Bounding the quantum capacity with flagged extensions

Farzad Kianvash¹, Marco Fanizza^{1,2}, and Vittorio Giovannetti¹

¹NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR, I-56126 Pisa, Italy

²Física Teòrica: Informació i Fenòmens Quàntics, Departament de Física, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona) Spain

In this article we consider flagged extensions of convex combination of quantum channels, and find general sufficient conditions for the degradability of the flagged extension. An immediate application is a bound on the quantum Q and private P capacities of any channel being a mixture of a unitary map and another channel, with the probability associated to the unitary component being larger than 1/2. We then specialize our sufficient conditions to flagged Pauli channels, obtaining a family of upper bounds on quantum and private capacities of Pauli channels. In particular, we establish new state-of-the-art upper bounds on the quantum and private capacities of the depolarizing channel, BB84 channel and generalized amplitude damping channel. Moreover, the flagged construction can be naturally applied to tensor powers of channels with less restricting degradability conditions, suggesting that better upper bounds could be found by considering a larger number of channel uses.

1 Introduction

Protecting quantum states against noise is a fundamental requirement for harnessing the power of quantum computers and technologies. In a transmission line or in a memory, noise is modeled as a quantum channel, and several accesses to the channel together with careful state preparation and decoding can protect quantum information against noise. The quantum capacity Qof a channel is the maximal amount of qubits which can be transmitted reliably, per use of the channel. It can be expressed in terms of an entropic functional, the coherent information I_c , which can be computed as a maximization over quantum states used as inputs of the communication line. The quantum capacity [Llo97; Sho02; Dev05] of a channel can then be obtained as a limit for large n of I_c per use of the channel, for n uses of the channel. A striking feature of the problem is the potential super-additivity of the coherent information [SS96; DSS98; SS07; FW08; SY08; SSY11; Cub+15; LLS18a; BL21; SG21; Sid21; Sid20; NPJ20; Yu+20], which which hinders the direct evaluation of the quantum capacity imposing an infinite number of optimizations on Hilbert spaces of dimension that grows exponentially in n. The existence of an algorithmically feasible evaluation of the quantum capacity remains as one of the most important open problems in quantum Shannon theory [Hol19; Wil17], while finding computable upper or lower bounds on the quantum capacity constitutes important progress.

The phenomenon of superadditivity is not restricted to the quantum capacity, as it shows up also for the classical capacity [Has09], the classical private capacity [Li+09] and the trade-off

Accepted in ()uantum 2021-12-16, click title to verify. Published under CC-BY 4.0.

Farzad Kianvash: farzad.kianvash@sns.it

Marco Fanizza: marco.fanizza@sns.it

capacity region [ZZS17; Zhu+19]. In this paper we are also interested in the classical private capacity, which is the optimal rate for classical communication protected by any eavesdropper [CWY04; Dev05]. In general this capacity is larger than the quantum capacity, but the upper bounds we obtain in this paper hold for both capacities.

Extending previous results, in this work we formulate sufficient conditions to obtain nontrivial upper bounds on the quantum capacity, using the so-called flagged extensions. A flagged extension of a channel that can be written as convex combinations of other channels is such that the receiver gets, together with the output of one of the channels in the convex combination, a flag carrying the information about which of the channels acted. This technique is particularly effective for a class of channels of physical significance, the Pauli channels. A qubit Pauli channel describes random bit flip and phase flip errors, which is a fundamental noise model; moreover, any qubit channel can be mapped to a Pauli channel by a twirling map [HHH99], which does not increase the quantum capacity [BKN00]. With these new flagged extensions we improve the results of [FKG20; Wan21] for two important Pauli channels: the depolarizing channel and BB84 channel, which are both superadditive [SS96; DSS98; BL21], and their quantum capacities are not known, despite a long history of efforts [DSS98; AC97; Bru+98; Rai99; Cer00; Rai01; SS07; FW08; Smi08; SSW08; Ouy11; Sut+17; LDS18; LLS18b; BL21]. We also find new bounds for quantum capacity of the generalized amplitude damping channel [GP+09; BL20; RMG18; KSW20; Wan21], improving the results of [Wan21]. The bounds we obtain are not necessarily the best bounds available with these techniques, being just good guesses among all the instances of flagged channels that satisfy the sufficient conditions. In fact, we obtain an infinite sequence of optimization problem depending on the number of uses of the channel, each of which gives a bound on the capacity. It is not clear if a phenomenon analogous to superadditivity appears in this scenario. Even with one use of the channel, different choices of Kraus operators give different bounds.

These bounds are based on the most fruitful technique to obtain upper bounds on the quantum capacity: finding a degradable extension of the channel (e.g. [Smi08; SSW08; Ouy11; LDS18].) In fact, degradable channels [DS05; CRS08] have the property that the coherent information is additive, therefore the quantum capacity is obtainable as the coherent information of the channel. Moreover, a fundamental property of capacities is that they are generically decreasing under composition of channels, a fact that has a clear operational justification. It is also known that the quantum capacity of a degradable channel is equal to its private capacity, therefore the quantum capacity of the original channel. Moreover, when the channel is also an upper bound for the private capacity of the original channel. Moreover, when the channel is approximately degradable useful bounds can still be obtained [Sut+17; LLS18b].

In a previous paper [FKG20] we contributed to this line of work by considering a flagged degradable extension of the depolarizing channel. While previous constructions [WPG07; Smi08; SSW08; LDS18] used orthogonal flags, our contribution was to consider non-orthogonal flags, showing that degradable extensions can be obtained even in this less restricted setting, obtaining better bounds. In a subsequent work [Wan21] the author combined non-orthogonal flags with approximate degradability, improving the bounds further by searching for the flagged extension with the best bound from approximate degradability. However, from careful inspection it seems that the advantage of the approximate degradability technique in this context is that it finds exactly degradable extensions for a choice of flags that our analysis did not cover. In fact, in the present work we extend the sufficient conditions for degradability for flagged channels and we find even better bounds by exploiting richer flag structures, while being able to reproduce the bounds already obtained with approximate degradability techniques. In principle, the new bounds could be obtained by extending the space of the flags, evaluating the bounds with the approximate degradability method applied to the flagged extension, and minimizing over the

possible flags. Unfortunately, this brute force search with more flags and in a larger Hilbert space for the flags becomes rapidly unpractical.

