + (1-p_1)\,\mathrm{tr}(m_1) &= p_2\,\mathrm{tr}(I) + (1-p_2)\,\mathrm{tr}(m_2) \\ 3p_1 - (1-p_1) &= 3p_2 - (1-p_2) \\ p_1 &= p_2. \end{aligned} \tag{16}$$

Therefore, p is unique. Renaming $p = p_1 = p_2$, we have from Eq. 15 that

$$(1-p)m_1 = (1-p)m_2. \tag{17}$$

Consequently, since $p_1 \in [0,1)$, we are left to conclude that $m_1 = m_2$, and therefore m is also unique. □

Corollary 2.1.5. *For every symmetric unital channel f:*

(i) $-1 \leq tr(f) \leq 3$.

(ii) *There exists a $g \in \mathscr{U}_s$ where $f \sqsubseteq g$ and $tr(g) = -1$.*

(iii) *f has a non-zero fixed point if and only if f is the identity or there exists a rotation r in $SO(3)$ such that $f = pI + (1-p)rs_1r^t$ for some unique $p \in [0,1)$.*

Proof.

(i) From Theorem 2.1.4 either $f = I$, in which case $\mathrm{tr}(f) = 3$ or $f = pI + (1-p)m$ where m has trace -1 and $p \in [0,1)$. In the latter case

$$\mathrm{tr}(f) = p\,\mathrm{tr}(I) + (1-p)\mathrm{tr}(m) = 3p - (1-p) = 4p - 1. \tag{18}$$

Therefore, we have that $-1 \leq \mathrm{tr}(f) \leq 3$ where the minimum and maximum values are obtained when $p = 0$ and $p = 1$, respectively.

(ii) Again writing $f = pI + (1-p)m$, if we let $g = m$, then

$$f - g = p(I - m) \geq 0, \tag{19}$$

where we used the fact that I is the least element, Theorem 2.1.3.

(iii) When $f = I$, our result is trivial as every point is fixed. Assuming $f \neq I$, then because f is non-expansive we have that for all $x \in S^2$

$$\begin{aligned} \langle x, fx \rangle &= ||x||\ ||fx|| \cos(\theta) \\ &= ||fx|| \cos(\theta) \leq ||x|| \cos(\theta) = \cos(\theta), \end{aligned} \tag{20}$$

where θ is the angle between the vectors x and fx. It then follows from Eq. 20 that there exists some $x \in S^2$ where $fx = x$ if and only if $\langle x, fx \rangle = 1$. Explicitly, f has a non-zero fixed point if and only if there exists some $x \in S^2$ such that

$$\begin{aligned} \langle x, fx \rangle &= p\langle x, Ix \rangle + (1-p)\langle x, mx \rangle \\ &= p + (1-p)\langle x, mx \rangle = 1. \end{aligned} \tag{21}$$

Thus, since $p \in [0,1)$, by basic arithmetic the following statements are equivalent:

$$\begin{aligned} p + (1-p)\ \langle x, mx \rangle &= 1 \\ (1-p)\ \langle x, mx \rangle &= 1 - p \\ \langle x, mx \rangle &= 1 \end{aligned} \tag{22}$$

Therefore, if a unital channel f has a non-zero fixed point, then $1 \in \sigma(m)$. Consequently, letting m have eigenvalues $\alpha_3 \leq \alpha_2 \leq \alpha_1$, we have that

$$\mathrm{tr}(m) = 1 + \alpha_2 + \alpha_3 = -1, \tag{23}$$

or equivalently, $\alpha_2 + \alpha_3 = -2$. It then follows that since the magnitude of each eigenvalue is less than or equal to 1, $\sigma(m) = \{1, -1, -1\}$. Then there exists a rotation r such that $r^t m r = s_1$; or equivalently, $m = r s_1 r^t$. $\square$

The set of trace -1 symmetric unital channels is not just of interest because it is present in the decomposition of each channel, Theorem 2.1.4. To this end we introduce the following lemma:

Lemma 2.1.6. *The trace function $tr : \mathscr{U}_s \to \mathbb{R}$ is strictly monotone, where the standard order on $\mathbb{R}$ is reversed. That is, for all $a, b \in \mathbb{R}$, we say $a \sqsubseteq b$ if $b \leq a$.*

Proof. If $f \sqsubseteq g$, then the smallest eigenvalue of $f - g$ is non-negative, i.e. $\mathrm{tr}(f-g) \geq 0$. With this in mind, it follows that

$$\mathrm{tr}(f - g) = \mathrm{tr}(f) - \mathrm{tr}(g) \geq 0. \tag{24}$$

Consequently, $\mathrm{tr}(f) \geq \mathrm{tr}(g)$, and we have that $\mathrm{tr}(f) \sqsubseteq \mathrm{tr}(g)$. Additionally, when $\mathrm{tr}(f) = \mathrm{tr}(g)$ and $f \sqsubseteq g$, we have that both $\mathrm{tr}(f-g) = 0$ and $f - g \geq 0$. Then the eigenvalues of $f - g$ are all non-negative and sum to 0. This occurs if and only if each eigenvalue itself is 0. Being symmetric, this is equivalent to $f - g = 0$. Consequently we are forced to conclude that the trace function is strictly monotone. $\square$

Theorem 2.1.7. *The set of maximal elements in $(\mathscr{U}_s, \sqsubseteq)$ is the set of channels with trace -1.*

Proof. Let f be a maximal element in $(\mathscr{U}_s, \sqsubseteq)$. By Corollary 2.1.5 there exists some symmetric unital channel g such that $\mathrm{tr}(g) = -1$ and $f \sqsubseteq g$. Since f is maximal, then $f = g$, and $\mathrm{tr}(f) = -1$.

Conversely, let $\mathrm{tr}(f) = -1$. If there exists some element $g \in \mathscr{U}_s$ where $f \sqsubseteq g$, then $\mathrm{tr}(g) \leq \mathrm{tr}(f) = -1$. However, from part (i) of Corollary 2.1.5, we know that $-1 \leq \mathrm{tr}(g) \leq 3$, and thus $\mathrm{tr}(g) = -1$. Finally, because the trace function is strictly monotone, as shown in Lemma 2.1.6, it follows that that $f = g$ and the proof is complete. □

With several properties for the elements of $\mathscr{U}_s$ established, we now turn our attention to the order theoretic structure of the poset $(\mathscr{U}_s, \sqsubseteq)$.

