

CHANNEL COVARIANCE, TWIRLING, CONTRACTION, AND SOME UPPER BOUNDS ON THE QUANTUM CAPACITY

YINGKAI OUYANG

*Department of Combinatorics and Optimization, Institute of Quantum Computing
University of Waterloo, 200 University Avenue West
Waterloo, Ontario N2L 3G1, Canada*^a

*Department of Engineering and Product Development
Singapore University of Technology and Design
20 Dover Drive, Singapore 138682, Singapore*^b

Received December 6, 2012

Revised November 11, 2013

Evaluating the quantum capacity of quantum channels is an important but difficult problem, even for channels of low input and output dimension. Smith and Smolin showed that the quantum capacity of the Clifford-twirl of a qubit amplitude damping channel (a qubit depolarizing channel) has a quantum capacity that is at most the coherent information of the qubit amplitude damping channel evaluated on the maximally mixed input state. We restrict our attention to obtaining upper bounds on the quantum capacity using a generalization of Smith and Smolin’s degradable extension technique. Given a degradable channel \mathcal{N} and a finite projective group of unitaries \mathcal{V} , we show that the \mathcal{V} -twirl of \mathcal{N} has a quantum capacity at most the coherent information of \mathcal{N} maximized over a \mathcal{V} -contracted space of input states. As a consequence, degradable channels that are covariant with respect to diagonal Pauli matrices have quantum capacities that are their coherent information maximized over just the diagonal input states. As an application of our main result, we supply new upper bounds on the quantum capacity of some unital and non-unital channels – d -dimensional depolarizing channels, two-qubit locally symmetric Pauli channels, and shifted qubit depolarizing channels.

Keywords: Quantum information theory, quantum capacity, upper bounds, degradable, twirling, contraction, depolarizing channel

Communicated by: R. Jozsa & A. Harrow

1 Introduction

The quantum capacity of a quantum channel is the maximum rate at which quantum information can be transmitted reliably across it, given arbitrarily many uses of it [1]. However, evaluating the best known regularized expressions for the quantum capacity of a general quantum channel is in general an infinite-dimensional optimization problem, and hence difficult, even for quantum channels with low dimensional input and output states. The quantum

^a*y3ouyang@math.uwaterloo.ca*

^b*yingkai_ouyang@sutd.edu.sg*

capacity of even the simply described family of qubit depolarizing channels is undetermined, in spite of much effort [2, 3, 4, 5, 6, 7, 8, 9]. Thus, obtaining upper bounds on the quantum capacity of quantum channels is a non-trivial and important problem.

Our main result generalizes the technical results of Smith and Smolin [6] pertaining to the use of degradable extensions to obtain upper bounds on the quantum capacity of channels in terms of the coherent information of other channels. In our extension of Smith and Smolin's recipe, we prove that the quantum capacity of a degradable channel twirled with respect to a projective unitary group is at most the coherent information of the degradable channel maximized over a contracted input state space (Theorem 4.1). Smith and Smolin's recipe is produced as a special case of our extension when the projective unitary group is chosen to be the full qubit Clifford group. As a consequence, a degradable channel that is covariant with respect to diagonal Pauli matrices has a quantum capacity that is equal to its coherent information maximized over just the diagonal input states.

As an application of our main result, we supply new upper bounds on the quantum capacity of some unital and non-unital channels – d -dimensional depolarizing channels, two-qubit locally symmetric Pauli channels, and shifted qubit depolarizing channels. The main ingredients that we introduce to obtain these new upper bounds are our higher dimensional amplitude damping channels that are degradable. These higher dimensional amplitude damping channels generalize qubit amplitude damping channels.

The rest of the paper is organized in the following way. In Section 2, we introduce notations and review concepts pertaining to the quantum capacity, degradable channels and the degradable extensions of Smith and Smolin. In Section 3, we review the notion of channel covariance, channel twirling, and channel contraction. In Section 4, we present the main result of this paper, which is Theorem 4.1, placed in the context of channel twirlings and channel covariance. In Section 5, we apply our main result to obtain explicit upper bounds on the quantum capacity of d -dimensional depolarizing channels, locally symmetric and SWAP-invariant two-qubit Pauli channels, and shifted depolarizing channels. Our appendix contains the more technical ancillary results of this paper.

2 Preliminaries

2.1 General Notation

Given a function $f : \Omega \rightarrow \mathbb{R}$ and a subset $X \subseteq \Omega$, define the X -restricted convex hull of the function f evaluated on the argument x to be

$$\text{conv}(f; x, X) := \inf_{\substack{y, z \in X \\ \lambda \in [0, 1]}} \left\{ \lambda f(y) + (1 - \lambda)f(z) : x = \lambda y + (1 - \lambda)z \right\}.$$

Given a sequence of functions $f_1, \dots, f_n : \Omega \rightarrow \mathbb{R}$, define $\min\{f_1, \dots, f_n\}$ to be a function that is the pointwise minimum of the sequence f_1, \dots, f_n , that is,

$$(\min\{f_1, \dots, f_n\})(x) := \min\{f_1(x), \dots, f_n(x)\}.$$

Now define the X -restricted convex hull of the sequence of functions f_1, \dots, f_n evaluated on the argument x to be

$$\text{conv}(f_1, \dots, f_n; x, X) := \text{conv}(\min\{f_1, \dots, f_n\}; x, X).$$

We introduce this notion of the X -restricted convex hull because it is a tool that we later use to establish upper bounds on the quantum capacity of various quantum channels.

Define $\eta(z) := -z \log_2 z$ where $z \in [0, 1]$ and $\eta(0) := 0$. Let $H_2(q) := \eta(q) + \eta(1 - q)$ be the binary entropy function. Define the Pauli matrices to be

$$\mathbb{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{X} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathbf{Z} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \mathbf{Y} := i\mathbf{XZ}.$$

Define the Pauli group on m qubits modulo phases, to be $\mathcal{P}_m := \{\mathbb{1}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}^{\otimes m}$. For all $\mathbf{P} \in \mathcal{P}_m$, define the weight of \mathbf{P} to be the number of qubits on which the operator \mathbf{P} acts non-trivially.

2.2 Quantum Channels and the Quantum Capacity

For a complex separable Hilbert space \mathcal{H} , let $\mathfrak{B}(\mathcal{H})$ be the set of bounded linear operators mapping \mathcal{H} to \mathcal{H} . In this paper, we only deal with finite-dimensional Hilbert spaces. A quantum channel $\mathcal{N} : \mathfrak{B}(\mathcal{H}_A) \rightarrow \mathfrak{B}(\mathcal{H}_B)$ is a completely positive and trace-preserving (CPT) linear map, and can be written in terms of a Kraus representation [10]

$$\mathcal{N}(\rho) = \sum_k \mathbf{A}_k \rho \mathbf{A}_k^\dagger,$$

where the completeness relation $\sum_k \mathbf{A}_k^\dagger \mathbf{A}_k = \mathbb{1}_{d_A}$ is satisfied, $d_A = \dim(\mathcal{H}_A)$ and $\mathbb{1}_{d_A}$ is a dimension d_A identity matrix. We can also write down the action of a quantum channel \mathcal{N} in terms of an isometry on the input state. Now define an isometry $\mathbf{W} : \mathfrak{B}(\mathcal{H}_A) \rightarrow \mathfrak{B}(\mathcal{H}_E \otimes \mathcal{H}_B)$

$$\mathbf{W} = \sum_k |k\rangle \otimes \mathbf{A}_k.$$

Here $\{|k\rangle\}$ is an orthonormal set, and spans a Hilbert space \mathcal{H}_E that we interpret to be the environment. Then

$$\mathbf{W} \rho \mathbf{W}^\dagger = \sum_{j,k} |j\rangle \langle k| \otimes \mathbf{A}_j \rho \mathbf{A}_k^\dagger$$

and

$$\text{Tr}_{\mathcal{H}_E}(\mathbf{W} \rho \mathbf{W}^\dagger) = \mathcal{N}(\rho).$$

Then we can define the **complementary channel** $\mathcal{N}^C : \mathfrak{B}(\mathcal{H}_A) \rightarrow \mathfrak{B}(\mathcal{H}_E)$ [11] as

$$\mathcal{N}^C(\rho) = \text{Tr}_{\mathcal{H}_B}(\mathbf{W} \rho \mathbf{W}^\dagger).$$

Since we are free to choose the orthonormal basis of the environment \mathcal{H}_E , \mathcal{N}^C is only unique up to a unitary transformation. We use the above definition as our canonical one. Let

$\mathcal{N}^C(\rho) = \sum_{\mu} \mathbf{R}_{\mu} \rho \mathbf{R}_{\mu}^{\dagger}$. The j -th row of \mathbf{R}_{μ} is the μ -th row of \mathbf{A}_j , where $\mathbf{R}_{\mu} = \sum_j |j\rangle\langle\mu| \mathbf{A}_j$ [12]. To see this, observe that

$$\begin{aligned} \mathcal{N}^C(\rho) &= \text{Tr}_{\mathcal{H}_B}(\mathbf{W}\rho\mathbf{W}^{\dagger}) \\ &= \text{Tr}_{\mathcal{H}_B}\left(\sum_{j,k} |j\rangle\langle k| \otimes \mathbf{A}_j \rho \mathbf{A}_k^{\dagger}\right) \\ &= \sum_{j,k} |j\rangle\langle k| \text{Tr}\left(\mathbf{A}_j \rho \mathbf{A}_k^{\dagger}\right) \\ &= \sum_{j,k} |j\rangle\langle k| \sum_{\mu} \langle\mu| \left(\mathbf{A}_j \rho \mathbf{A}_k^{\dagger}\right) |\mu\rangle\langle k| \\ &= \sum_{\mu} \left(\sum_j |j\rangle\langle\mu| \mathbf{A}_j\right) \rho \left(\sum_k \mathbf{A}_k^{\dagger} |\mu\rangle\langle k|\right) \\ &= \sum_{\mu} \mathbf{R}_{\mu} \rho \mathbf{R}_{\mu}^{\dagger}. \end{aligned}$$

For a quantum channel $\mathcal{N} : \mathfrak{B}(\mathcal{H}_A) \rightarrow \mathfrak{B}(\mathcal{H}_B)$, Schumacher and Nielsen defined its coherent information [13] with respect to an input state as a difference of von Neumann entropies

$$I_{\text{coh}}(\mathcal{N}, \rho) := S(\mathcal{N}(\rho)) - S(\mathcal{N}^C(\rho))$$

where the von Neumann entropy of a state ρ is

$$S(\rho) := -\text{Tr}(\rho \log_2 \rho).$$

We denote the channel's optimized coherent information as

$$I_{\text{coh}}(\mathcal{N}) := \max_{\rho} I_{\text{coh}}(\mathcal{N}, \rho).$$

Here, the maximization of ρ is performed over all quantum states in $\mathfrak{B}(\mathcal{H}_A)$. Lloyd [14], Shor [15] and Devetak [16] showed that the quantum capacity of \mathcal{N} is

$$Q(\mathcal{N}) = \lim_{n \rightarrow \infty} \frac{1}{n} I_{\text{coh}}(\mathcal{N}^{\otimes n}), \quad (1)$$

and the limit on the right hand side of (1) exists [17]. Schumacher and Westmoreland also demonstrated that a channel's coherent information is also a lower bound on the amount of its private information [18].