The outline of the paper is the following: after the preliminaries in Section 2, we show the derivation of the sufficient conditions for degradability of flagged channels in Section 3. We then apply this result to obtain a general bound on the quantum capacity of any channel which is the convex combination of a unitary channel and any other channel in Section 4. In Section 5, we briefly review qudit Pauli channels, then rewrite our sufficient conditions for Pauli channels, where the bounds on the quantum capacity appear to have a simpler form; we also show that two explicit choices of degradable extensions give state-of-the-art bounds for the quantum and private capacities of the depolarizing channel and the BB84 channel. In Section 6, we apply the our method to bound the quantum and private capacity of the generalized amplitude damping channel. In Section 7 we add some observations about the possibility of getting even better bounds with this method. We conclude with a summary of the results.

2 Preliminaries

We consider a finite dimensional Hilbert space \mathcal{H} , and we denote the space of linear operators on \mathcal{H} as $\mathcal{L}(\mathcal{H})$. Then a quantum channel $\Lambda : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is a Completely Positive Trace Preserving (CPTP) map with input system A and output system B. Any CPTP map can be written in Kraus representation

$$\Lambda[\rho] = \sum_{i=1}^{r} K_i \rho K_i^{\dagger} , \qquad (1)$$

for some collection of Kraus operators $\{K_i\}_{i=1,...,r}$ satisfying the normalization condition $\sum_{i=1}^{r} K_i^{\dagger} K_i = I$. Equivalently, we can cast any quantum channel in the Stinespring representation

$$\Lambda[\rho] = \operatorname{Tr}_E[V\rho V^{\dagger}], \qquad (2)$$

where V is an isometry from \mathcal{H}_A to $\mathcal{H}_B \otimes \mathcal{H}_E$, the system E formally acting as the channel environment. For any Stinespring dilation one can define a complementary channel of Λ , that is a channel $\tilde{\Lambda} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_E)$ defined as

$$\tilde{\Lambda}[\rho] = \operatorname{Tr}_B[V\rho V^{\dagger}].$$
(3)

Stinespring dilations and complementary channels are uniquely identified up to an isometry acting on the environment. If there exist a degrading channel W such that $W \circ \Lambda = \tilde{\Lambda}$, we say that Λ is degradable [DS05] (since for a given channel different complementary channels are related by an isometry, the corresponding degrading maps are also related by the same isometry). We call Λ a degradable extension of Λ if Λ is degradable and there exist another channel N such that $N \circ \Lambda = \Lambda$. This is a particular example of a degradable lifting [WY16].

The quantum capacity of a channel $Q(\Lambda)$ is the maximum asymptotic rate at which quantum information can be transmitted reliably using quantum channel Λ . In [Llo97; Sho02; Dev05] it was showed that this quantity can be computed as

$$Q(\Lambda) = \lim_{n \to \infty} \frac{1}{n} Q_n(\Lambda) , \qquad Q_n(\Lambda) = \max_{\rho} I_c(\Lambda^{\otimes n}, \rho) , \qquad (4)$$

where $I_c(\Lambda, \rho) := S(\Lambda(\rho)) - S(\tilde{\Lambda}(\rho))$ is the coherent information functional and $S(\rho) := -\operatorname{Tr}[\rho \log \rho]$ is the von Neumann entropy. Since the number of parameters grows exponentially with n, the maximization over all input states of n uses of channel is computationally demanding. In addition, one also needs to solve the optimization problem for any n in order to use the regularized formula to evaluate the capacity. We also consider the private capacity of a channel $P(\Lambda)$ [CWY04; Dev05], which is the maximum rate of classical communication protected from any eavesdropper. This capacity also has a regularized expression

$$P(\Lambda) = \lim_{n \to \infty} \frac{1}{n} P_n(\Lambda), \qquad P_n(\Lambda) = \max_{\mathcal{E}_n} \{ \chi(\Lambda^{\otimes n}(\mathcal{E}_n)) - \chi(\tilde{\Lambda}^{\otimes n}(\mathcal{E}_n)) \} , \tag{5}$$

where now the maximization has to be performed over all possible ensembles $\mathcal{E}_n := \{p_i, \rho_i\}$ of input states for *n* channel uses $\Lambda^{\otimes n}$, and Holevo information of *n* channel uses is defined as

$$\chi(\Lambda^{\otimes n}(\mathcal{E}_n)) = S(\Lambda^{\otimes n}(\sum_i p_i \rho_i)) - \sum_i p_i S(\Lambda^{\otimes n}(\rho_i)).$$
(6)

In general, $P_n(\Lambda) \ge Q_n(\Lambda)$ and therefore $P(\Lambda) \ge Q(\Lambda)$. Additivity of $P(\Lambda)$ and $Q(\Lambda)$ means

$$Q_n(\Lambda) = nQ_1(\Lambda) = nQ(\Lambda). \qquad P_n(\Lambda) = nP_1(\Lambda) = nP(\Lambda).$$
(7)

In general additivity does not hold. However, for any degradable channel Λ , the coherent information is additive [DS05], and we get a single letter formula for the quantum capacity. Moreover, for degradable channels [Smi08]:

$$P(\Lambda) = Q(\Lambda) = Q_1(\Lambda), \tag{8}$$

therefore any upper bound we find on the quantum capacity via a degradable extension is also an upper bound for the private capacity.

3 Sufficient conditions for degradability of flagged extensions

We outline a systematic construction of degradable flagged extensions for any convex combination of channels, i.e. channels of the form $\Lambda = \sum_{i=0}^{l} p_i \Lambda_i$, with $\{p_i\}_{i=0,\dots l}$ a set of probabilities and with Λ_i channels themselves. We establish the following:

Proposition 3.1 (Sufficient conditions for degradability of flagged extensions). Let Λ be a channel acting on the quantum system A and its flagged extension

$$\mathbb{A} = \sum_{i=0}^{l} p_i \Lambda_i \otimes |\phi_i\rangle \langle \phi_i| , \qquad (9)$$

with $|\phi_i\rangle$ normalized states of an auxiliary system F. The map \wedge is degradable if there exists a choice of Kraus operators $\{K_j^{(i)}\}_{j=1,...,r_i}$ for each channel Λ_i and an orthonormal basis $\{|i\rangle\}_i$ for the space of F, such that

$$\langle i' | \phi_i \rangle \sqrt{p_i} K_{j'}^{(i')} K_j^{(i)} = \langle i | \phi_{i'} \rangle \sqrt{p_{i'}} K_j^{(i)} K_{j'}^{(i')} \qquad \forall i, j, i', j'.$$
(10)