The Directed-Complete Poset of Symmetric Unital Channels

Theorem 2.1.8. *Let f be a symmetric unital channel. The principal lower and upper sets $\downarrow f$ and $\uparrow f$ are each closed in $(\mathscr{U}_s, \tau)$, where τ is the uniform metric topology.*

Proof. Let the principal lower set $\downarrow f$ contain the sequence (y_n) such that $y_n \to y$ in τ. Then since $y_n \in \downarrow f$, it follows that $y_n - f \geq 0$ for all n. Therefore, $\lim(y_n - f) = y - f \geq 0$. That is, $y \in \downarrow f$. Similarly, if (z_n) is some sequence in $\uparrow f$ such that $z_n \to z$ in τ, then $\lim(z_n - f) = z - f \leq 0$ and $z \in \uparrow f$. Moreover, since $(\mathscr{U}_s, \tau)$ is a metric space, every limit point is the limit of a sequence. Therefore, both $\downarrow f$ and $\uparrow f$ contain all their limit points and we have that the principal upper and lower sets are closed in $(\mathscr{U}_s, \tau)$. □

Theorem 2.1.9. *The partially ordered set $(\mathscr{U}_s, \sqsubseteq)$ is directed-complete.*

Proof. This proof directly follows from Theorem 2.1.8 and the results of "A new fixed point theorem in Domain Theory" by Martin and Feng [25]. In this paper, it is shown in Theorem 3.2 that every poset with a compact, Hausdorff topology in which the principal upper and lowers sets are closed, is a directed-complete partially ordered set and every filtered subset has an infimum. Therefore, since $\mathscr{U}_s$ is a closed subset of $\mathscr{U}$, we have that $(\mathscr{U}_s, \tau)$ is a compact metric space in which $\uparrow f$ and $\downarrow f$ are closed and the proof is complete. □

2.2 The Approximation Relation

We begin our efforts to find a approximation relation by making some initial observations about $(\mathscr{U}_s, \sqsubseteq)$. The following theorem is a direct result of the more generalized result by Martin and Panangaden in [2].

Theorem 2.2.1. *Every directed subset $A \subseteq \mathscr{U}_s$ contains a convergent cofinal net whose limit is $\bigsqcup A$ in the uniform metric topology τ.*

As every increasing sequence is a directed set, we immediately see that Theorem 2.2.1 applies to any increasing sequence in $\mathscr{U}_s$. Furthermore, we may assume that each convergent cofinal subnet is a convergent infinite subsequence. Consequently, we have the following corollary:

Corollary 2.2.2. *Every increasing sequence $g_n \in \mathscr{U}_s$ has a convergent infinite subsequence such that* $\lim(g_{n_k}) = \bigsqcup g_{n_k} = \bigsqcup g_n$.

Theorem 2.2.3. *Every increasing sequence $g_n \in \mathscr{U}_s$ has a limit given by its supremum, explicitly* $\lim(g_n) = \bigsqcup g_n$.

Proof. If (g_n) is an increasing sequence in $\mathscr{U}_s$, then by Corollary 2.2.2, we have that there exists a convergent infinite subsequence where $\lim(g_{n_k}) \to \bigsqcup g_n$. Furthermore, the proof of Theorem 2.2.1 in [2] implicitly shows that all convergent infinite subsequence of (g_n) have the same limit. Lastly, $\mathscr{U}_s$ is a compact Hausdorff space in the uniform metric topology. With all this in mind, we can invoke Lemma 3.1 in [20], where Martin shows that a sequence in a compact Hausdorff space converges if and only if all its convergent infinite subsequences converge to the same limit. Consequently, we have that $\lim(g_n) = \lim(g_{n_k}) = \bigsqcup g_n$. □

Theorem 2.2.4. *Let $[0,\infty)^*$ denote the set of non-negative real numbers with the reverse standard order. Then the map $\mu : \mathscr{U}_s \to [0,\infty)^*$ given by*

$$\mu(f) = \frac{1+tr(f)}{4} \tag{25}$$

is a strictly monotone, Scott continuous function.

Proof. We prove this result by first showing that μ is a monotone and strictly monotone map that preserves the supremum of every increasing sequence in $\mathscr{U}_s$, and then invoke part (ii) of Theorem 2.2.1 from [17] which shows that these conditions imply Scott continuity.

From Lemma 2.1.6, we know that the trace function $\mathrm{tr} : \mathscr{U}_s \to [0,\infty)^*$ is monotone and strictly monotone. The same is then true of μ, as it is simply $1+\mathrm{tr}$ divided by the constant 4. Furthermore, it then follows that

$$\begin{aligned} \mu(f) &= \tfrac{1}{4}\Big(1+\mathrm{tr}(f)\Big) \\ &= \tfrac{1}{4}\Big(1+\sum_{i=1}^{3} f_{ii}\Big) = \tfrac{1}{4}\Big(1+\sum_{i=1}^{3}\langle e_i, fe_i\rangle\Big), \end{aligned} \tag{26}$$

where for each $x \in S^2$ the inner product $\langle x, fx\rangle$ is a continuous function from $\mathscr{U}_s$ to $\mathbb{R}$. Consequently, μ is the sum of continuous functions, and is therefore also continuous. Considering an increasing sequence $g_n \in \mathscr{U}_s$, we have from Theorem 2.2.3 that the sequence is convergent with $\lim(g_n) = \bigsqcup g_n$. Thus, by the continuity of μ

$$\mu\big(\bigsqcup g_n\big) = \mu\big(\lim g_n\big) = \lim\big(\mu g_n\big). \tag{27}$$

And since μg_n is a bounded, monotone sequence in $\mathbb{R}$, it follows that $\lim\big(\mu g_n\big) = \bigsqcup(\mu g_n)$. Altogether we then have that

$$\mu\big(\bigsqcup g_n\big) = \lim\big(\mu g_n\big) = \bigsqcup \mu(g_n). \tag{28}$$

Thus we have shown that μ is a monotone and strictly monotone map that preserves the supremum of increasing sequences. Therefore, by [17], μ is a Scott continuous function. □

With the strictly monotone Scott continuous map μ, we have the following result which directly follows from Theorem 2.2.1 as shown by Martin in [17] and Theorems 2.2.3 and 2.2.4 of this section:

Corollary 2.2.5. *In the domain $(\mathscr{U}_s, \sqsubseteq)$ we may work with increasing sequences and their limits in lieu of the supremum of directed sets.*

Corollary 2.2.5 might be the most significant tool that will be utilized in this section as it allows us to work with sequences and their limits instead of directed sets. If this does not appear paramount, we implore the reader to attempt the remaining proofs of this paper using only directed sets. While this feat may be possible, doing so will leave one with a great appreciation for Martin's result. Let us now continue to further explore the structure of our partial order and ultimately characterize the approximation relation on the dcpo $(\mathscr{U}_s, \sqsubseteq)$. The following result is a direct result of part (iii) of Corollary 2.1.5.

Proposition 2.2.6. *Let f be a symmetric unital channel with a non-zero fixed point. Then the channel f has a degenerate eigenvalue.*

Proof. Let $f \in \mathscr{U}_s$ with eigenvalues $\lambda_1 \geq \lambda_2 \geq \lambda_3$. If $\lambda_1 = 1$, then from Proposition 1.1.8 we have that the following inequalities are true.

$$\lambda_2 - \lambda_3 \geq 0 \;\; \& \;\; \lambda_3 - \lambda_2 \geq 0.$$

This directly implies that $\lambda_2 = \lambda_3$ and the proof is complete. $\square$

Theorem 2.2.7. *Let f and g be symmetric unital channels. If $f \sqsubseteq g$ and g has a non-zero fixed point, then f is a convex sum of g and the identity.*

Proof. We begin by noting that when $g = I$, then because I is the least element $f \sqsubseteq g$ implies that $f = g$, and our result is immediate. The case where $f = I$ also follows trivially. Consequently, we will continue under the assumption that neither f or g are the identity. If g has a non-zero fixed point, then by Proposition 2.2.6 its spectrum is $\sigma(g) = \{1, \mu, \mu\}$, and from part (iii) of Corollary 2.1.5 there exists some $r \in SO(3)$ and $p \in [0,1)$ such that

$$g = pI + (1-p)rs_1r^t. \tag{29}$$

Furthermore, since conjugation by any rotation is an order isomorphism, as shown in Theorem 2.1.2, we may assume that g is diagonal. Explicitly, we may assume that

$$g = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \mu \end{bmatrix}. \tag{30}$$