2.3 Degradable Channels and Degradable Extensions

A channel \mathcal{N} is *degradable* [11] if it can be composed with another quantum channel Ψ to become equivalent to its complementary channel \mathcal{N}^C , that is $\mathcal{N}^C = \Psi \circ \mathcal{N}$. Physically, this means that the environment associated with the channel \mathcal{N} can be simulated using the output quantum state of channel the \mathcal{N} . Conversely, \mathcal{N} is *antidegradable* if its complementary channel \mathcal{N}^C is degradable. A channel \mathcal{N}_{ext} is a *degradable extension* [6] of channel \mathcal{N} if \mathcal{N}_{ext} is degradable and there exists a quantum operation Ψ such that $\Psi \circ \mathcal{N}_{\text{ext}} = \mathcal{N}$.

A degradable channel \mathcal{N} has a simple expression for its quantum capacity, which is $Q(\mathcal{N}) = I_{\text{coh}}(\mathcal{N})$ [11]. If the degradable channel \mathcal{N} also extends a channel \mathcal{M} that is not necessarily degradable, we have $Q(\mathcal{M}) \leq I_{\text{coh}}(\mathcal{N})$. Moreover if $\mathcal{N} = \sum_i \lambda_i \mathcal{N}_i$ is a convex combination of degradable channels \mathcal{N}_i , then we have the crucial convexity property [6] given by

$$Q(\mathcal{M}) \leq \sum_i \lambda_i I_{\text{coh}}(\mathcal{N}_i).$$

Thus, degradable extensions can be used to construct upper bounds on the quantum capacity of quantum channels [6].

3 Channel Covariance, Twirling and Contraction

In this section, we introduce the concepts of covariance, twirling and contraction which are essential to state our main result in Theorem 4.1.

Let \mathcal{V} be a set of unitary operators^c. A channel \mathcal{N} is said to be \mathcal{V} -covariant if for all input quantum states ρ and elements \mathbf{V} of \mathcal{V} , we have $\mathcal{N}(\mathbf{V}\rho\mathbf{V}^\dagger) = \mathbf{V}\mathcal{N}(\rho)\mathbf{V}^\dagger$. Properties of quantum channels covariant with respect to locally compact groups were studied by Holevo [19].

Define $\mathcal{V}_\triangleright(\rho) := \frac{1}{|\mathcal{V}|} \sum_{\mathbf{V} \in \mathcal{V}} \mathbf{V}\rho\mathbf{V}^\dagger$ to be a \mathcal{V} -contraction channel. We also denote the \mathcal{V} -twirl of \mathcal{N} as the channel $\mathcal{N}_{\times \mathcal{V} \times}$ where $\mathcal{N}_{\times \mathcal{V} \times}(\rho) := \frac{1}{|\mathcal{V}|} \sum_{\mathbf{V} \in \mathcal{V}} \mathbf{V}^\dagger \mathcal{N}(\mathbf{V}\rho\mathbf{V}^\dagger) \mathbf{V}$. When the set \mathcal{V} is the m -qubit Pauli set \mathcal{P}_m , the \mathcal{V} -twirl of a channel \mathcal{N} has the Kraus operators

$$\frac{\mathbf{P}}{2^m} \sqrt{\sum_{\mathbf{K} \in \mathfrak{K}_{\mathcal{N}}} |\text{Tr}(\mathbf{P}\mathbf{K})|^2},$$

where $\mathbf{P} \in \mathcal{P}_m$ and $\mathfrak{K}_{\mathcal{N}}$ is the Kraus set of \mathcal{N} [20].

We say that a finite set of unitary matrices \mathcal{V} is a finite projective group if (i) no two distinct elements of \mathcal{V} are equivalent up to a constant, and (ii) for all \mathbf{V} and \mathbf{W} in the set \mathcal{V} , there exists a unique complex number of unit magnitude $z_{\mathbf{V}, \mathbf{W}^\dagger}$ such that $z_{\mathbf{V}, \mathbf{W}^\dagger} \mathbf{V}\mathbf{W}^\dagger$ is also an element of \mathcal{V} . A channel that is \mathcal{V} -covariant need not be invariant under \mathcal{V} -twirling. However this is the case when \mathcal{V} is a multiplicative (or projective) group \mathcal{V} .

4 Main Result

The main result of this paper is a generalization of Smith and Smolin’s technique of degradable extensions (see Lemma 8 of [6]). Our main result states that the quantum capacity of a \mathcal{V} -twirled degradable channel is at most its coherent information maximized over the set of correspondingly \mathcal{V} -contracted input states. Here \mathcal{V} is a finite projective group of d -dimensional unitary operators. Our result is a generalization of Smith and Smolin’s technique in the sense that the set \mathcal{V} need not be restricted to just the set of single-qubit Clifford operators.

^cThe only instance where \mathcal{V} is not a group in this paper is in the proof of Theorem 5.9.

To state our main result formally, first define $\tilde{\mathcal{N}}$ to be an extension of the \mathcal{V} -twirl $\mathcal{N}_{\times\mathcal{V}\times}$, where

$$\tilde{\mathcal{N}}(\rho) := \sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} \mathbf{V}^\dagger \mathcal{N}(\mathbf{V}\rho\mathbf{V}^\dagger) \mathbf{V} \otimes |\mathbf{V}\rangle\langle\mathbf{V}|. \quad (2)$$

Theorem 4.1 (Twirling and Contraction). *Let \mathcal{V} be a projective group of d -dimensional unitary matrices, \mathcal{N} be a degradable channel with d -dimensional input and output states, and $\tilde{\mathcal{N}}$ be as defined in (2). Then $Q(\mathcal{N}_{\times\mathcal{V}\times}) \leq Q(\tilde{\mathcal{N}}) \leq \max_{\rho} I_{\text{coh}}(\mathcal{N}, \mathcal{V}_{\triangleright}(\rho))$.*

We supply the proof of Theorem 4.1 in Section 4.2. The main idea of the proof is a straightforward extension of the methods used by Smith and Smolin (Lemma 8 in [6]). A technical result needed in the proof is the following proposition.

Proposition 4.2. *Let \mathcal{N} be a quantum channel with d -dimensional input and output states, \mathcal{V} be a set of d -dimensional unitary matrices, and $\tilde{\mathcal{N}}$ be as defined in (2). Then*

$$\tilde{\mathcal{N}}^C(\rho) = \sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} \mathcal{N}^C(\mathbf{V}\rho\mathbf{V}^\dagger) \otimes |\mathbf{V}\rangle\langle\mathbf{V}|. \quad (3)$$

The proof of Proposition 4.2 uses only techniques from [6], and we defer its proof to Section B.

Corollary 4.3 (Degradable and Covariant Channels). *Let \mathcal{V} be a finite projective unitary group. If a degradable channel \mathcal{N} is also \mathcal{V} -covariant, then $Q(\mathcal{N}) = \max_{\rho} I_{\text{coh}}(\mathcal{N}, \mathcal{V}_{\triangleright}(\rho))$.*

Proof of Corollary 4.3. Since the channel \mathcal{N} is degradable,

$$Q(\mathcal{N}) = I_{\text{coh}}(\mathcal{N}) \geq \max_{\rho} I_{\text{coh}}(\mathcal{N}, \mathcal{V}_{\triangleright}(\rho)).$$

Since $\mathcal{N}_{\times\mathcal{V}\times} = \mathcal{N}$, Theorem 4.1 implies that $Q(\mathcal{N}) \leq \max_{\rho} I_{\text{coh}}(\mathcal{N}, \mathcal{V}_{\triangleright}(\rho))$. \square

The set of diagonal m -qubit Pauli matrices $\mathcal{Z}_m := \{\mathbb{1}, \mathbf{Z}\}^{\otimes m}$ is an example of a finite projective group of unitary matrices. Our result shows that a degradable channel \mathcal{N} which is \mathcal{Z}_m -covariant has quantum capacity equal to $I_{\text{coh}}(\mathcal{N}, \rho)$ maximized over all diagonal m -qubit quantum states ρ .

4.1 Examples of Degradable Channels that are Covariant

Here, we show that examples of degradable channels that are \mathcal{Z}_m -covariant include special m -qubit Hadamard channels that admit a Pauli decomposition with diagonal Kraus operators, all m -qubit almost-Pauli channels, all single-qubit degradable channels, and the higher dimensional amplitude damping channels that we introduce in Section 5.1. We prove these facts in this section.

We say that a quantum channel is *almost-Pauli* if it admits a Kraus decomposition with all of its Kraus operators having the form $\mathbf{K}_j = \mathbf{D}_j \mathbf{P}_j$ where \mathbf{D}_j is a size 2^m diagonal matrix and $\mathbf{P}_j \in \mathcal{P}_m$. Almost-Pauli channels are covariant with respect to the m -qubit diagonal Pauli matrices because

$$(\mathbf{D}_j \mathbf{P}_j)(\Lambda \mathbf{W} \Lambda)(\mathbf{P}_j \mathbf{D}_j^\dagger) = \Lambda(\mathbf{D}_j \mathbf{P}_j) \mathbf{W}(\mathbf{P}_j \mathbf{D}_j^\dagger) \Lambda$$

for all Paulis \mathbf{W} and diagonal Paulis $\Lambda \in \{\mathbb{1}, \mathbf{Z}\}^{\otimes m}$. The above equality holds because we can ‘propagate’ the Λ ’s ‘outwards’. This is because Pauli matrices either commute or anti-commute under multiplication, and diagonal matrices commute under multiplication. Hence a degradable almost-Pauli channel is \mathcal{Z}_m -covariant.

Proposition 4.4. *Qubit degradable channels are \mathcal{Z}_1 -covariant.*

Proof. All qubit degradable channels necessarily have Kraus operators of the following form [21, 22]

$$\begin{pmatrix} \cos \alpha & 0 \\ 0 & \cos \beta \end{pmatrix}, \quad \begin{pmatrix} 0 & \sin \beta \\ \sin \alpha & 0 \end{pmatrix} = \begin{pmatrix} \sin \beta & 0 \\ 0 & \sin \alpha \end{pmatrix} \mathbf{X}.$$

Hence these channels are almost-Pauli and the result follows. □

Any Hadamard channel maps a quantum state to some Hadamard product of it, and is the complementary channel of an entanglement breaking channel (which admits a Kraus decomposition with Kraus operators of rank one) (see [12, 23] and the references therein). Consider a special almost-Pauli m -qubit channel \mathcal{A} with only diagonal Kraus operators $\mathbf{A}_i = \sum_{j \in \mathbb{Z}_{2^m}} c_{i,j} |j\rangle\langle j|$ for $i \in \mathbb{Z}_{2^m}$. This channel \mathcal{A} is Hadamard because its complementary channel \mathcal{A}^C has Kraus operators $R_\mu = \sum_{i \in \mathbb{Z}_{2^m}} |i\rangle\langle \mu| c_{i,\mu}$ of column rank at most one. Hence almost-Pauli channels with purely diagonal Kraus operators are examples of Hadamard channels that are also \mathcal{Z}_m -covariant.