Proof. Observe that starting from a Kraus set $\{K_j^{(i)}\}_{j=1,...,r_i}$ of the channel Λ_i , we can construct the following isometric Stinespring dilation for such channel,

$$V_i |\psi\rangle_A := \sum_{j=1}^{r_i} K_j^{(i)} |\psi\rangle_A |i\rangle_B |j\rangle_{\bar{B}} , \qquad (11)$$

for all $|\psi\rangle_A$ states of A, with the systems B and \overline{B} playing the role of the effective channel environment. A Stinespring representation of the flagged channel (9) can then be obtained as

$$V |\psi\rangle_A := \sum_{i=0}^l \sqrt{p_i} V_i |\psi\rangle_A |\phi_i\rangle_F , \qquad (12)$$

which, via Eq. (3) allows to express the complementary of the flagged channel as

$$\tilde{\mathbb{A}}[|\psi\rangle_A \langle \psi|] = \sum_{i,j} \sqrt{p_i p_j} F_i \langle \phi_j | \phi_i \rangle_F \operatorname{Tr}_A[V_i | \psi\rangle_A \langle \psi| V_j^{\dagger}].$$
(13)

Our goal is to find a channel such as W that degrades the flagged channel to its complementary channel i.e. $W \circ \mathbb{A} = \tilde{\mathbb{A}}$. A natural candidate for the Stinespring representation of the degrading channel is as follows

$$V' |\psi\rangle_A |i\rangle_F := V_i |\psi\rangle_A . \tag{14}$$

Consider hence the following state

$$V'V |\psi\rangle_{A} = \sum_{i=0}^{l} \sqrt{p_{i}} V'V_{i} |\psi\rangle_{A} |\phi_{i}\rangle_{F} = \sum_{i=0}^{l} \sum_{i'=0}^{l} \sqrt{p_{i}} \langle i' |\phi_{i}\rangle V_{i'}V_{i} |\psi\rangle_{A}$$
$$= \sum_{i=0}^{l} \sum_{i'=0}^{l} \sum_{j=1}^{r_{i}} \sum_{j'=1}^{r_{i'}} \langle i' |\phi_{i}\rangle \sqrt{p_{i}} K_{j'}^{(i')} K_{j}^{(i)} |\psi\rangle_{A} |i\rangle_{B} |j\rangle_{\bar{B}} |i'\rangle_{B'} |j'\rangle_{\bar{B}'} , \qquad (15)$$

where for ease of notation $\langle i'|\phi_i\rangle$ stands for $_F\langle i'|\phi_i\rangle_F$. By construction the states of subsystem $B\bar{B}$ and $B'\bar{B}'$ are equal to $\tilde{\mathbb{A}}[|\psi\rangle\langle\psi|]$ and $W \circ \mathbb{A}[|\psi\rangle\langle\psi|]$ respectively. Therefore, a sufficient condition for the degradability of \mathbb{A} is that $V'V |\psi\rangle_A$ is invariant if we swap subsystem $B\bar{B}$ with $B'\bar{B}'$. Writing the swap operator as S_{\leftrightarrow} , we have

$$S_{\leftrightarrow}V'V|\psi\rangle_{A} = \sum_{i=0}^{l}\sum_{i'=0}^{l}\sum_{j=1}^{r_{i}}\sum_{j'=1}^{r_{i'}}\langle i'|\phi_{i}\rangle\sqrt{p_{i}}K_{j'}^{(i')}K_{j}^{(i)}|\psi\rangle_{A}|i\rangle_{B}|j\rangle_{\bar{B}}|i'\rangle_{B'}|j'\rangle_{\bar{B}'}$$

$$= \sum_{i=0}^{l}\sum_{i'=0}^{l}\sum_{j=1}^{r_{i}}\sum_{j'=1}^{r_{i'}}\langle i'|\phi_{i}\rangle\sqrt{p_{i}}K_{j'}^{(i')}K_{j}^{(i)}|\psi\rangle_{A}|i'\rangle_{B}|j'\rangle_{\bar{B}}|i\rangle_{B'}|j\rangle_{\bar{B}'}$$

$$= \sum_{i=0}^{l}\sum_{i'=0}^{l}\sum_{j=1}^{r_{i}}\sum_{j'=1}^{r_{i'}}\langle i|\phi_{i'}\rangle\sqrt{p_{i'}}K_{j}^{(i)}K_{j'}^{(i')}|\psi\rangle_{A}|i\rangle_{B}|j\rangle_{\bar{B}}|i'\rangle_{B'}|j'\rangle_{\bar{B}'},$$

$$= V'V|\psi\rangle_{A},$$
(16)

where we used Eq. (10) in the second equality. Since $S_{\leftrightarrow}V'V |\psi\rangle_A = V'V |\psi\rangle_A$, the flagged channel \wedge is degradable.

In this way we reduced the degradability conditions to commutation conditions on the Kraus operators. In the case that all the Kraus operators commute, we choose all of the flags to be equal to $|\phi_i\rangle = |\phi\rangle = \sum_j \sqrt{p_j} |j\rangle$ to satisfy the degradability conditions, therefore the original channel itself is degradable. In this way we can recover the known fact that channels with commuting Kraus operators are degradable [DS05]. In the case that the Kraus operators of each Λ_i commute with each other i.e. $K_j^{(i)} K_{j'}^{(i)} = K_{j'}^{(i)} K_j^{(i)} \quad \forall j, j', i$, we can choose orthogonal flags $|\phi_i\rangle = |i\rangle$ to construct a degradable extension. However, our proof is not sufficient to recover the known fact that orthogonal flagged convex combination of degradable channels are

degradable. Nonetheless, by allowing in our construction more freedom in the choice of V' we can recover this fact. In particular, one can use $V' |\psi\rangle_A |i\rangle_F = \sum_{j=1}^{r_i} D_j^{(i)} |\psi\rangle_A |i\rangle_{B'} |j\rangle_{\bar{B}'}$, where $D_j^{(i)}$ are the Kraus operators of the complementary of the degrading map of Λ_i . Therefore, allowing arbitrary $D_j^{(i)}$ and checking for equality of partial traces in the systems BB' and $\bar{B}\bar{B}'$ one obtains more general sufficient conditions, covering both the case of Proposition 3.1 and orthogonal flagged convex combination of degradable channels.