It then follows from direct calculation that

$$\langle e_1, [f-g]e_1 \rangle = f_{11} - g_{11} = f_{11} - 1 \geq 0, \tag{31}$$

which is true if and only if $f_{11} \geq 1$. Moreover, since f is non-expansive $\big($i.e. $||fe_1|| \leq ||e_1||\big)$ we have that $fe_1 = e_1$. Note, this directly implies that $f_{21} = f_{31} = 0$, otherwise $fe_1 = [1, f_{21}, f_{31}]^t$ and $fe_1 \neq e_1$. Lastly, since f is symmetric, we are left to conclude that

$$f = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & b & c \end{bmatrix}. \tag{32}$$

Upon calculation, the eigenvalues of f are then

$$\begin{aligned} \lambda_1 &= 1, \\ \lambda_2 &= \tfrac{1}{2}\Big(a+c+\sqrt{(a-c)^2+4b^2}\Big), \\ \lambda_3 &= \tfrac{1}{2}\Big(a+c-\sqrt{(a-c)^2+4b^2}\Big). \end{aligned} \tag{33}$$

Again utilizing Proposition 2.2.6, since $1 \in \sigma(f)$ we know that $\lambda_2 = \lambda_3$. Then, setting $\lambda = \lambda_2 = \lambda_3$, the following statements are equivalent:

$$\begin{aligned} \tfrac{1}{2}\Big(a+c+\sqrt{(a-c)^2+4b^2}\Big) &= \tfrac{1}{2}\Big(a+c-\sqrt{(a-c)^2+4b^2}\Big) \\ \sqrt{(a-c)^2+4b^2} &= -\sqrt{(a-c)^2+4b^2} \\ \sqrt{(a-c)^2+4b^2} &= 0. \end{aligned} \tag{34}$$

Squaring both sides, we have that $(a-c)^2+4b^2 = 0$. Moreover, since $a,b,c \in \mathbb{R}$, it follows that that $(a-c)^2$ and $4b^2$ are both non-negative. Therefore, their sum is zero if and only if they are both zero. That is, $a = c$ and $b = 0$. We then finally have that

$$f = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}. \tag{35}$$

Lastly, since $f \sqsubseteq g$ $\big($i.e. $\langle x, [f-g]x\rangle \geq 0$ for all $x \in S^2\big)$, it follows that $1 \geq \lambda \geq \mu$. Thus, letting $p = \frac{\lambda-\mu}{1-\mu} \in [0,1]$, we have that $(1-p) = \frac{1-\lambda}{1-\mu}$ and

$$\begin{aligned} \lambda(1-\mu) &= \lambda(1-\mu)+\mu-\mu = \lambda-\mu+\mu-\lambda\mu \\ &= (\lambda-\mu)+(1-\lambda)\mu = (1-\mu)\big[p+(1-p)\mu\big]. \end{aligned} \tag{36}$$

Dividing each side by $(1-\mu)$, Eq. 36 then implies that $\lambda = p+(1-p)\mu$. Therefore,

$$\begin{aligned} f = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix} &= \begin{bmatrix} p+(1-p) & 0 & 0 \\ 0 & p+(1-p)\mu & 0 \\ 0 & 0 & p+(1-p)\mu \end{bmatrix} \\ = p\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + (1-p)\begin{bmatrix} 1 & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \mu \end{bmatrix} &= pI+(1-p)g. \end{aligned} \tag{37}$$

□

Corollary 2.2.8. *Let $f,g \in \mathscr{U}_s$. If $1 \in \sigma(g)$ and $f \sqsubseteq g$, then any matrix that diagonalizes g also diagonalizes f.*

Theorem 2.2.9. *The approximation relation for each symmetric unital channel $g \neq I$ is characterized as follows:*

(i) *If* $1 \notin \sigma(g)$, *then* $f \ll g \iff f - g > 0$,

(ii) *If* $1 \in \sigma(g)$, *then* $f \ll g \iff f \neq g$ *and* $f \sqsubseteq g$,

where $f - g > 0$ *denotes the condition that* $\langle x, [f-g]x\rangle > 0$ *for all* $x \in S^2$.

Proof.

(i) $1 \notin \sigma(g)$:
(⇐) Due to Corollary 2.2.5 instead of using directed subsets and their supremum we may work with the limits of increasing sequences. With this in mind, we consider an increasing sequence $(y_n) \to \lim(y_n)$, where $g \sqsubseteq \lim(y_n)$, and show that $f - g > 0$ implies that there exists some y_k such that $f \sqsubseteq y_k$, i.e. $f \ll g$. We begin by defining the function $\phi : \mathscr{U}_s \times S^2 \to \mathbb{R}$ where

$$\phi(g,x) = \langle x, [f-g]x\rangle. \tag{38}$$

Since ϕ is continuous by Corollary 2.10 in [3], the map $\underline{\phi} : \mathscr{U}_s \to \mathbb{R}$

$$\underline{\phi}(g) = \inf_{x \in S^2} \langle x, [f-g]x\rangle \tag{39}$$

is also continuous. Note, since S^2 is compact, we know that the infimum of $\langle x, [f-g]x\rangle$ is assumed by some $x \in S^2$. So if $f - g > 0$ and $g - \lim(y_n) \geq 0$, then

$$\begin{aligned} \langle x, [f - \lim(y_n)]x\rangle &= \langle x, [f - g + g - \lim(y_n)]x\rangle \\ &= \langle x, [f-g]x\rangle + \langle x, [g - \lim(y_n)]x\rangle > 0 \end{aligned} \tag{40}$$

for all $x \in S^2$. Then by the continuity of $\underline{\phi}$,

$$\lim\big(\underline{\phi}(y_n)\big) = \underline{\phi}\big(\lim(y_n)\big) > 0. \tag{41}$$

It then follows that $\underline{\phi}(y_n) > 0$ for most n. Thus, we have shown that $f - g > 0$ implies $f \ll g$.

(⇒) We begin by noting that if $f \ll g$, then for every increasing sequence (y_n) where $g \sqsubseteq \lim(y_n) = \bigsqcup y_n$, there exists some y_k such that $f \sqsubseteq y_k$. Letting $y_n = \frac{1}{n}I + (1 - \frac{1}{n})g$, we have

$$\begin{aligned} y_n - y_{n+1} &= \big(\tfrac{1}{n} - \tfrac{1}{n+1}\big)I + \big(1 - \tfrac{1}{n} - 1 + \tfrac{1}{n+1}\big)g \\ &= \big(\tfrac{1}{n} - \tfrac{1}{n+1}\big)I + \big(\tfrac{1}{n+1} - \tfrac{1}{n}\big)g = \big(\tfrac{1}{n} - \tfrac{1}{n+1}\big)(I - g) > 0, \end{aligned} \tag{42}$$

where the last inequality follows from the fact that $\langle x, gx\rangle < 1$, by assumption, while $\langle x, Ix\rangle = 1$, for all $x \in S^2$. Furthermore,

$$\begin{aligned} y_n - g &= \tfrac{1}{n}I + \big(1 - \tfrac{1}{n}\big)g - g \\ &= \tfrac{1}{n}I + \big(1 - \tfrac{1}{n} - 1\big)g = \tfrac{1}{n}(I - g) > 0, \end{aligned} \tag{43}$$

where the last inequality follows by the same arguments used in Inequality 42. In other words, (y_n) is an increasing sequence with $\bigsqcup y_n = \lim(y_n) = g$. Then since $f \ll g$, there exists some y_k where $f \sqsubseteq y_k$.