4.2 Proof of Theorem 4.1

Since \mathcal{V} is a finite projective unitary group, for all $\mathbf{V}, \mathbf{W} \in \mathcal{V}$, there exists a unique phase constant $z_{\mathbf{V}, \mathbf{W}} \in \mathbb{R}$ such that $z_{\mathbf{V}, \mathbf{W}} \mathbf{V} \mathbf{W} \in \mathcal{V}$. Define the \star product to be the binary operation given by

$$\mathbf{V} \star \mathbf{W} := z_{\mathbf{V}, \mathbf{W}} \mathbf{V} \mathbf{W}.$$

Hence for all $\mathbf{V}, \mathbf{W} \in \mathcal{V}$, we also have $\mathbf{V} \star \mathbf{W} \in \mathcal{V}$. Since every element of \mathcal{V} is a unitary matrix and \mathcal{V} is also a group, $\mathbf{V} \in \mathcal{V}$ also implies that $\mathbf{V}^\dagger \in \mathcal{V}$. Hence if $\mathbf{R} = \mathbf{V} \star \mathbf{W}$, we also have $\mathbf{V} = \mathbf{R} \star \mathbf{W}^\dagger$.

$$\begin{aligned} \tilde{\mathcal{N}}(\mathbf{W} \rho \mathbf{W}^\dagger) &= \sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} (\mathbf{W} \mathbf{W}^\dagger) \mathbf{V}^\dagger \mathcal{N}(\mathbf{V} \mathbf{W} \rho \mathbf{W}^\dagger \mathbf{V}^\dagger) \mathbf{V} (\mathbf{W} \mathbf{W}^\dagger) \otimes |\mathbf{V}\rangle\langle \mathbf{V}| \\ &= \sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} \mathbf{W} (z_{\mathbf{V}, \mathbf{W}} \mathbf{V} \mathbf{W})^\dagger \mathcal{N}((z_{\mathbf{V}, \mathbf{W}} \mathbf{V} \mathbf{W}) \rho (z_{\mathbf{V}, \mathbf{W}} \mathbf{V} \mathbf{W})^\dagger) (z_{\mathbf{V}, \mathbf{W}} \mathbf{V} \mathbf{W}) \mathbf{W}^\dagger \otimes |\mathbf{V}\rangle\langle \mathbf{V}|. \end{aligned}$$

Making the substitution $\mathbf{R} = \mathbf{V} \star \mathbf{W} = z_{\mathbf{V}, \mathbf{W}} \mathbf{V} \mathbf{W}$ we get

$$\tilde{\mathcal{N}}(\mathbf{W} \rho \mathbf{W}^\dagger) = \sum_{\mathbf{R} \star \mathbf{W}^\dagger \in \mathcal{V}} \frac{1}{|\mathcal{V}|} \mathbf{W} \mathbf{R}^\dagger \mathcal{N}(\mathbf{R} \rho \mathbf{R}^\dagger) \mathbf{R} \mathbf{W}^\dagger \otimes |\mathbf{R} \star \mathbf{W}^\dagger\rangle\langle \mathbf{R} \star \mathbf{W}^\dagger|.$$

Let $\mathbf{U}_{\mathbf{W}} := \sum_{\mathbf{R} \in \mathcal{V}} |\mathbf{R} \star \mathbf{W}^\dagger\rangle\langle \mathbf{R}|$ be a unitary matrix that depends on $\mathbf{W} \in \mathcal{V}$. Since \mathcal{V} is a group under the binary operation \star , $\mathcal{V} \star \mathbf{W} = \mathcal{V}$, and we can replace the summation index of the right hand side of the above equation to get

$$\tilde{\mathcal{N}}(\mathbf{W} \rho \mathbf{W}^\dagger) = (\mathbf{W} \otimes \mathbf{U}_{\mathbf{W}}) \tilde{\mathcal{N}}(\rho) (\mathbf{W}^\dagger \otimes \mathbf{U}_{\mathbf{W}}^\dagger). \tag{4}$$

Now we can use the isometric extensions of the channels \mathcal{N} and $\tilde{\mathcal{N}}$ to show that (see Proposition 4.2)

$$\tilde{\mathcal{N}}^C(\rho) = \sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} \mathcal{N}^C(\mathbf{V}\rho\mathbf{V}^\dagger) \otimes |\mathbf{V}\rangle\langle\mathbf{V}|.$$

By a similar argument as in (4),

$$\tilde{\mathcal{N}}^C(\mathbf{V}\rho\mathbf{V}^\dagger) = (\mathbb{1}_{d_E} \otimes \mathbf{U}_{\mathbf{V}}) \tilde{\mathcal{N}}^C(\rho) (\mathbb{1}_{d_E} \otimes \mathbf{U}_{\mathbf{V}}^\dagger), \tag{5}$$

where d_E is the dimension of the output states of the complementary channel \mathcal{N}^C . Note that the von Neumann entropy is additive with respect to each block in a block diagonal matrix, and is also invariant under unitary conjugation of its argument. Hence the coherent information of the degradable extension $\tilde{\mathcal{N}}$ evaluated on the input state ρ is

$$\begin{aligned} S(\tilde{\mathcal{N}}(\rho)) - S(\tilde{\mathcal{N}}^C(\rho)) &= \left(\sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} S(\mathcal{N}(\mathbf{V}\rho\mathbf{V}^\dagger)) \right) - \left(\sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} S(\mathcal{N}^C(\mathbf{V}\rho\mathbf{V}^\dagger)) \right) \\ &= \sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} I_{\text{coh}}(\mathcal{N}, \mathbf{V}\rho\mathbf{V}^\dagger) \\ &\leq I_{\text{coh}}\left(\mathcal{N}, \sum_{\mathbf{V} \in \mathcal{V}} \frac{1}{|\mathcal{V}|} \mathbf{V}\rho\mathbf{V}^\dagger\right), \end{aligned}$$

where the inequality above results from the concavity of the coherent information of degradable channels with respect to the input state [24]. Hence the coherent information of the degradable channel \mathcal{N} maximized over all output states of the \mathcal{V} -contraction channel upper bounds the coherent information and the quantum capacity of the degradable extension $\tilde{\mathcal{N}}$. \square

5 Application to obtain Upper Bounds

5.1 Degradable Amplitude Damping Channels

Qubit amplitude damping channels model spontaneous decay in two-level quantum systems [25], and also model the map induced by beamsplitter acting on a superposition of the vacuum and a single photon with a trace taken over one output mode [26]. Hence knowledge of their quantum capacity is a physically relevant problem. These channels (when degradable) are essential ingredients of Smith and Smolin’s recipe [6] for upper bounding the quantum capacity of the qubit depolarizing channel [6]. Analogously, higher dimensional generalizations of the qubit amplitude damping channel that are degradable are essential ingredients of Theorem 4.1 in upper bounding the quantum capacity of higher dimensional channels.

In this section, we introduce uniform amplitude damping channels and special two-qubit amplitude damping channels which generalize the single-qubit amplitude damping channels. We also introduce the beamsplitter-type amplitude damping channel that models multi-photon input states passing through a beamsplitter. We give sufficient conditions for these channels to be degradable.

Define a *uniform amplitude damping channel* $\mathcal{A}_{\gamma,d}$ to be a channel with the Kraus operators $|0\rangle\langle 0| + \sum_{i=1}^{d-1} \sqrt{1-\gamma}|i\rangle\langle i|$ and $\sqrt{\gamma}|0\rangle\langle j|$, where $1 \leq j \leq d-1$.

Proposition 5.1. *Let integer $d \geq 2$, and $0 \leq \gamma \leq \frac{1}{2}$. Then $\mathcal{A}_{\gamma,d}$ is a degradable channel.*

Proof. Note that $\mathcal{A}_{\frac{1-2\gamma}{1-\gamma},d} \circ \mathcal{A}_{\gamma,d} = \mathcal{A}_{1-\gamma,d} = \mathcal{A}_{\gamma,d}^C$. □

We assume that a beamsplitter of transmissivity $\eta \in [0, 1]$ is a unitary operation $\mathcal{U}_{BS,\eta}$ that (1) maps an input bosonic mode (with annihilation operator a and Hilbert space A) and an external bosonic mode (with annihilation operator b and Hilbert space B) to two output bosonic modes [26, 27], (2) maps a tensor product of vacuum states to a tensor product of vacuum states [27], and (3) maps the annihilation operators a and b to $\eta a + \sqrt{1-\eta}b$ and $\sqrt{1-\eta}a + \eta b$ respectively. We also assume that the input state in the external bosonic mode is the vacuum state $(|0\rangle\langle 0|)_B$. If these assumptions are self-consistent, one can show that $\text{Tr}_B(\mathcal{U}_{BS,1-\gamma}(|i\rangle\langle j|)_A \otimes (|0\rangle\langle 0|)_B)$ is equivalent to the expression on the right hand side of (6) summed over all natural numbers n for all $i, j \in \mathbb{N}$. This motives us to define a *beamsplitter-type amplitude damping channel* $\mathcal{A}_{BS,\gamma}$ to be a channel with Kraus operators

$$A_{n,\gamma} := \sum_{k \geq 0} |k\rangle\langle k+n| \sqrt{\binom{n+k}{n} \gamma^n (1-\gamma)^k}$$

for all $n \in \mathbb{N}$ and $\gamma \in [0, 1]$.