4 General applications

4.1 Convex combination of a unitary operation with an arbitrary channel

Consider a channel that is obtained as a convex combination of a unitary mapping induced by the unitary operator U plus an extra CPTP term Λ_1 , i.e.

$$\Lambda[\rho] = (1-p)U\rho U^{\dagger} + p\Lambda_1[\rho] = (1-p)U\rho U^{\dagger} + p\sum_{j=1}^r K_j \rho K_j^{\dagger}, \qquad (17)$$

where $p \in [0, 1]$ and the K_i being a Kraus set of Λ_1 . As the quantum and private capacities are invariant under unitary transformations, in what follow without loss of generality we shall set U as the identity map I, redefining the rest accordingly if necessary. Following the construction of the previous section we hence define the flagged extension (see Eq. (9)) of Λ as

$$\mathbb{A}[\rho] = (1-p)\rho \otimes |\phi_0\rangle \langle \phi_0| + p\Lambda_1[\rho] \otimes |\phi_1\rangle \langle \phi_1| , \qquad (18)$$

for which the degradability conditions in Eq. (10) becomes

$$\langle 1|\phi_0\rangle \sqrt{1-p} = \langle 0|\phi_1\rangle \sqrt{p} , \qquad \langle 1|\phi_1\rangle K_j K_{j'} = \langle 1|\phi_1\rangle K_{j'} K_j .$$
⁽¹⁹⁾

Since K_j operators do not need to commute, we set $\langle 1|\phi_1\rangle = 0$ and if $p \leq 1/2$ we get the following solution

$$|\phi_1\rangle = |0\rangle, \qquad |\phi_0\rangle = \sqrt{\frac{1-2p}{1-p}} |0\rangle + \sqrt{\frac{p}{1-p}} |1\rangle.$$
(20)

Surprisingly, without any assumption on the form of Λ_1 we found a regime for which the channel in Eq. (18) is degradable with non-orthogonal flags. Therefore, we get the following upper bound

$$Q(\Lambda) \le Q(\Lambda) = Q_1(\Lambda).$$
(21)

Note that, in the same regime $p \leq 1/2$, one also has that the extension with orthogonal flags is degradable. Consider indeed a map acting as follows on product states (it can be trivially extended): $W[\rho \otimes |\phi_0\rangle\langle\phi_0|] = \frac{1-2p}{1-p}|0\rangle\langle 0| \otimes |\phi_0\rangle\langle\phi_0| + \frac{p}{1-p}\tilde{\Lambda}_1[\rho] \otimes |\phi_1\rangle\langle\phi_1|, W[\rho \otimes |\phi_1\rangle\langle\phi_1|] =$ $|0\rangle\langle 0| \otimes |\phi_0\rangle\langle\phi_0|$. One can verify that this map is a valid degrading map. However, the extension with non-orthogonal flags has a lower quantum capacity and therefore gives a better upper bound. Note also that one can also consider the family of extensions

$$\mathbb{A}_{c}[\rho] := (1 - c^{2})(1 - p)\rho \otimes |\phi_{0}\rangle \langle \phi_{0}| + \left(c^{2}(1 - p)\rho + p\Lambda_{1}[\rho]\right) \otimes |\phi_{1}\rangle \langle \phi_{1}| , \qquad (22)$$

which according to Eq. (20) are degradable for $|\langle \phi_0 | \phi_1 \rangle|^2 = \frac{1-2(p+c^2-pc^2)}{1-(p+c^2-pc^2)}$, for $0 \le c^2 \le \frac{1-2p}{2(1-p)}$. Each of these extensions gives an upper bound, and the best bound is found by minimization.

$$Q(\Lambda) \le \min_{\substack{0 \le c^2 \le \frac{1-2p}{2(1-p)}}} Q_1(\Lambda_c) \,. \tag{23}$$

Putting $\Lambda_1[\rho] = I/d$, one recovers degradable flagged extension of depolarizing channel. The best previous upper bound for qubit depolarizing channel is given in [Wan21]. In [Wan21], by fixing the structure of the flagged extension as in Eq. (18), the author found the optimal upper bound for the quantum capacity of the qubit depolarizing channel using approximate degradability, and minimizing over flagged extensions. In fact, the best bound with this method is obtained for an exactly degradable extension, and the flags giving the optimal upper bound in [Wan21] are the same that we find analytically in Eq. (19). On the other hand, considering the family of extensions Eq. (22) we can also recover mixed state flags associated to the identity channel, by writing

$$\mathbb{A}_{c}[\rho] = (1-p)\rho \otimes \left((1-c^{2}) |\phi_{0}\rangle \langle \phi_{0}| + c^{2} |\phi_{1}\rangle \langle \phi_{1}| \right) + p\Lambda_{1}[\rho] \otimes |\phi_{1}\rangle \langle \phi_{1}| .$$

$$(24)$$

For $c^2 = \frac{1-2p}{2(1-p)}$, $\langle \phi_0 | \phi_1 \rangle = 0$ and we recover the best bound from [FKG20], obtained with the same flag structure. The minimization over c gives in general some improvement on this class of upper bounds.

Another non-trivial construction is the following: if $K_j = \sqrt{p_j}U_j$ for some unitaries U_j , with $\sum_{i=1}^{r} p_j = 1 - p$, then we can consider the mixed unitary flagged channel,

$$\Lambda[\rho] = (1-p)\rho \otimes |\phi_0\rangle\langle\phi_0| + \sum_{j=1}^r p_j U_j \rho U_j^{\dagger} \otimes |\phi_j\rangle\langle\phi_j| \quad ,$$
(25)

and any flag choice such that

$$\langle i|\phi_i\rangle = 0 \text{ if } i \neq 0 \text{ and } j \neq 0 \text{ and } i \neq j ,$$
 (26)

gives a degradable extension. The best upper bounds we obtain from degradable extensions with more than two flags, for the depolarizing channel and BB84 channel, have exactly this flag structure. However, the degradability conditions are more general than this and we give a more specialized treatment to these channels in the following sections.

Finally, as an extension of the argument presented in Eq. (24), we remark that even general extensions with mixed flags can be considered in this framework, by changing the convex combination considered. For example, a rank two flag can be introduced by splitting a term $K\rho K^{\dagger} \otimes (q |0\rangle\langle 0| + (1-q) |1\rangle\langle 1|) = \sqrt{q}K\rho\sqrt{q}K^{\dagger} \otimes |0\rangle\langle 0| + \sqrt{1-q}K\rho\sqrt{1-q}K^{\dagger} \otimes |1\rangle\langle 1|$, where we now flag a channel with new Kraus operators $\sqrt{q}K$ and $\sqrt{1-q}K$, each with a pure flag associated.

5 Pauli channels

In this section we concentrate on an important subclass of mixed unitary channels, the Pauli channels, which describe random bit flip and phase flip errors in qubits and their generalization to qudits models. For this class of channels the structure of degradable flagged extensions is quite rich and the upper bounds can be made more explicit. The following treatment of generalized Pauli channels follows the phase-space description of finite dimensional quantum mechanics [Woo87; App05; Gro06; GE08; dBe13; GNW21].