Consequently, we have

$$f-g=f-y_k+y_k-g=(f-y_k)+(y_k-g)>0, \tag{44}$$

where the last inequality is follows from the fact that $f-y_k\geq 0$ and $y_k-g>0$. Therefore, we have shown that if $1\notin\sigma(g)$, then $f\ll g$ if and only if $f-g>0$.

(ii) $\underline{1\in\sigma(g)}$:
We begin by noting that if $1\in\sigma(g)$, then there does not exist a $f\in\mathscr{U}_s$ where $f-g>0$. Otherwise, for the point x^* where $gx^*=x^*$, we would have that

$$\langle x^*,[f-g]x^*\rangle=\langle x^*,fx^*\rangle-1>0. \tag{45}$$

However, recalling Equation 20, which results from the fact that the unital channels are non-expansive, we have that $\langle x^*,fx^*\rangle\leq\cos(\theta)\leq 1$, where θ is the angle between the vectors x^* and fx^*. Therefore, we are left to conclude that $f-g\not>0$. With this in mind, it is clear that we need a different relation for the set of unital channels with non-zero fixed points. Otherwise, nothing would approximate these channels, which contradicts the fact that the least element I can be shown to approximate every channel.

$(\Leftarrow)$: We use some of the same arguments for this proof as those found in part (i). In particular, from Corollary 2.2.5 we can work with increasing sequences and their limits instead of supremum of directed subsets. With this in mind, we assume $f\sqsubseteq g$, $f\neq g$, and let (y_n) be an increasing sequence where $g\sqsubseteq\lim(y_n)=y$. We then arrive at one of two cases: $1\notin\sigma(y)$ or $1\in\sigma(y)$. We begin with the former.

(a) $\underline{1\notin\sigma(y)}$:
We remind the reader that we are now in the case where $1\in\sigma(g)$. Since conjugation by a rotation is an order isomorphism, we may consider the case where g is diagonal, in particular

$$g=\begin{bmatrix}1&0&0\\0&\mu&0\\0&0&\mu\end{bmatrix}. \tag{46}$$

Therefore, if $f\neq g$, and $f\sqsubseteq g$, we have by Corollary 2.2.8 that

$$f=\begin{bmatrix}1&0&0\\0&\lambda&0\\0&0&\lambda\end{bmatrix} \tag{47}$$

where $\lambda>\mu$. Since both $f-g$ and $g-y$ are greater than or equal to 0, we then have for all $x\in S^2$

$$\langle x,[f-y]x\rangle=\langle x,[f-g]x\rangle+\langle x,[g-y]x\rangle\geq 0, \tag{48}$$

where $\langle x,[f-y]x\rangle=0$ if and only if

$$\langle x,[f-g]x\rangle=\langle x,[g-y]x\rangle=0. \tag{49}$$

Then because g and f are diagonal matrices given by Equations 46 and 47 respectively and $\lambda>\mu$, it follows that

$$\langle x,\big[f-g\big]x\rangle=(x_2^2+x_3^2)(\lambda-\mu)=0 \tag{50}$$

if and only if $x = e_1$. However, since $ge_1 = e_1$ and $y_{11} = \langle e_1, ye_1 \rangle < 1$, it is also true that

$$\langle e_1, [g-y]e_1 \rangle = 1 - y_{11} \neq 0. \tag{51}$$

Consequently, there does not exist an $x \in S^2$ where $\langle x, [f-g]x \rangle = \langle x, [g-y]x \rangle = 0$, and we are left to conclude that $\langle x, [f-y]x \rangle > 0$ for all $x \in S^2$, i.e. $f - y = f - \lim(y_n) > 0$. We then have by the definition of $\underline{\phi}$ that

$$\underline{\phi}\big(\lim y_n\big) = \inf_{x \in S^2} \langle x, [f - \lim y_n]x \rangle > 0. \tag{52}$$

It then follows from the continuity of $\underline{\phi}$ that $\underline{\phi}\big(\lim y_n\big) = \lim \underline{\phi}(y_n) > 0$, and therefore, $f - y_n > 0$ for most n. Thus, when $1 \notin \sigma(y)$, we have that $f \ll g$.

(b) $\underline{1 \in \sigma(y)}$:
As this proof is long, we remind the reader once again that we are considering an increasing sequence $(y_n) \to y$ where $1 \in \sigma(g)$, $f \neq g$, $f \sqsubseteq g$, and $g \sqsubseteq \bigsqcup y_n = y$. Therefore, $f \sqsubseteq g \sqsubseteq y$ and $y_n \sqsubseteq y$. It then follows from Corollary 2.2.8 that if $1 \in \sigma(y)$, then any rotation r that diagonalizes y also diagonalizes f, g, and each y_n. Consequently, since conjugation by a rotation is an order isomorphism, we may assume

$$f = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}, \quad g = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \mu \end{bmatrix}, \quad y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{bmatrix}, \quad y_n = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha_n & 0 \\ 0 & 0 & \alpha_n \end{bmatrix}, \tag{53}$$

where $\alpha_n \to \alpha$. Furthermore, since $y_n \sqsubseteq y$ and $f \sqsubseteq g \sqsubseteq y$, we have that $\alpha_n \geq \alpha$ and $\lambda > \mu \geq \alpha$, where the strict inequality follows from the fact that $f \neq g$. It then follows that

$$\lambda - \alpha = \lambda - \lim(\alpha_n) = \lim(\lambda - \alpha_n) > 0, \tag{54}$$

and therefore, $\lambda - \alpha_n > 0$ for most n. Consequently, there exists some y_k such that $f \sqsubseteq y_k$, and we are left to conclude that $f \ll g$.

Thus far we have shown that when $1 \in \sigma(g)$, if $f \neq g$ and $f \sqsubseteq g$, then $f \ll g$.

($\Rightarrow$): Conversely, let $f \ll g$ and $1 \in \sigma(g)$. By the definition of approximation we immediately have that $f \sqsubseteq g$. Therefore, we need only show that $f \neq g$. With this in mind, we once again consider the sequence $y_n = \frac{1}{n}I + (1 - \frac{1}{n})g$. Furthermore, this sequence is increasing with $\lim(y_n) = \bigsqcup y_n = g$. Then since $f \ll g$, there exists some y_k such that $f \sqsubseteq y_k$. Moreoever, $f = g$ if and only if

$$f - g = \big(f - y_k\big) + \big(y_k - g\big) = 0, \tag{55}$$

where we know that $f - y_k \geq 0$ and $y_k - g \geq 0$. It then follows that $f = g$ if and only if $f = y_k$ and $g = y_k$. On the other hand,

$$\begin{aligned} y_k - g &= \tfrac{1}{k}I + \big(1 - \tfrac{1}{k}\big)g - g \\ &= \tfrac{1}{k}I + \big(1 - \tfrac{1}{k} - 1\big)g = \tfrac{1}{k}(I - g). \end{aligned} \tag{56}$$

Therefore, $g = y_k$ if and only if $g = I$. However, by assumption $g \neq I$, and it then follows that $f \neq g$.