Proposition 5.2. *Let $0 \leq \gamma \leq \frac{1}{2}$. Then $\mathcal{A}_{BS,\gamma}$ is a degradable channel.*

Proof. Note that for all $i, j, n \in \mathbb{N}$ and $0 \leq \gamma < 1$,

$$A_{n,\gamma} |i\rangle\langle j| A_{n,\gamma}^\dagger = |i-n\rangle\langle j-n| \left(\frac{\gamma}{1-\gamma}\right)^n \sqrt{\binom{i}{n} \binom{j}{n} (1-\gamma)^{i+j}}. \tag{6}$$

Let $\gamma_1, \gamma_2 \in [0, \frac{1}{2}]$. The identity $\binom{i}{n_1} \binom{j}{n_1} \binom{i-n_1}{n_2} \binom{j-n_1}{n_2} = \binom{n}{n_1}^2 \binom{i}{n} \binom{j}{n}$ and the above equation implies that

$$\begin{aligned} & \sum_{\substack{n_1+n_2=n \\ n_1, n_2 \in \mathbb{N}}} A_{n_2,\gamma_2} A_{n_1,\gamma_1} |i\rangle\langle j| A_{n_1,\gamma_1}^\dagger A_{n_2,\gamma_2}^\dagger \\ &= \sum_{n_1=0}^n \binom{n}{n_1} \left(\frac{\gamma_1}{1-\gamma_1}\right)^{n_1} \left(\frac{\gamma_2}{1-\gamma_2}\right)^{n-n_1} \sqrt{\binom{i}{n} \binom{j}{n} (1-\gamma_1)^{i+j} (1-\gamma_2)^{i+j}} \\ &= A_{n,\gamma_1+\gamma_2-\gamma_1\gamma_2} |i\rangle\langle j| A_{n,\gamma_1+\gamma_2-\gamma_1\gamma_2}^\dagger, \end{aligned}$$

from which it follows that $\mathcal{A}_{BS,\frac{1-2\gamma}{1-\gamma}} \circ \mathcal{A}_{BS,\gamma} = \mathcal{A}_{BS,1-\gamma} = \mathcal{A}_{BS,\gamma}^C$. □

Let $s_1 = \sqrt{1-x}$ and $s_2 = \sqrt{1-2y-z}$. For $x, y, z \geq 0$ and $1-2y-z \geq 0$, we define $\mathcal{A}_{x,y,z}$ to be a channel with the Kraus operators

$$\begin{aligned} \mathbf{A}_0 &= |0\rangle\langle 0| + s_1(|1\rangle\langle 1| + |2\rangle\langle 2|) + s_2|3\rangle\langle 3| \\ \mathbf{A}_1 &= \sqrt{x}|0\rangle\langle 1| + \sqrt{y}|2\rangle\langle 3| \\ \mathbf{A}_2 &= \sqrt{x}|0\rangle\langle 2| + \sqrt{y}|1\rangle\langle 3| \\ \mathbf{A}_3 &= \sqrt{z}|0\rangle\langle 3|. \end{aligned} \tag{7}$$

Observe that $\mathcal{A}_{z,0,z} = \mathcal{A}_{z,4}$, and hence the channels $\mathcal{A}_{x,y,z}$ generalize the uniform amplitude damping channels of dimension four.

Define the set

$$\mathfrak{F}_{x,y,z} = \left\{ (x, y, z) \geq 0 : 2y + z < 1, \quad x < \frac{1}{2}, \quad 2z \leq 1 - 2y \left(2 - \frac{x}{1-x} \right) \right\}. \quad (8)$$

Lemma 5.3. *Let $(x, y, z) \in \mathfrak{F}_{x,y,z}$. Then $\mathcal{A}_{x,y,z}$ is a degradable channel with degrading map $\mathcal{A}_{g,h,k}$, where*

$$\begin{aligned} g &= \frac{1-2x}{1-x}, & h &= \frac{gy}{(1-2y-z)} \\ k &= 1-2h - \frac{z}{1-2y-z}. \end{aligned} \quad (9)$$

We supply the proof of Lemma 5.3 in Section C. Our special two-qubit channels are also \mathcal{Z}_2 -covariant, which simplifies the evaluation of their quantum capacities via use of Corollary 4.3 when they are also degradable.

Proposition 5.4. *If the linear map $\mathcal{A}_{x,y,z}$ defined by (7) is a quantum channel, then it is also \mathcal{Z}_2 -covariant.*

Proof. It suffices to show that $\mathcal{A}_{x,y,z}$ is almost-Pauli. This means that we have to show that every Kraus operator of $\mathcal{A}_{x,y,z}$ can be written in the form $\mathbf{K}_i = \mathbf{D}_i \mathbf{P}_i$ where \mathbf{D}_i is diagonal and \mathbf{P}_i is a two-qubit Pauli. We define the vectors $|0\rangle, |1\rangle, |2\rangle, |3\rangle$ to be the two qubit states $|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle$ respectively. One can verify using equations (A.14), (A.15), (A.12), (A.13), (A.11) that a suitable choice of the matrices \mathbf{D}_i and \mathbf{P}_i is given by

$$\begin{aligned} \mathbf{D}_0 &= \sum_{i=0}^3 a_{0,i} |i\rangle \langle i|, & \mathbf{P}_0 &= \mathbf{1} \otimes \mathbf{1} \\ \mathbf{D}_1 &= a_{1,1} |0\rangle \langle 0| - a_{1,2} |2\rangle \langle 2|, & \mathbf{P}_1 &= \mathbf{Z} \otimes \mathbf{X} \\ \mathbf{D}_2 &= a_{2,1} |0\rangle \langle 0| - a_{2,2} |1\rangle \langle 1|, & \mathbf{P}_2 &= \mathbf{X} \otimes \mathbf{Z} \\ \mathbf{D}_3 &= |0\rangle \langle 0|, & \mathbf{P}_3 &= \mathbf{X} \otimes \mathbf{X}. \end{aligned}$$

□

5.2 d -dimensional Depolarizing Channels

The d -dimensional depolarizing channel of depolarizing probability p can be described as a quantum channel that maps an d -dimensional input state to a convex combination of the maximally mixed d -dimensional state and the input state, and is defined as

$$\mathcal{D}_{p,d}(\rho) = \rho \left(1 - p \frac{d^2 - 1}{d^2} \right) + \frac{\mathbb{1}_d}{d} \left(p \frac{d^2 - 1}{d^2} \right) \text{Tr}(\rho).$$

Upper bounds [2, 3, 4, 5, 6] and lower bounds [28, 7, 8, 9] on the quantum capacity of qubit depolarizing channels, the simplest type of depolarizing channels, have been studied. However

these bounds are not tight when the depolarizing probability is in the interval $(0, \frac{1}{4})$. Even less is known about the quantum capacity of higher dimensional depolarizing channels. The goal of this section is to tighten the upper bounds for the quantum capacity of d -dimensional depolarizing channels.

The obvious upper bounds for the quantum capacity of depolarizing channels come from combining Cerf's no-cloning bounds [2] with Smith and Smolin's technique [6]. By Cerf's result, a d -dimensional depolarizing channel of depolarizing probability p is both degradable and anti-degradable when

$$p = \frac{d}{2d+2} \frac{d^2-1}{d^2} = \frac{d^2-1}{2d(d+1)} = \frac{d-1}{2d}. \tag{10}$$

Hence applying Smith and Smolin's technique of degradable extensions [6] immediately gives the upper bound of

$$Q(\mathcal{D}_{p,d}) \leq (\log_2 d) \left(1 - p \frac{2d}{d-1} \right) \tag{11}$$

for depolarizing probability $0 \leq p \leq \frac{2d}{d-1}$. We call this upper bound the no-cloning upper bound for the quantum capacity of the depolarizing channel.

Conversely, an obvious lower bound for the quantum capacity of the d -dimensional depolarizing channel of noise strength p is $\max(0, \log_2 d + (1-p) \log_2(1-p) + p \log_2(\frac{p}{d^2-1}))$, which is the maximum of zero and its coherent information evaluated on the maximally mixed state.

The following theorem gives our upper bound on the quantum capacity of d -dimensional depolarizing channels. We depict our upper bound for the two-qubit case in Figure 1.

Theorem 5.5. For integers d at least two and $0 \leq p \leq \frac{d-1}{2d}$,

$$Q(\mathcal{D}_{p,d}) \leq \text{conv}\left(f_1, f_2; p, \left[0, \frac{d-1}{2d}\right]\right)$$

where

$$f_1(p) = I_{\text{coh}}\left(\mathcal{A}_{\frac{2d}{(d-1)^2}(\sqrt{1-p}-(1-\frac{pd}{2})),d}, \frac{\mathbb{1}}{d}\right)$$

and

$$f_2(p) = \left(1 - p \frac{2d}{d-1}\right) \log_2 d.$$

Remark 5.6. To evaluate the upper bound of the theorem above, note that

$$I_{\text{coh}}\left(\mathcal{A}_{\gamma,d}, \frac{\mathbb{1}}{d}\right) = \eta\left(\frac{1+(d-1)\gamma}{d}\right) + (d-1)\eta\left(\frac{1-\gamma}{d}\right) - \eta\left(1 - \frac{(d-1)\gamma}{d}\right) - (d-1)\eta\left(\frac{\gamma}{d}\right).$$

Proof of Theorem 5.5. The channel $\mathcal{A}_{\gamma,d}$ has exactly one Kraus operator of non-zero trace equal to $1 + (d-1)\sqrt{1-\gamma}$. Hence the complete Clifford-twirl of $\mathcal{A}_{\gamma,d}$ is $\mathcal{D}_{p,d}$, where $1-p = \left(\frac{1+(d-1)\sqrt{1-\gamma}}{d}\right)^2$. The non-negative solution for γ of the preceding equation for feasible values of p and d gives $\gamma = \frac{2d}{(d-1)^2} \left(\sqrt{1-p} - (1-\frac{pd}{2})\right)$ as required. Hence with Theorem 4.1, we have the bound $Q(\mathcal{D}_{p,d}) \leq I_{\text{coh}}(\mathcal{A}_{\gamma,d}, \frac{\mathbb{1}}{d})$. Cerf's no-cloning bound also gives $Q(\mathcal{D}_{p,d}) \leq f_2(p)$. The convexity of upper bounds obtained from degradable extensions then gives the result. \square

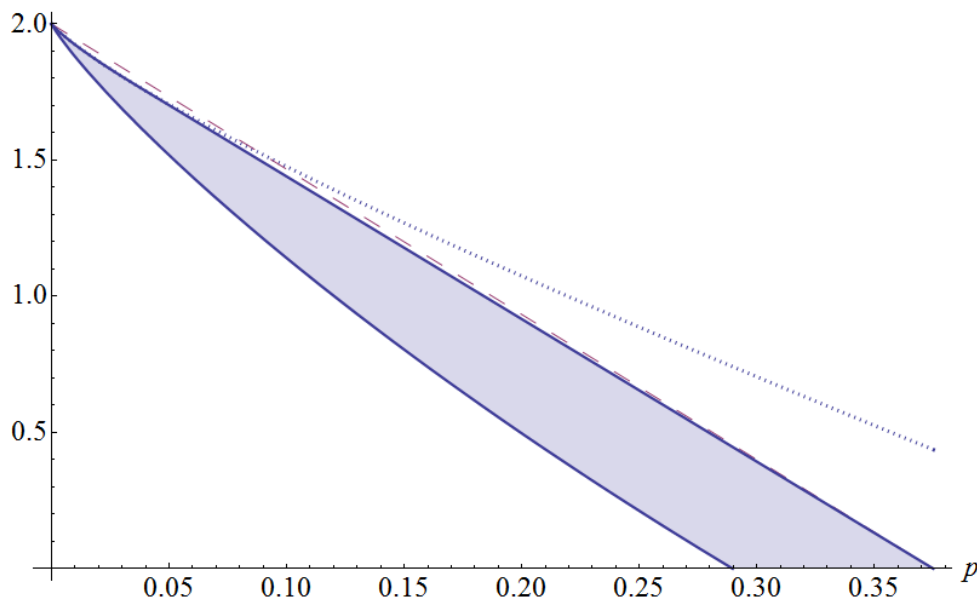


Fig. 1. The upper and lower boundaries of the shaded region depict the upper and lower bounds for $Q(\mathcal{D}_{p,4})$. The dotted line and dashed lines are upper bounds that comes from Cerf’s no-cloning bound and our uniform amplitude damping channel respectively (see Theorem 5.5).