5.1 Qubit Pauli group

We start by recalling the Pauli group of one qubit:

$$\mathcal{P} := \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\},\tag{27}$$

where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The Pauli group of n qubits is obtained as the tensor product of n copies of the Pauli group of one qubit $\mathcal{P}^n := \{ \bigotimes_{j=1}^n \omega_j | \omega_j \in \mathcal{P} \}$. For our purposes it suffices to consider $\mathsf{P}^n := \mathcal{P}^n/\mathbb{C}^n$, the quotient of the Pauli group with its center $\mathbb{C}^n := \{ \pm I^{\otimes n}, \pm iI^{\otimes n} \}$. Each element of P^n can be identified by a pair of n bit-strings x = (q, p) according to the definition

$$P_{(q,p)} := i^{-p \cdot q} \otimes_{j=1}^{n} Z^{p_j} X^{q_j}.$$
(28)

It is then immediate to see that for any two x = (q, p), y = (q', p') we have $P_x P_y = (-1)^{\langle x, y \rangle} P_y P_x$, where

$$\langle x, y \rangle = p \cdot q' - q \cdot p' \mod 2$$
, (29)

and that $\operatorname{Tr}[P_x] = 2\delta_{x,0}$.

5.2 Qudit Pauli group

The generalization of the Pauli group for one qudit is the group \mathcal{W}_d generated by τI ($\tau := e^{\frac{(d^2+1)\pi i}{d}}$), and the Weyl-Heisenberg operators X, Z acting as

$$X|j\rangle = |j+1\rangle \mod d, \qquad Z|j\rangle = e^{j\frac{2\pi i}{d}}|j\rangle \qquad j=0,...,d-1.$$
(30)

For several qudits, likewise we set $\mathcal{W}_d^n := \{ \otimes_{j=1}^n \omega_j | \omega_j \in \mathcal{W}_d \}$. The center of this group is still a set of multiples of the identity $C_d^n = \{ \tau^j I^{\otimes n} : j = 0, ..., D-1 \}$, where D = d if d is odd and D = 2d if d is even; we define $\mathbb{W}_d^n := \mathcal{W}_d^n / C_d^n$. Each element of \mathbb{W}_d^n can be identified by a pair of n Dit-strings $x = (q, p) \in \mathbb{Z}_D^{2n}$ according to the definition

$$W_{(q,p)} := e^{-\frac{(d^2+1)\pi i}{d}(p \cdot q)} \otimes_{j=1}^{n} Z^{p_j} X^{q_j}.$$
(31)

By close inspection it holds that

$$W_x W_y = e^{\frac{2\pi i}{d} \langle x, y \rangle} W_y W_x, \qquad (32)$$

where now

$$\langle x, y \rangle = p \cdot q' - q \cdot p' \mod D.$$
 (33)

Moreover, for any $x, z \in \mathbb{Z}_D^{2n}$ we have

$$W_{x+dz} = (-1)^{(d+1)\langle x,z \rangle} W_x,$$
(34)

and $\operatorname{Tr}[W_x] = d^n \delta_{x,0}$.

5.3 Flagged Pauli channels

Each element of W_d^n is a unitary matrix, therefore it describes a reversible evolution of the system of n qudits. Pauli channels are defined as convex combination of Pauli unitaries:

$$\Phi_{\mathbf{w}}[\rho] = \sum_{x \in \mathbb{Z}_d^{2n}} w_x W_x \rho W_x^{\dagger}, \tag{35}$$

where now it suffices to sum over \mathbb{Z}_d^{2n} instead of \mathbb{Z}_D^{2n} because of Eq. (34), and they are parametrically described by the probability distribution $\mathbf{w}(x) = w_x$. For these channels, our sufficient

conditions for degradability are less stringent than in general, because of the relations (32) occurring for any couple of Pauli unitaries. To construct the flagged version of these channels, we note that the flags live, without loss of generality, in a Hilbert space \mathcal{H}_F of dimension d^{2n} , with computational basis $\{|x\rangle\}_{x\in\mathbb{Z}_d^{2n}}$. We also consider the space $\mathcal{H}_C \otimes \mathcal{H}_F$, with \mathcal{H}_C isomorphic to \mathcal{H}_F , and denote the partial trace with respect to \mathcal{H}_C as $\mathrm{Tr}_C[\cdot]$.

Consider a flagged Pauli channel Φ_{Ψ}

$$\Phi_{\Psi}[\rho] = \sum_{x \in \mathbb{Z}_d^{2n}} w_x W_x \rho W_x^{\dagger} \otimes |\phi_x\rangle \langle \phi_x|, \qquad (36)$$

where the label Ψ determines Φ_{Ψ} through the definition of the state $|\Psi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_F$ as

$$|\Psi\rangle = \sum_{x \in \mathbb{Z}_d^{2n}} \sqrt{w_x} \, |x\rangle_C \otimes |\phi_x\rangle_F = \sum_{x \in \mathbb{Z}_d^{2n}, y \in \mathbb{Z}_d^{2n}} \sqrt{w_x} \, \langle y | \phi_x \rangle \, |x\rangle_C \otimes |y\rangle_F \, . \tag{37}$$

We define the projectors Π_j on $\mathcal{H}_C \otimes \mathcal{H}_F$ projecting on span $\{|x\rangle |y\rangle - e^{j\frac{2\pi i}{d}} |y\rangle |x\rangle : \langle x, y\rangle = j \mod d\}$. For a probability vector \mathbf{w} over \mathbb{Z}_d^{2n} , we denote its Shannon entropy as $S(\mathbf{w}) := -\sum_{x \in \mathbb{Z}_d^{2n}} w_x \log w_x$. With these definitions, we are equipped to establish the following proposition:

Proposition 5.1 (Upper bound on the quantum capacity of Pauli channels). Given a Pauli channel $\Phi_{\mathbf{w}}$, for any $|\Psi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_F$ satisfying

$$\operatorname{Tr}[\Pi_j |\Psi\rangle\!\langle\Psi|] = 0 \ \forall j \in \{0, ..., d-1\} \qquad \operatorname{Tr}[(|x\rangle\!\langle x| \otimes I) |\Psi\rangle\!\langle\Psi|] = w_x \qquad \forall x \in \mathbb{Z}_d^{2n}.$$
(38)

the quantum and private capacities of $\Phi_{\mathbf{w}}$ satisfy

$$Q(\Phi_{\mathbf{w}}) \le P(\Phi_{\mathbf{w}}) \le n \log d - S(\mathbf{w}) + S(\operatorname{Tr}_{C}[|\Psi\rangle\!\langle\Psi|]).$$
(39)

In particular, the optimal upper bound is obtained by minimizing $S(\text{Tr}_C[|\Psi\rangle\langle\Psi|])$ with the constraints (38).