Thus, when $1 \in \sigma(g)$, we have shown that $f \sqsubseteq g$ and $f \neq g$ if and only if $f \ll g$. $\square$

With an approximation relation established, we may now finally verify whether or not $(\mathscr{U}_s, \sqsubseteq)$ is a continuous dcpo. We start with the following lemma, whose proof is admitted as it is well-documented in the literature by Abramsky and Jung.

Lemma 2.2.10. *Let X be a dcpo. If $A \subseteq \downarrow x$ where A is a directed subset and $\bigsqcup A = x$, then $\downarrow x$ is directed with $\bigsqcup \downarrow x = x$.*

Theorem 2.2.11. *The set of symmetric unital channels is a continuous dcpo.*

Proof. Let $f = I$. Then $\downarrow f = \emptyset$ and the result follows trivially. Therefore, for the remainder of the proof we assume that $f \neq I$. Let (y_n) be a sequence of functions $y_n : \mathscr{U}_s \to \mathscr{U}_s$ where

$$y_n(f) = \tfrac{1}{n} I + \big(1 - \tfrac{1}{n}\big) f. \tag{57}$$

Then for every symmetric unital channel, $y_n(f)$ is a sequence in $\mathscr{U}_s$ that converges to f. In particular, since I is the least element and

$$\begin{aligned} y_n(f) - y_{n+1}(f) &= \tfrac{1}{n} I + \big(1 - \tfrac{1}{n}\big) f - \tfrac{1}{n+1} I - (1 - \tfrac{1}{n+1}) f \\ &= \big(\tfrac{1}{n} - \tfrac{1}{n+1}\big) I + \big(\tfrac{1}{n+1} - \tfrac{1}{n}\big) f \\ &= \big(\tfrac{1}{n} - \tfrac{1}{n+1}\big)(I - f), \end{aligned} \tag{58}$$

$y_n(f)$ is an increasing sequence for all $f \in \mathscr{U}_s$, and therefore, a directed set. Furthermore,

$$y_n(f) - f = \tfrac{1}{n} I + \big(1 - \tfrac{1}{n}\big) f - f = \tfrac{1}{n}(I - f). \tag{59}$$

Since $f \neq I$ by assumption, we then have that $f \neq y_n(f)$ for all n. Thus, when $1 \in \sigma(f)$, we have that $y_n(f) \neq f$ and $y_n(f) \sqsubseteq f$, which implies $y_n(f) \ll f$.

On the other hand, when $1 \notin \sigma(f)$, since $\langle x, [I - f]x\rangle > 0$ for all $x \in S^2$, it follows that $y_n(f) - f > 0$. Therefore, in either case $y_n(f) \ll f$ for all n. We then have by Theorem 2.2.3, that $\lim(y_n(f)) = \bigsqcup y_n(f) = f$, and we have thus shown that the sequence $(y_n(f))$ is a directed subset of $\downarrow f$ with $\bigsqcup y_n(f) = f$. It then follows from Lemma 2.2.10, that for all $f \in \mathscr{U}_s$, the way below set $\downarrow f$ is directed with supremum f. Thus, the dcpo $(\mathscr{U}_s, \sqsubseteq)$ is continuous. □

2.3 A Measurement on the Symmetric Unital Channels

Theorem 2.3.1. *The strictly monotone Scott continuous map $\mu : \mathscr{U}_s \to [0,\infty)^*$ given by*

$$\mu(f) = \frac{1 + tr(f)}{4} \tag{60}$$

measures all of $\mathscr{U}_s$.

Proof. Let $f, g \in \mathscr{U}_s$ where $f \ll g$. We prove that there exists an $\varepsilon \in [0,\infty)$ such that $f \in \mu_\varepsilon(f) \subseteq \uparrow g$. We will do so by considering two cases: $1 \in \sigma(f)$ and $1 \notin \sigma(f)$.

(i) $1 \in \sigma(f)$: We show that for all $g \in \downarrow f$, there exists an ε where $h \in \mu_\varepsilon(f) = \{h \sqsubseteq f \mid \varepsilon \ll \mu(h)\}$ implies that $g \ll h$. Since $1 \in \sigma(f)$ and $g, h \sqsubseteq f$, then because conjugation by a rotation is an order isomorphism, by Corollary 2.2.8 we may consider f, g, and h to be given by the following matrices:

$$f = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix}, \tag{61}$$

where $\lambda < \alpha$ and $\lambda \leq \beta$. The strict inequality follows from Theorem 2.2.9 where we have shown that $1 \in \sigma(f)$ and $g \ll f$ if and only if $g \sqsubseteq f$ and $g \neq f$. Then letting

$$\varepsilon = \frac{1+\alpha}{2}, \tag{62}$$

for any $h \in \mu_\varepsilon(f)$ we have that

$$\varepsilon = \frac{1+\alpha}{2} > \mu(h) = \frac{1+\mathrm{tr}(h)}{4} = \frac{1+\beta}{2}. \tag{63}$$

Consequently, $\alpha > \beta$, and it then follows that $g \sqsubseteq h$ and $g \neq h$. Thus, because $1 \in \sigma(h)$, we have again from Theorem 2.2.9 that $g \ll h$. Furthermore, since $\lambda < \alpha$, it follows that

$$\mu(f) = \frac{1+\lambda}{2} < \frac{1+\alpha}{2}. \tag{64}$$

Therefore, $\varepsilon > \mu(f)$, and we also have that $f \in \mu_\varepsilon(f)$. So we have shown that if $1 \in \sigma(f)$, then for each $g \in \downarrow f$, there exists an ε such that $f \in \mu_\varepsilon(f) \subseteq \uparrow g$.

(ii) $1 \notin \sigma(f)$: For this case we show that for all $g \in \downarrow f$, if

$$\varepsilon = \mu(f) + \tfrac{1}{4} \min_{x \in S^2} \langle x, [g-f]x \rangle, \tag{65}$$

then $f \in \mu_\varepsilon(f) \subseteq \uparrow g$. First off, because $\langle x, [g-f]x \rangle$ is continuous its minimum value is assumed by some point in the compact set S^2. Furthermore, since $g \ll f$ with $1 \notin \sigma(f)$, we have that $g - f > 0$, and thus $\min_{x \in S^2} \langle x, [g-f]x \rangle > 0$. It then follows that $\varepsilon > \mu(f)$ and therefore $f \in \mu_\varepsilon(f)$.