5.3 Two-Qubit Pauli Channels

The tensor product of a pair of qubit Pauli channels is a two-qubit Pauli channel, but conversely a two-qubit Pauli channel need not admit a tensor product decomposition into a pair of qubit Pauli channels. The two-qubit Pauli channels that we study are invariant under the SWAP operation, and local Clifford twirling. We call such channels (q_1, q_2) -channels; these channels apply weight i Paulis from \mathcal{P}_2 with probabilities q_i .

To obtain upper bounds on the quantum capacity of (q_1, q_2) -channels, we first consider the equalities

$$\begin{aligned}
 q_1 &= \frac{(1 - \sqrt{1 - 2y - z})^2}{8} + \frac{(\sqrt{x} + \sqrt{y})^2}{4} \\
 q_2 &= \frac{(1 - 2\sqrt{1 - x} + \sqrt{1 - 2y - z})^2}{16} + \frac{(\sqrt{x} - \sqrt{y})^2}{4} + \frac{z}{4}.
 \end{aligned}
 \tag{12}$$

Theorem 5.7. *Let $q_1 \in [0, 0.2]$ and $q_2 \in [0, 0.3]$. Then the quantum capacity of a (q_1, q_2) -channel is at most $\text{conv}\left(f; (q_1, q_2), [0, 0.2] \times [0, 0.3]\right)$ where $f((q_1, q_2))$ is the infimum of $I_{\text{coh}}(\mathcal{A}_{x,y,z}, \frac{1}{4})$ over the vectors (x, y, z) in $\mathfrak{F}_{x,y,z}$ that satisfy (12).*

Remark 5.8. To evaluate the upper bound in the theorem above, note that

$$\begin{aligned}
 I_{\text{coh}}(\mathcal{A}_{x,y,z}, \frac{1}{4}) &= \eta\left(\frac{1 + 2x + z}{4}\right) + 2\eta\left(\frac{1 - x + y}{4}\right) + \eta\left(\frac{1 - 2y - z}{4}\right) \\
 &\quad - \eta\left(1 - \frac{2x + 2y + z}{4}\right) - 2\eta\left(\frac{x + y}{4}\right) - \eta\left(\frac{z}{4}\right).
 \end{aligned}
 \tag{13}$$

Proof of Theorem 5.7. Let (x, y, z) be a vector in $\mathfrak{F}_{x,y,z}$ that satisfies (12). Then $\mathcal{A}_{x,y,z}$ is a degradable channel (Lemma 5.3), and can be twirled to become a (q_1, q_2) -channel (Proposition D.1). The use of Theorem 4.1 and the convexity of upper bounds obtained from degradable extensions then gives the result. \square

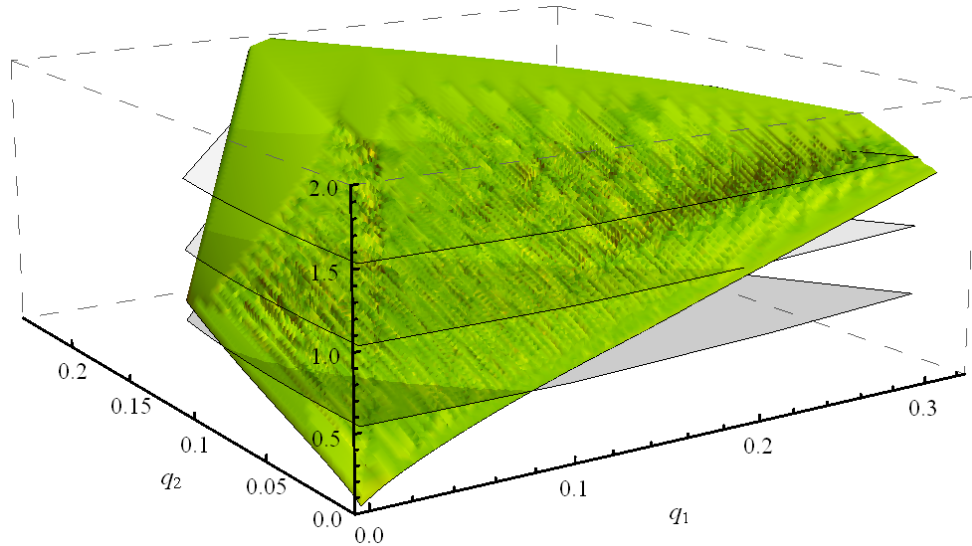


Fig. 2. The concave roof of the depicted dimpled surface is our lower bound of $(2 - Q(\mathcal{N}))$ where \mathcal{N} is a (q_1, q_2) -channel (see Theorem 5.7).

5.4 Shifted Qubit Depolarizing Channels

Various non-unital and non-degradable channels have interesting information theoretic properties [29, 30, 31, 32], and it is natural to obtain upper bounds on their quantum capacities as well. We demonstrate that it is possible to obtain non-trivial upper bounds on the quantum capacity of a special non-unital and non-degradable qubit channel – the shifted qubit depolarizing channel [30, 31].

The shifted depolarizing channel [30, 31] of dimension d is defined by

$$\mathcal{D}_{p,d,\mathbf{A}}(\rho) := \mathcal{D}_{p,d}(\rho) + \mathbf{A} \tag{14}$$

where \mathbf{A} is a d -dimensional Hermitian traceless matrix such that $\mathcal{D}_{p,d,\mathbf{A}}$ is a completely positive map and hence still a quantum channel. Here, the operator \mathbf{A} quantifies the amount by which the depolarizing channel $\mathcal{D}_{p,d}$ is shifted. In the following theorem, we provide explicit upper bounds for the quantum capacity of the shifted qubit depolarizing channel (see also Figure 3). To prove the theorem, we have to perform a specialized twirl on the qubit amplitude damping channel; this twirl is not the Pauli-twirl.

Theorem 5.9. For $0 < p \leq \frac{1}{4}$, let

$$\gamma_1 = \sqrt{16 - 9p} + \frac{9p - 16}{4}$$

and

$$\gamma_2 = 4\sqrt{1-p}(1 - \sqrt{1-p}).$$

Also let

$$g_1(p) = H_2\left(\frac{1-\gamma_2}{2}\right) - H_2\left(\frac{\gamma_2}{2}\right),$$

$g_2(p) = 1 - H_2(p)$, and $g_3(p) = 1 - 4p$. Then for all ϵ in the interval $[0, \gamma_1]$, we have

$$Q(\mathcal{D}_{p,2,\epsilon\mathbf{Z}}) \leq \epsilon\gamma_1^{-1} \max_{q \in [0,1]} \left\{ I_{\text{coh}}(\mathcal{A}_{\gamma_1,2}, \text{diag}(1-q, q)) \right\} + (1 - \epsilon\gamma_1^{-1}) \text{conv}(g_1, g_2, g_3; p, [0, \frac{1}{4}]).$$

Proof. Let \mathcal{U} be the set of unitaries $\{\mathbb{1}, \frac{\mathbf{X}+\mathbf{Z}}{\sqrt{2}}, \frac{\mathbf{Y}+\mathbf{Z}}{\sqrt{2}}\}$. Then the \mathcal{U} -twirl of $\mathcal{A}_{\gamma_1,2}$ is a shifted depolarizing channel, in the sense that

$$\begin{aligned} (\mathcal{A}_{\gamma_1,2})_{\times\mathcal{U}\times}(\mathbb{1}) &= \mathbb{1} + \gamma_1\mathbf{Z} \\ (\mathcal{A}_{\gamma_1,2})_{\times\mathcal{U}\times}(\mathbf{P}) &= \frac{2\sqrt{1-\gamma_1} + (1-\gamma_1)}{3}\mathbf{P} \end{aligned}$$

for all non-trivial Paulis $\mathbf{P} \in \{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$. Thus $(\mathcal{A}_{\gamma_1,2})_{\times\mathcal{U}\times} = \mathcal{D}_{p,2,\gamma_1\mathbf{Z}}$ where

$$p = \frac{4}{3} \left(1 - \frac{2\sqrt{1-\gamma_1} + (1-\gamma_1)}{3} \right).$$

Solving for non-negative γ_1 in terms of $p \in (0, \frac{1}{4}]$, we get $\gamma_1 = \sqrt{16-9p} + \frac{9p-16}{4}$. Hence $\mathcal{D}_{p,2,\epsilon\mathbf{Z}} = \epsilon\gamma_1^{-1}(\mathcal{A}_{\gamma_1,2})_{\times\mathcal{U}\times} + (1 - \epsilon\gamma_1^{-1})\mathcal{D}_{p,2}$. Now $Q((\mathcal{A}_{\gamma_1,2})_{\times\mathcal{U}\times}) \leq I_{\text{coh}}(\mathcal{A}_{\gamma_1,2})$. By the method of degradable extension, $Q(\mathcal{D}_{p,2}) \leq \text{conv}(g_1, g_2, g_3; p, [0, \frac{1}{4}])$ [6], and the result follows from the convexity of the upper bounds. \square

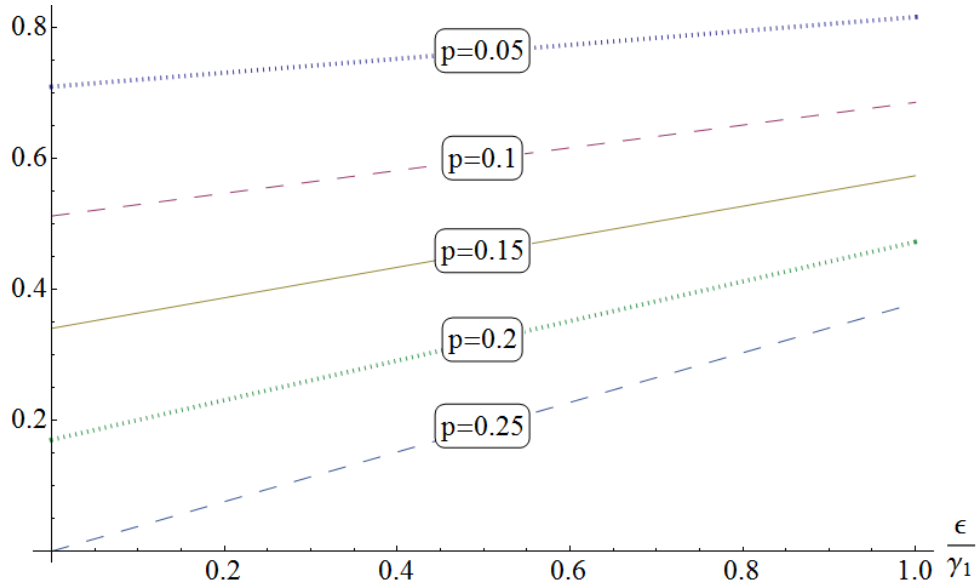


Fig. 3. Upper bounds on $Q(\mathcal{D}_{p,2,\epsilon\mathbf{Z}})$ are depicted for different values of depolarizing probabilities p . Here γ_1 is a function of p as defined in Theorem 5.9.