Proof. Given a channel of the form (36), consider a state on $\mathcal{H}_C \otimes \mathcal{H}_F$ of the form

Any state $|\Psi\rangle$ on $\mathcal{H}_C \otimes \mathcal{H}_F$ satisfying the second condition in Eq. (38) can be written as

$$|\Psi\rangle = \sum_{x \in \mathbb{Z}_d^{2n}} \sqrt{w_x} |x\rangle_C \otimes |\phi_x\rangle_F = \sum_{x \in \mathbb{Z}_d^{2n}, y \in \mathbb{Z}_d^{2n}} \sqrt{w_x} \langle y | \phi_x \rangle |x\rangle_C \otimes |y\rangle_F,$$
(40)

identifying a flagged extension Φ_{Ψ} of $\Phi_{\mathbf{w}}$. Moreover, the degradability conditions for Φ_{Ψ} can be rewritten as

$$\operatorname{Tr}[\Pi_j |\Psi\rangle\!\langle\Psi|] = 0 \ \forall j \in \{0, ..., d-1\},\tag{41}$$

therefore Φ_{Ψ} is degradable. For flagged degradable Pauli channels, $Q_1 = Q$ has a very simple form. By the covariance property of (flagged) Pauli channels, i.e. $\Phi_{\Psi}[W_x \rho W_x^{\dagger}] =$ $(W_x \otimes I) \Phi_{\Psi}[\rho](W_x^{\dagger} \otimes I)$ for all $W_x \in \mathcal{W}_d^n$. Moreover, we can also write the coherent information as $I_c(\Phi_{\Psi}, \rho) = S(\Phi_{\Psi}[\rho]) - S(\Phi_{\Psi} \otimes \mathcal{I}[|\rho\rangle\rangle\langle\langle\rho|])$, for any purification $|\rho\rangle\rangle$ of ρ and \mathcal{I} identity channel, therefore using unitarily invariance of the von Neumann entropy and covariance we have $I_c(\Phi_{\Psi}, \rho) = I_c(\Phi_{\Psi}, W_x \rho W_x^{\dagger})$. By concavity of coherent information for degradable channels [YHD08], we thus get

$$I_c(\Phi_{\Psi},\rho) = \frac{1}{d^{2n}} \sum_{x \in \mathbb{Z}_d^{2n}} I_c(\Phi_{\Psi}, W_x \rho W_x^{\dagger}) \le I_c(\Phi_{\Psi}, \frac{1}{d^{2n}} \sum_{x \in \mathbb{Z}_d^{2n}} W_x \rho W_x^{\dagger}) = I_c(\Phi_{\Psi}, \frac{I}{d^n}).$$
(42)

Therefore, the maximum of coherent information corresponds to the maximally mixed state, which is purified by the maximally entangled state $|\Xi\rangle = \frac{1}{d^{n/2}} \sum_{j=0,\dots,d-1} |j\rangle \otimes |j\rangle$. It holds that $\langle \Xi | W_x^{\dagger} W_y \otimes I | \Xi \rangle = \frac{1}{d^n} \operatorname{Tr} \left[W_x^{\dagger} W_y \right] = \delta_{x,y}$, therefore

$$Q_{1}(\Phi_{\Psi}) = S\left(\Phi_{\Psi}\left[\frac{I}{d^{n}}\right]\right) - S(\Phi_{\Psi} \otimes I[|\Xi\rangle\langle\Xi|]) = n\log d + S(\sum_{x \in \mathbb{Z}_{d}^{2n}} w_{x} |\phi_{x}\rangle\langle\phi_{x}|) - S(\mathbf{w})$$
$$= n\log d - S(\mathbf{w}) + S(\operatorname{Tr}_{C}[|\Psi\rangle\langle\Psi|]), \tag{43}$$

hence leading to Eq. (39).

Note that the minimization problem suggested by Proposition (5.1) is non-convex, therefore it is hard to treat numerically. Its solution is also not unique in general. However, some useful upper bounds on the quantum capacity can be obtained, case by case, by simply minimizing over families of states which satisfy the constraints, but can be expressed in terms of a few parameters. In this way, we obtain state-of-the art results for the depolarizing channel and the BB84 channel. As a side comment, the treatment in this section does not seem to cover the flag choice of [FKG20; Wan21] for the depolarizing channel. However, this is easily amended by splitting the Kraus operator proportional to the identity in Eq. (35) into two Kraus operators with suitable probabilities, and assigning a different flag to each of them, respecting the sufficient conditions for degradability (see the comments after Eq. (21)).

5.4 Depolarizing channel

The depolarizing channel on one qudit is

$$\Lambda_p^d[\rho] := (1 - \frac{d^2 - 1}{d^2}p)\rho + \frac{p}{d^2} \sum_{x \in \mathbb{Z}_d^2 \setminus \{0\}} W_x \rho W_x^{\dagger} .$$
(44)

The symmetries of this channel causes some potential redundancies in the states that achieve the optimal upper bound according to Proposition (5.1). Consider the unitary operation U_{σ} indexed by permutations $\sigma \in S_{d^2-1}$ which act by permuting the orthogonal set $\{|x\rangle\}_{x\in\mathbb{Z}^2_d\setminus\{0\}}$ while leaving $|0\rangle$ invariant. Then, for any state $|\Psi\rangle$ satisfying the constraints, $U_{\sigma} \otimes U_{\sigma} |\Psi\rangle$ also satisfies the constraints, and it has the same entanglement entropy $S(\text{Tr}_C[|\Psi\rangle\langle\Psi|]) = S(\text{Tr}_C[U_{\sigma} \otimes U_{\sigma} |\Psi\rangle\langle\Psi| (U_{\sigma} \otimes U_{\sigma})^{\dagger}])$. We cannot establish if the minimization problem has a unique solution, but if this was the case, then we could restrict the candidate states to those which are invariant under $U_{\sigma} \otimes U_{\sigma}$ for every $\sigma \in S_{d^2-1}$. We just take this observation as a suggestion for a guess, and we minimize $S(\text{Tr}_C[|\Psi\rangle\langle\Psi|])$ on this restricted family of states. This is convenient because $S(\text{Tr}_C[|\Psi\rangle\langle\Psi|])$ can be determined analytically and we can reduce the problem to a one-parameter minimization.