We begin by assuming $h \in \mu_\varepsilon(f)$, and let $\eta_3 \leq \eta_2 \leq \eta_1$ be the eigenvalues of the matrix $h - f$. Since $h \in \mu_\varepsilon(f)$, we have that $h \sqsubseteq f$, i.e. $h - f$ is positive semi-definite. Therefore, $\eta_i \geq 0$ for all i. It then follows that since $h - f$ is symmetric,

$$\begin{aligned} \max_{x \in S^2} \langle x, [h-f]x \rangle = \eta_1 &= \mathrm{tr}(h-f) - \eta_2 - \eta_3 \\ &= \mathrm{tr}(h) - \mathrm{tr}(f) - \eta_2 - \eta_3 \\ &\leq \mathrm{tr}(h) - \mathrm{tr}(f) \\ &= 4\Big[\mu(h) - \mu(f)\Big] \\ &< 4\Big[\varepsilon - \mu(f)\Big] \\ &= 4\Big[\tfrac{1}{4} \min_{x \in S^2} \langle x, [g-f]x \rangle + \mu(f) - \mu(f)\Big] \\ &= \min_{x \in S^2} \langle x, [g-f]x \rangle, \end{aligned} \tag{66}$$

where the first inequality follows from the fact that $\eta_2, \eta_3 \geq 0$ while the second inequality is due to the assumption that $\mu(h) < \varepsilon$. Simply put, we have shown that

$$\min_{x \in S^2} \langle x, [g-f]x \rangle - \max_{x \in S^2} \langle x, [h-f]x \rangle > 0. \tag{67}$$

Then by basic arithmetic, we finally have that

$$\begin{aligned} \min_{x \in S^2} \langle x, [g-h]x \rangle &= \min_{x \in S^2} \Big[\langle x, [g-f]x \rangle + \langle x, [f-h]x \rangle \Big] \\ &\geq \min_{x \in S^2} \langle x, [g-f]x \rangle + \min_{x \in S^2} \langle x, [f-h]x \rangle \\ &= \min_{x \in S^2} \langle x, [g-f]x \rangle + \min_{x \in S^2} \Big[- \langle x, [h-f]x \rangle \Big] \\ &= \min_{x \in S^2} \langle x, [g-f]x \rangle - \max_{x \in S^2} \langle x, [h-f]x \rangle \\ &> 0. \end{aligned} \tag{68}$$

Therefore, we have that $g - h > 0$. Of course, this implies that $1 \notin \sigma(h)$, otherwise the inner product $\langle x, [g-h]x \rangle \leq 0$ when $hx = x$. Consequently, by Theorem 2.2.9 we have that $g \ll h$. Thus, $f \in \mu_\varepsilon(f) \subseteq \uparrow g$, as desired. Thus we have shown that μ measures the content of each symmetric unital channel. □

The measurement of a continuous domain provides a qualitative view of its elements. We remind the reader that our order is defined such that two channels compare if and only if one channel produces a lower error rate than the other for all representations of information. With our measurement we now have a means of assigning a numeric value to each channel that is directly correlated to the error it produces; explicitly, $\mu(f)$.

3. DYNAMIC ENVIRONMENTS

In quantum information theory it is assumed that environmental noise is unchanged for the duration of a given protocol. While this is sometimes true, it fails in a large number of situations. Anytime there is relative motion between communicating parties the environment is constantly changing, and therefore so are its effects. For example, if someone on Earth were trying to communicate with a satellite in orbit, the motion of the satellite relative to Earth would result in a dynamic environment. Even in the case of two ships at sea, the waves would introduce relative motion between the two parties via changing spatial rotations. Additional examples will be explored throughout this chapter.

3.1 Environment Operators and their Algebraic Properties

For us an environment is an operator ϕ on the set of qubit channels Ω. As we argued earlier, since the set of unital qubit channels ensures non-decreasing entropy and the rate of errors due to a channel f can be calculated by the symmetric channel $\frac{1}{2}(f+f^t)$, we will be restricting ourselves to the set of symmetric unital qubit channels $\mathscr{U}_s$. That is, every environment we discuss is represented by an operator ϕ on $\mathscr{U}_s$.

Definition 3.1.1. *An environment is a self map on the set of symmetric unital channels.*

3.1.1 Static Noise in a Dynamic Environment

We will see that even when our environment is dynamic it is possible to have noise that does not change over time.

Definition 3.1.2. *Let $f \in \mathscr{U}_s$. We say the environment ϕ is static at f when $\phi(f) = f$, otherwise the environment is dynamic at f. If ϕ is the identity map, then we say the environment is trivially static.*

Remark. *In current quantum information theory the environment operator is assumed to always be the identity.*

With Definition 3.1.2, the question then becomes "When does an environment operator have a fixed point?". While we do not answer this question in its entirety, due to the order theoretic structure of $\mathscr{U}_s$ we can establish a subset of environment operators that do admit static noise. We remind the reader of the following well-known result which can be found in [6]:

Theorem 3.1.3. *A monotone map $\phi : D \to D$ on a dcpo D with least element $\perp$ has a least fixed point given by*

$$\lim_{n\to\infty} \phi^n(\perp).$$

Thus, each dynamic environment described by a monotone operator admits static noise. Furthermore, there exists a least fixed point f^*, i.e. there exists a fixed point that produces less error than all the other fixed points. To this end, we spend the remainder of this paper looking at the set of monotone self maps on $\mathscr{U}_s$.

3.1.2 Monotone Transformations

Theorem 3.1.4. *Let $\mathscr{M}$ be the set of monotone self maps on $\mathscr{U}_s$. Then $\mathscr{M}$ is convex and closed under composition.*

Proof. We begin by showing that $\mathscr{M}$ is convex. Let $\phi_1, \phi_2 \in \mathscr{M}$, $f \in \mathscr{U}_s$, and $p \in [0,1]$. Then

$$\phi(f) = p\ \phi_1(f) + (1-p)\phi_2(f),$$

where $\phi_i(f) \in \mathscr{U}_s$. Since $\mathscr{U}_s$ is a convex set, it follows that $\phi(f) \in \mathscr{U}_s$. Furthermore, if $f \sqsubseteq g$, then

$$\langle x, [\phi(f) - \phi(g)]x\rangle = p\langle x, [\phi_1(f) - \phi_1(g)]x\rangle + (1-p)\langle x, [\phi_2(f) - \phi_2(g)]x\rangle \geq 0,$$

where the inequality follows from the assumption that ϕ_1 and ϕ_2 are monotone. Therefore, $f \sqsubseteq g$ implies $\phi(f) \sqsubseteq \phi(g)$, and we have shown that $\mathscr{M}$ is convex.

Lastly we show that that $\mathscr{M}$ is closed under composition. Let $\phi_1, \phi_2 \in \mathscr{M}$. It then follows that $f \sqsubseteq g$ implies $\phi_1(f) \sqsubseteq \phi_1(g)$, which in turn implies $\phi_2\big(\phi_1(f)\big) \sqsubseteq \phi_2\big(\phi_1(g)\big)$. That is, $\phi_2 \circ \phi_1$ is monotone. Similar arguments follow for $\phi_1 \circ \phi_2$. $\square$

Theorem 3.1.5. *The following are all monotone self maps on $\mathscr{U}_s$.*

(i) *Constant maps.*

(ii) $\phi(f) = pf$ *for all* $p \in [0,1]$.

(iii) $\phi(f) = p\mathrm{tr}(f)I$ *for all* $p \in [0, \frac{1}{3}]$.

(iv) $\phi(f) = hfh^t$ *for all* $h \in \mathscr{U}$ *such that* $hh^t = h^t h$.

Proof.

(i) Let ϕ be a constant self map on the set of symmetric unital channels. Then since every element compares with itself, we have that for any two channels f and g, $\phi(f) \sqsubseteq \phi(g)$. Thus ϕ is trivially monotone.