6 Concluding Remarks

In this paper, we have generalized Smith and Smolin's result (Lemma 8 of [6]) to our Theorem 4.1, thereby upper bounding the quantum capacity of \mathcal{V} -twirled degradable channels by their coherent information maximized on \mathcal{V} -contracted input states. In essence, our main result elucidates a relationship between channel twirling, channel covariance and channel contraction. Additionally, we used our result to provide new upper bounds for the quantum capacity of several families of quantum channels using generalizations of the qubit amplitude damping channels as our ingredients.

Acknowledgements

I thank Debbie Leung, Easwar Magesan, Graeme Smith, Mary Beth Ruskai, Mark Wilde, and the anonymous referees for their helpful comments. I acknowledge support from the Ministry of Education, Singapore.

References

1. M. M. Wilde, *From Classical to Quantum Shannon Theory*. Cambridge University Press, 2013. <http://arxiv.org/abs/1106.1445>.
2. N. J. Cerf, "Quantum cloning and the capacity of the Pauli channel," *Phys. Rev. Lett.*, vol. 84, p. 4497, 2000.
3. E. M. Rains, "Bounds on distillable entanglement," *Phys. Rev. A*, vol. 60, pp. 179–184, 1999.
4. E. M. Rains, "A semidefinite program for distillable entanglement," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2921–2933, 2001.
5. G. Smith, J. A. Smolin, and A. Winter, "The quantum capacity with symmetric side channels," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4208–4217, 2008.
6. G. Smith and J. A. Smolin, "Additive extensions of a quantum channel," *IEEE Information Theory Workshop*, vol. 54, pp. 368 – 372, May 2008.
7. D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum channel capacity of very noisy channels," *Phys. Rev. A*, vol. 57, pp. 830 – 839, 1998.
8. G. Smith and J. A. Smolin, "Degenerate quantum codes for Pauli channels," *Phys. Rev. Lett.*, vol. 98, p. 030501, 2007.
9. J. Fern and K. B. Whaley, "Lower bounds on the nonzero capacity of Pauli channels," *Phys. Rev. A*, vol. 78, p. 062335, 2008.
10. K. Kraus, *Lecture Notes in Physics 190 : States, Effects, and Operations Fundamental Notions of Quantum Theory*. Springer Berlin / Heidelberg, first ed., 1983.
11. I. Devetak and P. W. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Communications in Mathematical Physics*, vol. 256, pp. 287–303, 2005. 10.1007/s00220-005-1317-6.
12. C. King, K. Matsumoto, M. Nathanson, and M. B. Ruskai, "Properties of conjugate channels with applications to additivity and multiplicativity," *Markov Process and Related Fields*, vol. 13, p. 391, 2007.
13. B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Phys. Rev. A*, vol. 54, p. 2629, 1996.
14. S. Lloyd, "The capacity of the noisy quantum channel," *Phys. Rev. A*, vol. 55, p. 1613, 1997.
15. P. Shor, "Lecture notes, MSRI Workshop on Quantum Computation.," 2002.
16. I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, p. 44, 2005.
17. H. Barnum, M. A. Nielsen, and B. Schumacher, "Information transmission through a noisy quantum channel," *Phys. Rev. A*, vol. 57, pp. 4153–4175, Jun 1998.

18. B. Schumacher and M. D. Westmoreland, “Quantum privacy and quantum coherence,” *Phys. Rev. Lett.*, vol. 80, pp. 5695–5697, Jun 1998.
19. A. Holevo, “A note on covariant dynamical semigroups,” *Reports on Mathematical Physics*, vol. 32, no. 2, pp. 211 – 216, 1993.
20. C. Dankert, R. Cleve, J. Emerson, and E. Livine, “Exact and approximate unitary 2-designs and their application to fidelity estimation,” *Phys. Rev. A*, vol. 80, p. 012304, Jul 2009.
21. M. M. Wolf and D. Perez-Garcia, “Quantum capacities of channels with small environment,” *Phys. Rev. A*, vol. 75, p. 012303, 2007.
22. T. S. Cubitt, M. B. Ruskai, and G. Smith, “The structure of degradable quantum channels,” *Journal of Mathematical Physics*, vol. 49, no. 10, 2008.
23. K. Bradler, P. Hayden, D. Touchette, and M. M. Wilde, “Trade-off capacities of the quantum Hadamard channels,” *Phys. Rev. A*, vol. 81, p. 062312, Jun 2010.
24. J. Yard, P. M. Hayden, and I. Devetak, “Capacity theorems for quantum multiple-access channels: Classical-quantum and quantum-quantum capacity regions,” *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3091–3113, 2008.
25. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, second ed., 2000.
26. V. Giovannetti and R. Fazio, “Information-capacity description of spin-chain correlations,” *Phys. Rev. A*, vol. 71, p. 032314, 2005.
27. C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, first ed., 2005.
28. C. Adami and N. J. Cerf, “Von Neumann capacity of noisy quantum channels,” *Phys. Rev. A*, vol. 56, pp. 3470–3483, Nov 1997.
29. M. B. Ruskai, S. Szarek, and E. Werner, “An analysis of completely-positive trace-preserving maps on \mathcal{M}_2 ,” *Linear Algebra and its Applications*, vol. 347, no. 13, pp. 159 – 187, 2002.
30. M. Fukuda, “Extending additivity from symmetric to asymmetric channels,” *J. Phys. A: Math. Gen.*, vol. 38, no. 45, p. L753, 2005.
31. V. Giovannetti, S. Lloyd, and M. B. Ruskai, “Conditions for multiplicativity of maximal ℓ_p -norms of channels for fixed integer p ,” *Journal of Mathematical Physics*, vol. 46, no. 4, p. 042105, 2005.
32. F. Caruso, V. Giovannetti, C. Macchiavello, and M. B. Ruskai, “Qubit channels with small correlations,” *Phys. Rev. A*, vol. 77, p. 052323, May 2008.
33. D. DiVincenzo, D. Leung, and B. Terhal, “Quantum data hiding,” *IEEE Transactions on Information Theory*, vol. 48, pp. 580 –598, Mar 2002.

Appendix

In the appendix, we explain some technical details in greater detail.

Appendix A Matrix Elements in the Pauli-basis

Observe that

$$4|0\rangle\langle 3| = \mathbf{X} \otimes \mathbf{X} - \mathbf{Y} \otimes \mathbf{Y} + i(\mathbf{X} \otimes \mathbf{Y} + \mathbf{Y} \otimes \mathbf{X}) \quad (\text{A.1})$$

$$4|1\rangle\langle 2| = \mathbf{X} \otimes \mathbf{X} + \mathbf{Y} \otimes \mathbf{Y} + i(-\mathbf{X} \otimes \mathbf{Y} + \mathbf{Y} \otimes \mathbf{X}) \quad (\text{A.2})$$

$$4|0\rangle\langle 2| = \mathbf{X} \otimes \mathbf{1} + \mathbf{X} \otimes \mathbf{Z} + i(\mathbf{Y} \otimes \mathbf{1} + \mathbf{Y} \otimes \mathbf{Z}) \quad (\text{A.3})$$

$$4|1\rangle\langle 3| = \mathbf{X} \otimes \mathbf{1} - \mathbf{X} \otimes \mathbf{Z} + i(\mathbf{Y} \otimes \mathbf{1} - \mathbf{Y} \otimes \mathbf{Z}) \quad (\text{A.4})$$

$$4|0\rangle\langle 1| = \mathbf{1} \otimes \mathbf{X} + \mathbf{Z} \otimes \mathbf{X} + i(\mathbf{1} \otimes \mathbf{Y} + \mathbf{Z} \otimes \mathbf{Y}) \quad (\text{A.5})$$

$$4|2\rangle\langle 3| = \mathbf{1} \otimes \mathbf{X} - \mathbf{Z} \otimes \mathbf{X} + i(\mathbf{1} \otimes \mathbf{Y} - \mathbf{Z} \otimes \mathbf{Y}). \quad (\text{A.6})$$

Also

$$4|0\rangle\langle 0| = \mathbf{1} \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{Z} + \mathbf{Z} \otimes \mathbf{1} + \mathbf{Z} \otimes \mathbf{Z} \quad (\text{A.7})$$

$$4|1\rangle\langle 1| = \mathbf{1} \otimes \mathbf{1} - \mathbf{1} \otimes \mathbf{Z} + \mathbf{Z} \otimes \mathbf{1} - \mathbf{Z} \otimes \mathbf{Z} \quad (\text{A.8})$$

$$4|2\rangle\langle 2| = \mathbf{1} \otimes \mathbf{1} + \mathbf{1} \otimes \mathbf{Z} - \mathbf{Z} \otimes \mathbf{1} - \mathbf{Z} \otimes \mathbf{Z} \quad (\text{A.9})$$

$$4|3\rangle\langle 3| = \mathbf{1} \otimes \mathbf{1} - \mathbf{1} \otimes \mathbf{Z} - \mathbf{Z} \otimes \mathbf{1} + \mathbf{Z} \otimes \mathbf{Z}. \quad (\text{A.10})$$

We can also rewrite the above matrices in the following form.

$$|0\rangle\langle 3| = (|0\rangle\langle 0|)(\mathbf{X} \otimes \mathbf{X}) \quad (\text{A.11})$$

$$|0\rangle\langle 2| = (|0\rangle\langle 0|)(\mathbf{X} \otimes \mathbf{Z}) \quad (\text{A.12})$$

$$|1\rangle\langle 3| = (-|1\rangle\langle 1|)(\mathbf{X} \otimes \mathbf{Z}) \quad (\text{A.13})$$

$$|0\rangle\langle 1| = (|0\rangle\langle 0|)(\mathbf{Z} \otimes \mathbf{X}) \quad (\text{A.14})$$

$$|2\rangle\langle 3| = (-|2\rangle\langle 2|)(\mathbf{Z} \otimes \mathbf{X}) \quad (\text{A.15})$$