Proposition 5.2. Any $|\Psi\rangle$ satisfying the constraint Eq. (40) for the map of Eq. (44) and the condition $|\Psi\rangle = U_{\sigma} \otimes U_{\sigma} |\Psi\rangle$ can be parametrized with three complex variables $\alpha = \langle 0, 0 | \Psi \rangle$, $\beta = \langle 0, x | \Psi \rangle$ for $x \neq 0$, $\gamma = \langle x, x | \Psi \rangle$ for $x \neq 0$. Accordingly we can write

$$S(\text{Tr}_C[|\Psi\rangle\!\langle\Psi|]) = -(d^2 - 2)|\gamma|^2 \log(|\gamma|^2) - v_+ \log v_+ - v_- \log v_-,$$
(45)

with

$$v_{\pm} = \frac{1}{2} (|\alpha|^2 + |\gamma|^2 + 2|\beta|^2 (d^2 - 1) \pm \sqrt{(|\alpha|^2 - |\gamma|^2)^2 + 4(d^2 - 1)|\beta|^2 |\alpha + \gamma^*|^2}).$$
(46)

Proof. From the constraints we have that $\beta = \langle 0, x | \Psi \rangle = \langle x, 0 | \Psi \rangle$, and from the action of a permutation U_{xy} that exchanges $x, y \neq 0$ we have $\langle 0, x | U_{xy} \otimes U_{xy} | \Psi \rangle = \langle 0, y | \Psi \rangle$. From the constraints we have that $\langle x, y | \Psi \rangle = e^{-\frac{2\pi i}{d} \langle x, y \rangle} \langle y, x | \Psi \rangle$ for $x \neq y$, $x, y \neq 0$, then $\langle x, y | U_{xy} \otimes U_{xy} | \Psi \rangle = \langle y, x | \Psi \rangle = e^{-\frac{2\pi i}{d} \langle x, y \rangle} \langle y, x | \Psi \rangle = 0$. Also, $\langle x, x | \Psi \rangle = \langle x, x | U_{xy} | \Psi \rangle = \langle y, y | \Psi \rangle = \gamma$ when $x, y \neq 0$. This completes the parametrization. The eigenvalues of $\operatorname{Tr}_C[|\Psi\rangle\langle\Psi|]$ can be determined from the singular values of the matrix M_{xy} of coefficients of $|\Psi\rangle = \sum_{x \in \mathbb{Z}_d^{2n}, y \in \mathbb{Z}_d^{2n}, M_{xy} | x \rangle_C \otimes | y \rangle_F$. We have that the coefficients of $M^{\dagger}M$ are

$$M^{\dagger}M_{0,0} = |\alpha|^2 + |\beta|^2(d^2 - 1) \qquad M^{\dagger}M_{0,x} = \alpha\beta^* + \beta\gamma^*, \ x \neq 0$$
(47)

$$M^{\dagger}M_{x,y} = |\beta|^2, \ x \neq y, \ x, y \neq 0 \qquad M^{\dagger}M_{x,x} = |\beta|^2 + |\gamma|^2, \ x \neq 0.$$
(48)

Then $M^{\dagger}M - |\gamma|^2 I$ has rank 2 and the nonzero eigenvalues can be determined by solving a quadratic equation.

Proposition 5.3. For $|\Psi\rangle$ satisfying $|\Psi\rangle = U_{\sigma} \otimes U_{\sigma} |\Psi\rangle$, the minimization of $S(\text{Tr}_{C}[|\Psi\rangle\langle\Psi|])$ is a one-parameter minimization problem.

Proof. From the expression of $S(\text{Tr}_C[|\Psi\rangle\langle\Psi|])$ in Eq. (45) and from Eq. (46) it's evident that the result does not depend on the phases of α , β and γ except for the term $|\alpha + \gamma^*|$, which should be maximized. This happens without loss of generality if α and γ^* are real and positive. Then the two constraints $|\alpha|^2 + (d^2 - 1)|\beta|^2 = (1 - \frac{d^2 - 1}{d^2}p)$ and $|\beta|^2 + |\gamma|^2 = \frac{p}{d^2}$ eliminate the remaining two parameters, with the constraint that γ is such that $|\alpha|, |\beta|, |\gamma| < 1$.

Summarizing, from Proposition 5.1 and 5.2 we obtain

$$Q(\Lambda_p^d) \le P(\Lambda_p^d) \le \log d - S(\mathbf{w}) + S(\operatorname{Tr}_C[|\Psi\rangle\langle\Psi|])$$

= $\log d - \left(1 - \frac{d^2 - 1}{d^2}p\right) \log \left(1 - \frac{d^2 - 1}{d^2}p\right) - \frac{p(d^2 - 1)}{d^2} \log \frac{p}{d^2}$
 $- (d^2 - 2)|\gamma|^2 \log(|\gamma|^2) - v_+(|\gamma|^2) \log v_+(|\gamma|^2) - v_-(|\gamma|^2) \log v_-(|\gamma|^2),$ (49)

where the allowed values of γ and the dependence on γ of $v_+(|\gamma|^2)$ and $v_-(|\gamma|^2)$ are obtained as in the argument of Proposition 5.3, i.e.

$$v_{\pm}(x) = \frac{1}{2} \left(1 - (d^2 - 2)x \right) \pm \frac{1}{2} \left\{ \left(1 - 2\frac{d^2 - 1}{d^2}p + (d^2 - 2)x \right)^2 + 4(d^2 - 1) \left(\frac{p}{d^2} - x \right) \left(xd^2 + 2\sqrt{x}\sqrt{x(d^2 - 1) - 2\frac{p(d^2 - 1)}{d^2} + 1} - 2\frac{p(d^2 - 1)}{d^2} + 1 \right) \right\}^{1/2}.$$
(50)

The bound Q_{fmin} obtained from this one-parameter minimization can be combined with the no-cloning bound [Bru+98; Cer00; Smi08; Ouy11]

$$Q(\Lambda_p^d) \le \left(1 - \frac{2p(d+1)}{d}\right) \log d \,. \tag{51}$$

using the fact that the convex hull of upper bounds from degradable extensions of the depolarizing channel is itself an upper bound [Smi08; Ouy11]. A comparison between the most competitive upper bounds for d = 2 is shown in Figure 1, where we can see that the bound



Figure 1: Bounds on the quantum capacity of the depolarizing channel for d = 2. Here Q_{conv} is the convex hull of the available upper bounds from degradable extensions, Q_{fmin} is the new upper bound, obtained from Eq. (39) by plugging in the expression Eq. (45) and minimizing over γ , eliminating the other parameters as explained in the proof of Proposition 5.3. Q_1 is the lower bound given by the coherent information of one use of the channel. Q_{LDS} is the bound from [LDS18] and Q_W is the bound from [Wan21].

we obtained outperforms all previous bounds in the whole parameter region. An improvement with respect to previous bounds can be obtained also for generic d, and we show as an example the bound for d = 4 in Figure 2. In this latter case, the bound from the convex hull is improved considering also the bound from Eq. (23).