(ii) Let $\phi(f) = pf$ for all $p \in [0,1]$. Then $f \sqsubseteq g \ \Rightarrow\ pf \sqsubseteq pg \ \Rightarrow\ \phi(f) \sqsubseteq \phi(g)$.

(iii) Let $\phi(f) = p\mathrm{tr}(f)I$ for all $p \in [0, \frac{1}{3}]$. From Theorem 2.3.1 we know that the trace function is strictly monotone under the reverse order. That is, $f \sqsubseteq g$ implies that $\mathrm{tr}(g) < \mathrm{tr}(f)$. It then directly follows that $f \sqsubseteq g \Rightarrow p\mathrm{tr}(g) < p\mathrm{tr}(f)$. Therefore, $p\mathrm{tr}(f)I \sqsubseteq p\mathrm{tr}(g)I$, or $\phi(f) \sqsubseteq \phi(g)$.

(iv) Let $f, g \in \mathscr{U}_s$ and $h \in \mathscr{U}$ such that $f \sqsubseteq g$. Since f and g are symmetric, then by the definition of our order, the matrix $f-g$ is positive semidefinite; i.e. $x^t(f-g)x \geq 0$ for all $x \in S^2$. Likewise, $\phi(f) \sqsubseteq \phi(g)$ if and only if $\phi(f) - \phi(g)$ is symmetric and $x^t\big(\phi(f) - \phi(g)\big)x \geq 0$ for all $x \in S^2$. We begin by first showing this matrix is symmetric.

$$\phi(f) - \phi(g) = hfh^t - hgh^t = (hfh^t)^t - (hgh^t)^t = [\phi(f) - \phi(g)]^t,$$

where the second equality is due to the fact that f and g are both symmetric and $(AB)^t = B^t A^t$ for all matrices A and B. Lastly we show that $x^t\big(\phi(f)-\phi(g)\big)x \geq 0$ for all $x \in S^2$.

$$x^t\big(\phi(f)-\phi(g)\big)x = x^t\big(hfh^t - hgh^t\big)x = x^t h(f-g)h^t x = (h^t x)^t(f-g)(h^t x) \geq 0,$$

where the inequality follows from the fact that $h \in \mathscr{U}$ and the assumption that $f-g$ is positive semidefinite. □

With these examples of monotone maps, it is natural to next examine their least fixed points. We will begin by considering the first three examples and explore the fourth on its own as its fixed points are far more interesting.

Theorem 3.1.6. *From the standard fixed point theorem in domain theory we have the following:*

(i) *The only fixed point of a constant map is the channel contained in its image.*

(ii) *The least fixed point of $\phi(f) = pf$ where $p \in [0,1]$ is I if $p = 1$ and 0 if $p < 1$.*

(iii) *The least fixed point of $\phi(f) = p\mathrm{tr}(f)I$ where $p \in [0, \frac{1}{3}]$ is I if $p = \frac{1}{3}$ and 0 if $p < \frac{1}{3}$.*

Proof.

(i) In the case of a constant self map every member of $\mathscr{U}_s$ is mapped to the szme channel. Therefore, it is trivially true that the only fixed point is the channel contained in the image.

(ii) From Theorem 3.1.3 we know that the least fixed point of a monotone map $\phi : \mathscr{U}_s \to \mathscr{U}_s$ is given by

$$\lim_{n\to\infty} \phi^n(I).$$

Thus, we have that when $\phi(f) = pf$ where $p \in [0,1]$, the least fixed point is

$$\lim_{n\to\infty} p^n(I).$$

It then follows that if $p = 1$ the least fixed point is I, and when $p < 1$ the least fixed point is the zero matrix.

(iii) Following similar arguments we have that the least fixed point of $\phi(f) = p\mathrm{tr}(f)I$ where $p \in [0, \frac{1}{3}]$ is

$$\lim_{n\to\infty} (3p)^n(I).$$

Therefore, if $p = \frac{1}{3}$, then the least fixed point is I, but if $p < \frac{1}{3}$, then $3p < 1$ and the least fixed point is the zero matrix. □

Theorem 3.1.7. *Let $\phi(f) = hfh^t$ where $h \in \mathscr{U}$ and $hh^t = h^t h$. Then the least fixed point of ϕ is either* (i) *the identity,* (ii) *the completely mixed channel, or* (iii) *a projection.*

Proof. From Theorem 3.1.3 we know that the least fixed point of ϕ is given by the limit

$$f^* = \lim_{n\to\infty} \phi^n(I) = \lim_{n\to\infty} h^n\big(h^t\big)^n = \lim_{n\to\infty} \big(hh^t\big)^n,$$

where the last equality follows from the assumption that h is normal. Let $\lambda_1 \geq \lambda_2 \geq \lambda_3$ be the eigenvalues of hh^t with associated eigenvectors x_1, x_2, and x_3. We then have the following:

(i) If $\lambda_1 = \lambda_2 = \lambda_3 = 1$, then for all i, we have that $\left(hh^t\right)x_i = x_i$. Therefore, if follows that

$$\lim_{n\to\infty}\left[\left(hh^t\right)^n\right]x_i = \lim_{n\to\infty}\left[\left(hh^t\right)^n x_i\right] = x_i,$$

and we have that the eigenvalues of f^* are all 1.

(ii) If $\lambda_i < 1$ for all i, then

$$\lim_{n\to\infty}\left[\left(hh^t\right)^n\right]x_i = \lim_{n\to\infty}\left[\left(hh^t\right)^n x_i\right] = \lim_{n\to\infty}\left[\lambda_i^n x_i\right] = 0,$$

and we have that the eigenvalues of f^* are all 0. Furthermore, since f^* is symmetric we are left to conclude that $f^* = 0$.

(iii) Lastly, if the spectrum of hh^t contains 1 and a value less than 1, then we must have that $\lambda_1 = 1$ and $\lambda_2 = \lambda_3 < 1$. It then follows from the arguments above that $f^*x_1 = x_1$ and $f^*x_2 = f^*x_3 = 0$. That is, f^* is symmetric and has spectrum $\{1,0,0\}$. □

Theorem 3.1.8. *Let f^* be the least fixed point of $\phi(f) = hfh^t$, where $h \in \mathscr{U}$. If h fixes $x \in S^2$, then f^* fixes x.*

Proof. Let $h \in \mathscr{U}$, then h has at least one eigenvalue. Let $hx = x$, then by the definition of adjoint $\langle x, hx\rangle = \langle x, h^t x\rangle = 1$. Furthermore, since $\mathscr{U}$ is closed under transpose and each of its members is non-expansive, we have that $h^t x = x$. Then

$$f^*x = \lim_{n\to\infty}\left[h^n(h^t)^n\right]x = \lim_{n\to\infty}\left[h^n(h^t)^n x\right] = \lim_{n\to\infty}[x] = x.$$

□

3.2 Security Implications

In this final section, we address the security Implications of a dynamic environment on the following protocols: Adaptive Quantum Information Processing, Authentication by Teleportation, and Quantum Key Distribution. In particular, with each of these protocols we will see that our measurement on the continuous domain of symmetric unital channels will serve as a qualitative metric for determining the security risks associated with a dynamic environment.