Appendix B Proof of Proposition 4.2

Let $\mathfrak{K}_{\mathcal{N}}$ denote the Kraus set of the channel \mathcal{N} . Using the canonical definition of the complementary channel of \mathcal{N} from its canonical isometric extension, we have for all $\mathbf{V} \in \mathcal{V}$,

$$\mathcal{N}^C(\mathbf{V}\rho\mathbf{V}^\dagger) = \text{Tr}_{\mathcal{H}_B} \left(\left(\sum_{\mathbf{A}, \mathbf{A}' \in \mathfrak{K}_{\mathcal{N}}} \mathbf{A}\mathbf{V}\rho\mathbf{V}^\dagger\mathbf{A}'^\dagger \right)_{\mathcal{H}_B} \otimes |\mathbf{A}\rangle\langle\mathbf{A}'| \right). \quad (\text{B.1})$$

Similarly, the canonical complementary channel of $\tilde{\mathcal{N}}$ is

$$\begin{aligned} \tilde{\mathcal{N}}^C(\rho) &= \text{Tr}_{\mathcal{H}_B \otimes \mathcal{H}_C} \left(\frac{1}{|\mathcal{V}|} \sum_{\substack{V, V' \in \mathcal{V} \\ A, A' \in \mathfrak{K}_{\mathcal{N}}}} \left(\mathbf{V}^\dagger \mathbf{A} \mathbf{V} \rho \mathbf{V}^\dagger \mathbf{A}'^\dagger \mathbf{V}' \right)_{\mathcal{H}_B} \otimes (|\mathbf{V}\rangle\langle\mathbf{V}'|)_{\mathcal{H}_C} \otimes |\mathbf{A}\rangle\langle\mathbf{A}'| \otimes |\mathbf{V}\rangle\langle\mathbf{V}'| \right) \\ &= \frac{1}{|\mathcal{V}|} \sum_{V \in \mathcal{V}} \text{Tr}_{\mathcal{H}_B} \left(\sum_{A, A' \in \mathfrak{K}_{\mathcal{N}}} \left(\mathbf{V}^\dagger \mathbf{A} \mathbf{V} \rho \mathbf{V}^\dagger \mathbf{A}'^\dagger \mathbf{V} \right)_{\mathcal{H}_B} \otimes |\mathbf{A}\rangle\langle\mathbf{A}'| \right) \otimes |\mathbf{V}\rangle\langle\mathbf{V}| \\ &= \frac{1}{|\mathcal{V}|} \sum_{V \in \mathcal{V}} \mathcal{N}^C(\mathbf{V}\rho\mathbf{V}^\dagger) \otimes |\mathbf{V}\rangle\langle\mathbf{V}| \end{aligned}$$

where we have used the unitary invariance of the partial trace. \square

Appendix C Proof of Lemma 5.3

When $(x, y, z) \in \mathfrak{F}_{x,y,z}$, the map $\mathcal{A}_{x,y,z}$ is a quantum channel and $g, h, k \in [0, 1]$. Hence $\mathcal{A}_{g,h,k}$ is also a quantum channel. Also note that $\mathcal{A}_{x,y,z}^C = \mathcal{A}_{1-x,y,1-2y-z}$.

We now proceed to show that $\mathcal{A}_{g,h,k} \circ \mathcal{A}_{x,y,z} = \mathcal{A}_{x,y,z}^C$ which will imply that $\mathcal{A}_{x,y,z}$ is a degradable channel. We denote the Kraus operators of $\mathcal{A}_{x,y,z}$, $\mathcal{A}_{x,y,z}^C$ and $\mathcal{A}_{g,h,k}$ by \mathbf{A}_i , \mathbf{R}_i

and \mathbf{G}_i respectively, where \mathbf{A}_i is given by (7),

$$\begin{aligned}\mathbf{R}_0 &= |0\rangle\langle 0| + \sqrt{x}|1\rangle\langle 1| + \sqrt{x}|2\rangle\langle 2| + \sqrt{z}|3\rangle\langle 3| \\ \mathbf{R}_1 &= \sqrt{1-x}|0\rangle\langle 1| + \sqrt{y}|2\rangle\langle 3| \\ \mathbf{R}_2 &= \sqrt{1-x}|0\rangle\langle 2| + \sqrt{y}|1\rangle\langle 3| \\ \mathbf{R}_3 &= \sqrt{1-2y-z}|0\rangle\langle 3|,\end{aligned}$$

and

$$\begin{aligned}\mathbf{G}_0 &= |0\rangle\langle 0| + \sqrt{1-g}(|1\rangle\langle 1| + |2\rangle\langle 2|) + \sqrt{1-2h-k}|3\rangle\langle 3| \\ \mathbf{G}_1 &= \sqrt{g}|0\rangle\langle 1| + \sqrt{h}|2\rangle\langle 3| \\ \mathbf{G}_2 &= \sqrt{g}|0\rangle\langle 2| + \sqrt{h}|1\rangle\langle 3| \\ \mathbf{G}_3 &= \sqrt{k}|0\rangle\langle 3|.\end{aligned}$$

By the Kraus representation, $\mathcal{A}_{g,h,k}(\mathcal{A}_{x,y,z}(\rho)) = \sum_{k,\ell \in \{0,1,2,3\}} \mathbf{G}_k \mathbf{A}_\ell \rho \mathbf{A}_\ell^\dagger \mathbf{G}_k^\dagger$. In this representation, the composite quantum channel $\mathcal{A}_{g,h,k} \circ \mathcal{A}_{x,y,z}$ has sixteen Kraus operators $\mathbf{G}_k \mathbf{A}_\ell$ for $k, \ell \in \mathbb{Z}_4$. Now we evaluate $\mathbf{G}_k \mathbf{A}_\ell$ explicitly.

$$\begin{aligned}\mathbf{G}_1 \mathbf{A}_3 &= \mathbf{G}_1 \mathbf{A}_1 = 0, \mathbf{G}_1 \mathbf{A}_2 = \sqrt{\frac{1-2x}{1-x}} y |0\rangle\langle 3| \\ \mathbf{G}_2 \mathbf{A}_3 &= \mathbf{G}_2 \mathbf{A}_2 = 0, \mathbf{G}_2 \mathbf{A}_1 = \sqrt{\frac{1-2x}{1-x}} y |0\rangle\langle 3| \\ \mathbf{G}_3 \mathbf{A}_3 &= \mathbf{G}_3 \mathbf{A}_2 = \mathbf{G}_3 \mathbf{A}_1 = 0.\end{aligned}$$

Also we have

$$\begin{aligned}\mathbf{G}_1 \mathbf{A}_0 &= \sqrt{1-2x}|0\rangle\langle 1| + \sqrt{\frac{1-2x}{1-x}} y |2\rangle\langle 3| \\ \mathbf{G}_2 \mathbf{A}_0 &= \sqrt{1-2x}|0\rangle\langle 2| + \sqrt{\frac{1-2x}{1-x}} y |1\rangle\langle 3| \\ \mathbf{G}_3 \mathbf{A}_0 &= \sqrt{\frac{1-x-2y(2-3x)}{1-x}} |0\rangle\langle 3|.\end{aligned}$$

Moreover

$$\begin{aligned}\mathbf{G}_0 \mathbf{A}_1 &= \sqrt{x}|0\rangle\langle 1| + \sqrt{\frac{xy}{1-x}} |2\rangle\langle 3| \\ \mathbf{G}_0 \mathbf{A}_2 &= \sqrt{x}|0\rangle\langle 2| + \sqrt{\frac{xy}{1-x}} |1\rangle\langle 3| \\ \mathbf{G}_0 \mathbf{A}_3 &= \sqrt{z}|0\rangle\langle 3|.\end{aligned}$$

Observe then that $\mathbf{G}_0 \mathbf{A}_1 = \sqrt{\frac{x}{1-2x}} \mathbf{G}_1 \mathbf{A}_0$ and $\mathbf{G}_0 \mathbf{A}_2 = \sqrt{\frac{x}{1-2x}} \mathbf{G}_2 \mathbf{A}_0$. Thus applying the Kraus operators $\mathbf{G}_i \mathbf{A}_0$ and $\mathbf{G}_0 \mathbf{A}_i$ is equivalent to applying the Kraus operator \mathbf{R}_i for $i \in \{1, 2\}$. Similarly, applying the Kraus operators $\mathbf{G}_1 \mathbf{A}_2, \mathbf{G}_2 \mathbf{A}_1$ and $\mathbf{G}_3 \mathbf{A}_0$ is equivalent to

applying the Kraus operator \mathbf{R}_3 . Moreover, since $1-g = \frac{x}{1-x}$ and $(1-2h-k)(1-2y-z) = z$, we have that $\mathbf{G}_0\mathbf{A}_0 = \mathbf{R}_0$. Hence $\mathcal{A}_{g,h,k} \circ \mathcal{A}_{x,y,z} = \mathcal{A}_{x,y,z}^C$. \square

Appendix D Twirling of Channels

To obtain locally symmetric Pauli channels, we introduce the notion of localized Clifford twirling. Instead of twirling our channel over the entire Clifford group over all the qubits [33], we can twirl the channel with respect to the Clifford group for individual qubits independently. The material below is an explicit discussion on the notion of localized Clifford twirling.

Now define the set of non-trivial Pauli matrices to be $\mathcal{P}_1^* := \{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$. We study a set of automorphisms on the non-trivial Pauli matrices. To define this set of automorphisms, we first define a Hermitian and traceless qubit operator

$$\mathbf{H}_{\tau_1, \tau_2} := \frac{\tau_1 + \tau_2}{\sqrt{2}}$$

for all non-trivial Pauli matrices τ_1 and τ_2 , which is just the Hadamard matrix in an arbitrary Pauli basis. For all non-trivial Pauli matrices \mathbf{W} , conjugation of \mathbf{W} with $\mathbf{H}_{\tau_1, \tau_2}$ gives the following.

$$\mathbf{H}_{\tau_1, \tau_2} \mathbf{W} \mathbf{H}_{\tau_1, \tau_2} = \begin{cases} \tau_1 & , \quad \mathbf{W} = \tau_2 \\ \tau_2 & , \quad \mathbf{W} = \tau_1 \\ -\mathbf{W} & , \quad \mathbf{W} \notin \{\tau_1, \tau_2\} \end{cases}$$

Hence the automorphism associated with the generalized Hadamards $\mathbf{H}_{\tau_1, \tau_2}$ on the set of non-trivial Pauli matrices swaps τ_1 and τ_2 . The size of the set of all automorphisms on the set of non-trivial Pauli matrices is the size of the symmetric group of order 3, which is 6. Hence we consider the set

$$\mathcal{B} := \{\mathbb{1}, \mathbf{H}_{\mathbf{X}, \mathbf{Y}}, \mathbf{H}_{\mathbf{X}, \mathbf{Z}}, \mathbf{H}_{\mathbf{Y}, \mathbf{Z}}, \mathbf{H}_{\mathbf{X}, \mathbf{Z}}\mathbf{H}_{\mathbf{X}, \mathbf{Y}}, \mathbf{H}_{\mathbf{X}, \mathbf{Y}}\mathbf{H}_{\mathbf{X}, \mathbf{Z}}\} \tag{D.1}$$

with six qubit operators, each operator corresponding to a distinct automorphism of the set of non-trivial Pauli matrices. For all $\mathbf{P}, \mathbf{V} \in \mathcal{P}_1$, observe that

$$\frac{1}{6} \sum_{\mathbf{B} \in \mathcal{B}} (\mathbf{B}^\dagger \mathbf{P} \mathbf{B}) \mathbf{V} (\mathbf{B}^\dagger \mathbf{P} \mathbf{B}) = \begin{cases} \frac{1}{3} \sum_{\mathbf{P}' \in \mathcal{P}_1^*} \mathbf{P}' \mathbf{V} \mathbf{P}' & , \quad \mathbf{P} \in \mathcal{P}_1^* \\ \mathbf{V} & , \quad \mathbf{P} = \mathbb{1} \end{cases} . \tag{D.2}$$

Proposition D.1. *Let \mathcal{N} be a two-qubit channel with Kraus set $\mathfrak{K}_{\mathcal{N}}$ and*

$$a_{\mathbf{P} \otimes \mathbf{P}'} = \frac{1}{16} \sum_{\mathbf{K} \in \mathfrak{K}_{\mathcal{N}}} \left| \text{Tr}((\mathbf{P} \otimes \mathbf{P}') \mathbf{K}) \right|^2 .$$

Then $((\mathcal{N}_{\times \mathcal{P}_2 \times})_{\times \mathcal{B} \otimes \mathbb{1} \times})_{\times \mathbb{1} \otimes \mathcal{B} \times}$ is a two-qubit Pauli channel with Kraus operators $\sqrt{a_{\mathbb{1} \otimes \mathbb{1}}} \mathbb{1} \otimes \mathbb{1}$, $\left(\sum_{\mathbf{R} \in \mathcal{P}_1^} \frac{1}{3} a_{\mathbf{R} \otimes \mathbb{1}}\right)^{\frac{1}{2}} \mathbf{R} \otimes \mathbb{1}$, $\left(\sum_{\mathbf{R} \in \mathcal{P}_1^*} \frac{1}{3} a_{\mathbb{1} \otimes \mathbf{R}}\right)^{\frac{1}{2}} \mathbb{1} \otimes \mathbf{R}$, and $\left(\sum_{\mathbf{R}, \mathbf{R}' \in \mathcal{P}_1^*} \frac{1}{9} a_{\mathbf{R} \otimes \mathbf{R}'}\right)^{\frac{1}{2}} \mathbf{R} \otimes \mathbf{R}'$ respectively where $\mathbf{R}, \mathbf{R}' \in \mathcal{P}_1$. Moreover if $\mathcal{N} = \mathcal{A}_{x,y,z}$, then $((\mathcal{N}_{\times \mathcal{P}_2 \times})_{\times \mathcal{B} \otimes \mathbb{1} \times})_{\times \mathbb{1} \otimes \mathcal{B} \times}$ is a (q_1, q_2) -channel with q_1 and q_2 given by (12).*

Proof. Let \mathbf{V} and \mathbf{W} be single qubit Pauli matrices. Then using (D.2) we get

$$\begin{aligned}\mathcal{N}_{\mathcal{B} \otimes \mathbb{1}_l}(\mathbf{V} \otimes \mathbf{W}) &= \frac{1}{6} \sum_{\mathbf{B} \in \mathcal{B}} \sum_{\mathbf{P}, \mathbf{P}' \in \mathcal{P}_1} \mathbf{B}^\dagger \mathbf{P} \mathbf{B} \mathbf{V} \mathbf{B}^\dagger \mathbf{P} \mathbf{B} \otimes \mathbf{P}' \mathbf{W} \mathbf{P}' a_{\mathbf{P} \otimes \mathbf{P}'} \\ &= \frac{1}{6} \sum_{\mathbf{P}, \mathbf{P}' \in \mathcal{P}_1} \left(\sum_{\mathbf{B} \in \mathcal{B}} (\mathbf{B}^\dagger \mathbf{P} \mathbf{B}) \mathbf{V} (\mathbf{B}^\dagger \mathbf{P} \mathbf{B}) \right) \otimes \mathbf{P}' \mathbf{W} \mathbf{P}' a_{\mathbf{P} \otimes \mathbf{P}'} \\ &= \sum_{\mathbf{P}' \in \mathcal{P}_1} \mathbf{V} \otimes \mathbf{P}' \mathbf{W} \mathbf{P}' a_{\mathbb{1} \otimes \mathbf{P}'} + \frac{1}{3} \sum_{\mathbf{P} \in \mathcal{P}_1^*} \left(\sum_{\mathbf{R} \in \mathcal{P}_1^*} \mathbf{R} \mathbf{V} \mathbf{R} \right) \otimes \sum_{\mathbf{P}' \in \mathcal{P}_1} \mathbf{P}' \mathbf{W} \mathbf{P}' a_{\mathbf{P} \otimes \mathbf{P}'}.\end{aligned}$$

By rearranging the terms above, we get

$$\mathcal{N}_{\mathcal{B} \otimes \mathbb{1}_l}(\mathbf{V} \otimes \mathbf{W}) = \mathbf{V} \otimes \sum_{\mathbf{P}' \in \mathcal{P}_1} \mathbf{P}' \mathbf{W} \mathbf{P}' a_{\mathbb{1} \otimes \mathbf{P}'} + \left(\sum_{\mathbf{R} \in \mathcal{P}_1^*} \mathbf{R} \mathbf{V} \mathbf{R} \right) \otimes \sum_{\mathbf{P}' \in \mathcal{P}_1} \mathbf{P}' \mathbf{W} \mathbf{P}' \sum_{\mathbf{P} \in \mathcal{P}_1^*} \frac{a_{\mathbf{P} \otimes \mathbf{P}'}}{3}.$$

Similarly,

$$\begin{aligned}(\mathcal{N}_{\mathcal{B} \otimes \mathbb{1}_l})_{\mathbb{1} \otimes \mathcal{B}_l}(\mathbf{V} \otimes \mathbf{W}) &= \mathbf{V} \otimes \frac{1}{6} \sum_{\mathbf{B} \in \mathcal{B}} \sum_{\mathbf{P}' \in \mathcal{P}_1} (\mathbf{B}^\dagger \mathbf{P}' \mathbf{B}) \mathbf{W} (\mathbf{B}^\dagger \mathbf{P}' \mathbf{B}) a_{\mathbb{1} \otimes \mathbf{P}'} \\ &\quad + \left(\sum_{\mathbf{R} \in \mathcal{P}_1^*} \mathbf{R} \mathbf{V} \mathbf{R} \right) \otimes \frac{1}{6} \sum_{\mathbf{B} \in \mathcal{B}} \sum_{\mathbf{P}' \in \mathcal{P}_1} (\mathbf{B}^\dagger \mathbf{P}' \mathbf{B}) \mathbf{W} (\mathbf{B}^\dagger \mathbf{P}' \mathbf{B}) \left(\sum_{\mathbf{P} \in \mathcal{P}_1^*} \frac{a_{\mathbf{P} \otimes \mathbf{P}'}}{3} \right) \\ &= a_{\mathbb{1} \otimes \mathbb{1}} \mathbf{V} \otimes \mathbf{W} + \mathbf{V} \otimes \left(\sum_{\mathbf{R}' \in \mathcal{P}_1^*} \mathbf{R}' \mathbf{W} \mathbf{R}' \right) \left(\sum_{\mathbf{P}' \in \mathcal{P}_1^*} \frac{a_{\mathbb{1} \otimes \mathbf{P}'}}{3} \right) \\ &\quad + \left(\sum_{\mathbf{R} \in \mathcal{P}_1^*} \mathbf{R} \mathbf{V} \mathbf{R} \right) \otimes \mathbf{W} \left(\sum_{\mathbf{P} \in \mathcal{P}_1^*} \frac{a_{\mathbf{P} \otimes \mathbb{1}}}{3} \right) \\ &\quad + \left(\sum_{\mathbf{R} \in \mathcal{P}_1^*} \mathbf{R} \mathbf{V} \mathbf{R} \right) \otimes \left(\sum_{\mathbf{R}' \in \mathcal{P}_1^*} \mathbf{R}' \mathbf{W} \mathbf{R}' \right) \sum_{\mathbf{P}, \mathbf{P}' \in \mathcal{P}_1^*} \frac{a_{\mathbf{P} \otimes \mathbf{P}'}}{9}.\end{aligned}$$

This completes the first part of the proof.

Now the Pauli-twirl of $\mathcal{A}_{x,y,z}$ has the Kraus operators

$$\begin{aligned}& \left(\frac{1 + 2\sqrt{1-x} + \sqrt{1-2y}}{4} \right) \mathbb{1} \otimes \mathbb{1}, \\ & \left(\frac{1 - \sqrt{1-2y}}{4} \right) \mathbf{P}, & \mathbf{P} \in \{\mathbb{1} \otimes \mathbf{Z}, \mathbf{Z} \otimes \mathbb{1}\} \\ & \left| \frac{1 - 2\sqrt{1-x} + \sqrt{1-2y}}{4} \right| \mathbf{Z} \otimes \mathbf{Z} \\ & \left| \frac{\sqrt{x} + \sqrt{y}}{4} \right| \mathbf{P}, & \mathbf{P} \in \{\mathbb{1} \otimes \mathbf{X}, \mathbb{1} \otimes \mathbf{Y}, \mathbf{X} \otimes \mathbb{1}, \mathbf{Y} \otimes \mathbb{1}\} \\ & \left| \frac{\sqrt{x} - \sqrt{y}}{4} \right| \mathbf{P}, & \mathbf{P} \in \{\mathbf{Z} \otimes \mathbf{X}, \mathbf{Z} \otimes \mathbf{Y}, \mathbf{X} \otimes \mathbf{Z}, \mathbf{Y} \otimes \mathbf{Z}\} \\ & \frac{\sqrt{z}}{2} \mathbf{P}, & \mathbf{P} \in \{\mathbf{X} \otimes \mathbf{X}, \mathbf{X} \otimes \mathbf{Y}, \mathbf{Y} \otimes \mathbf{X}, \mathbf{Y} \otimes \mathbf{Y}\}\end{aligned}$$

and hence combining this with the first result of our proposition, the second result of our proposition follows. \square