3.2.1 Authentication by Teleportation

Authentication by teleportation provides Alice and Bob a means to verify that they are communicating with one another. This method works in three steps: (1) Alice and Bob agree upon a password prior to the protocol. (2) Using a device to produce entangled pairs, Alice then teleports the previously agreed upon password to Bob. (3) Upon receiving the password Bob can then confirm that he is receiving information from Alice.

While this protocol appears to be outside the reach of the effects of dynamic environments, in Martin's paper [7] it is shown that teleportation with imperfect states produces a diagonal channel. Under the reasonable assumption that the device producing entangled pairs is imperfect, i.e. varies at least slightly from pair to pair in regards to degree of entanglement, then said device would induce a dynamic environment.

Moreover, the dynamic effects of said device could result in Alice and Bob's inability to verify from whom they are receiving information, and thus producing a major security risk.

Our measurement μ on the domain of symmetric unital channels has the potential to provide insight to this problem. The measurement μ provides a qualitative analysis of the potential error rates produced by imperfect entanglement and therefore the probability of success for authentication by teleportation. For instance, if $\mu(f) = 1$, then we know that f is the identity and produces no error. This translates to unaffected teleportation and thus no chance of failed authentication; i.e. the protocol is successful with a probability of 1. However, if $\mu(f) = 0$, then we know that the channel has trace -1, i.e. there is no channel that produces more error for all representation of information.

3.2.2 Adaptive Quantum Information Processing

Section 5547's newly patented process Adaptive Quantum Information Processing (AQIP) [**?**] can improve protocol performance in just two steps: (1) determine the representation that results in the lowest rate of error (2) exchange information using said representation [1]. However, in the case that an eavesdropper (Eve) does not know the choice of representation being used by the communicating parties, but is aware that AQIP is being used, she can introduce noise (creating a dynamic environment) in order to encourage a change of representation by the communicating parties. In this way, Eve is able to influence how the qubits are prepared, and therefore, greatly increase her chances of successfully stealing information.

3.2.3 Adaptive Quantum Key Distribution

Adaptive Quantum Key Distribution is the application of AQIP to the already established protocol Quantum Key Distribution. QKD is a protocol in which a one-time pad is securely generated between two parties. This protocol requires that Alice and Bob agree upon a pair of orthogonal communication bases, each one utilized with a probability of $\frac{1}{2}$ [2].

The requirement that the bases be orthogonal is of great importance. Let us assume there exists an eavesdropper $\big(\text{Eve}\big)$ that intercepts qubits sent by Alice, measures them, and then transmits the resulting qubit to Bob. Then any information Eve gains can introduce error in Bob's measurements because x and y are physically indistinguishable states. Let us explain this as follows:

Since Eve has no knowledge of the communication basis in which each qubit is prepared, she can only guess with a $\frac{1}{2}$ probability of accuracy when performing her own measurements. If she chooses correctly, then Eve will obtain the state sent by Alice and send it to Bob resulting in no error. However, if she chooses incorrectly, the state she obtains is not only in a different basis but random, and Bob will necessarily receive a state that is different from the one Alice prepared. That is, if Eve intercepts the state x but measures in the y basis, then she would send Bob either the state y or $-y$, each with probability

$$p(y|x) = \frac{1 + \langle x, y \rangle}{2} = \frac{1}{2}. \tag{69}$$

Assuming Bob measures the qubit in the same basis that Alice used to prepare (otherwise the qubit would have been discarded in the last step of the protocol), he would then obtain some result with a $\frac{1}{2}$ probability of error. Therefore, since Eve measures in the wrong basis with a probability of $\frac{1}{2}$, for each qubit sent Bob has an overall $\frac{1}{4}$ probability of error. Consequently, if the rate of error is too high, then Alice and Bob can agree

to abort the protocol as an eavesdropper could be present. Thus, we see that physically indistinguishable states can offer a means of security. Let us further explore protocols of this form.

In Adaptive QKD, Alice and Bob first engage in AQIP to determine the most efficient representation, after which they then perform QKD as normal with utilizing said representation. The security risks due to dynamic environment for AQIP then also apply to this protocol. Additionally, a dynamic environment would result in changing error rates that could potentially render the security measures of QKD useless. For instance, if the environment were to evolve in such a way that the rate of errors increase to or above the rate expected by the actions of an eavesdropper, then false abortions would occur at even greater probability. That is the design of QKD would no longer be providing a means of secure communication, but rather a reduction to its overall performance and successful key generation.

4. OPEN QUESTIONS AND FUTURE RESEARCH

With the security implications of dynamic environments established, the next natural step is to investigate processes that could minimize the effects of such risks. As discussed earlier and shown in Dr. Bonior's doctoral thesis [4], there exists a particular class of functions, namely Scott continuous maps, which have fixed points on the set of symmetric unital channels. Aside from being an interesting mathematical result, these fixed points give rise to a possible method for mitigating security risks posed by dynamic environments.

To this end, we plan to develop a theoretical process for which the environment can be forced into the fixed point of the dynamic environment operator. That is, an environment that leaves a particular channel unchanged over time, i.e. user-induced static noise. It would then follow that all security risks due to the dynamic nature of the environment can be alleviated by forcing the environment into the fixed point of the environmental operator.

Primary deliverables for methods for mitigating security risks in dynamic environments

- Determination of which dynamic environments are physically realizable; a method for constructing the operator that describes a given physical dynamic environment.
- Determination of the effects that dynamic environments have on the security measures of additional well-known protocols.
- The conditions that lead to the "equilibrium" represented by a static environment, and the existence of "user induced equilibrium".
- An annual and final report upon completion of the project and attendance and presentation at a Navy-wide NISE Technical Exchange Meeting (TEM).

Measure of Success: While the immediate desired results include the formulation of a theory of dynamic environments and the determination of processes aimed to improve the security and efficiency of information protocols, the best metric for our overall success will be determined by the range of applicability. That is, the diversity of physical environments can we study, and the variety of quantum information protocols whose security concerns are described within the context of our theory.

ACKNOWLEDGMENTS

We would like to thank Keye Martin not only for the inspiration and support as a friend, mentor, and colleague, but for the insightful discussions and his previous research that defined the very basis of this project.

BIBLIOGRAPHY

1. Martin K., *The scope of a quantum channel*. Mathematical Structures in Computer Science, Cambridge(UK): Cambridge University Press, 2008.

2. Martin K. and Panangaden P., *A Domain of Spacetime Intervals in General Relativity*. Springer-Verlag 267:563, 2006.

3. Martin, K., *Topology in information theory in topology*. Theoretical Computer Science, Vol. 405, Issues 1-2, pages 75-87, 2008.

4. Bonior, D. *Mathematical Foundations of Adaptive Quantum Processing* (2018). Electronic Theses and Dissertation. 6173.

5. Chuang I. L. and Nielsen M. A., *Quantum Computation and Quantum Information*. Cambridge(UK): Cambridge University Press, 2008.

6. Martin K, (2013) Nothing Can Be Fixed. In: Coecke B., Ong L., Panangaden P. (eds) Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky. Lecture Notes in Computer Science, vol 7860. Springer, Berlin, Heidelberg.

7. Martin K, Feng J, Krishnan S, *A free object in quantum information theory*. Electronic Notes in Theoretical Computer Science, vol 265, 6 September 2010, pages 35-47.