5.5 BB84 channel

In this section we consider the channel that describes the famous quantum key distribution protocol by Bennett and Brassard [BB14]. In its general form the channel is

$$B_{p_X,p_Z}[\rho] = (1 - p_X - p_Z + p_X p_Z)\rho + (p_X - p_X p_Z)X\rho X + (p_Z - p_Z p_X)Z\rho Z + p_X p_Z Y\rho Y,$$
(52)

As in [Sut+17] and [Wan21] we restrict to the case $p_X = p_Z = p$. The flagged extension we consider is

$$B_{p,\Psi}[\rho] = (1-p)^2 \rho \otimes |\phi_0\rangle\langle\phi_0| + p(1-p)X\rho X \otimes |\phi_1\rangle\langle\phi_1| + p(1-p)Z\rho Z \otimes |\phi_2\rangle\langle\phi_2| + p^2 Y\rho Y \otimes |\phi_3\rangle\langle\phi_3| .$$
(53)



Figure 2: Bounds on the quantum capacity of the depolarizing channel for d = 4. Here Q_{conv} is the convex hull of the available upper bounds from degradable extensions, Q_{fmin} is the new upper bound, and Q_1 is the lower bound given by the coherent information of one use of the channel. Q_{FKG} is the bound from [FKG20] and Q_{OU} is the bound from [Ouy11]. Note that in the main plot Q_{fmin} is the bound in Eq. (23), since at scale used the bound with more flags is not noticeably better; the situation is different for very small p, in the regime plotted in the inset: here we report Q_{conv} obtained from Eq. (39) by plugging in the expression Eq. (45) and minimizing over γ , eliminating the other parameters as explained in the proof of Proposition 5.3 (see Eq. (49) and Eq. (50)).



Figure 3: Bounds on the quantum and private capacity of BB84 channel. Q_1 is the coherent information of BB84 channel. Q_{fmin} is the new upper bound obtained by the degradable extension, from Eq. (39), using the parametrization for the flags in Eq. (54), for a suitable choice of the parameters. Q_W is the upper bound obtained in [Wan21]. Q_{SS} is the upper bound derived in [Smi08].

We choose the following parametrization for the flags

$$\begin{aligned} |\phi_0\rangle &= \sqrt{1 - 2\alpha^2 - \beta^2} |0\rangle + \alpha |1\rangle + \alpha |2\rangle + \beta |3\rangle \\ |\phi_1\rangle &= a |0\rangle + \sqrt{1 - a^2 - \gamma^2} |1\rangle - \gamma |3\rangle \\ |\phi_2\rangle &= a |0\rangle + \sqrt{1 - a^2 - \gamma^2} |2\rangle - \gamma |3\rangle \\ |\phi_3\rangle &= b |0\rangle + c |1\rangle + c |2\rangle + \sqrt{1 - b^2 - 2c^2} |3\rangle , \end{aligned}$$
(54)

where we impose the parameters $\alpha, \beta, \gamma, a, b, c$ to be real and satisfying the normalization conditions for the vectors in Eq. (54). The degradability conditions in Eq. (10) imply that $\alpha = a \sqrt{\frac{p(1-p)}{(1-p)^2}}, \beta = \frac{bp}{1-p}$ and $\gamma = c \sqrt{\frac{p}{1-p}}$. This is not the most general parametrization for the flags, however, because of the symmetry between the bit flip and phase flip error in Eq. (52), we chose this parametrization. Any set of flags in the form of Eq. (54) will result in a degradable extension of BB84 channel. Therefore, to get the best upper bound for the quantum capacity or private capacity of BB84 we should minimize the coherent information of its flagged channel with respect to three free parameters a, b, c. We have compared the result of the optimization with the previous bounds in Figure 3. The bound in [Wan21] by Wang can be reproduced in our framework just by choosing a = b = 1, c = 0.

6 Generalized amplitude damping

In this section we consider a bound on the quantum capacity of the generalized amplitude damping channel, which is a model of thermal loss on a qubit, relevant for quantum superconducting processors [CB08]. The generalized amplitude damping channel can be written as

$$\mathcal{A}_{y,N}[\rho] = N \,\mathcal{A}_{y}[\rho] + (1-N) \,X \circ \mathcal{A}_{y} \circ X[\rho], \tag{55}$$

where $\mathcal{A}_{y,N}$ is the conventional amplitude damping channel, with Kraus operators $K_1 = (|0\rangle\langle 0| + \sqrt{1-y} |1\rangle\langle 1|)$ and $K_2 = \sqrt{y} |1\rangle\langle 0|$. While \mathcal{A}_y , and $X \circ \mathcal{A}_y \circ X$ are degradable and their quantum capacity can be computed [GF05], their convex combination is not, and its quantum capacity is not determined. Previous upper bounds have been obtained by [RMG18; KSW20; GP+09; Wan21]. In particular [Wan21] used the following flagged extension together with approximate degradability to get the tightest bound available:

$$\mathcal{A}_{y,N}^{F}[\rho] = N \,\mathcal{A}_{y}[\rho] \otimes |0\rangle\langle 0| + (1-N) \,X \circ \mathcal{A}_{y} \circ X[\rho] \otimes |1\rangle\langle 1| \,, \tag{56}$$

In fact this extension is exactly degradable: the output of a complementary channel is

$$\tilde{\mathcal{A}}_{y,N}^{F}[\rho] = N \,\tilde{\mathcal{A}}_{y}[\rho] \otimes |0\rangle\!\langle 0| + (1-N) \, X \circ \tilde{\mathcal{A}}_{y} \circ X[\rho] \otimes |1\rangle\!\langle 1| \,, \tag{57}$$

and if the degrading map of A_y is W_y , we have $\tilde{\mathcal{A}}_{y,N}^F[\rho] = (W_y \otimes |0\rangle \langle 0| + X \circ W_y \circ X \otimes |1\rangle \langle 1|) \circ \mathcal{A}_{y,N}^F[\rho]$. The quantum capacity of this extension can be evaluated to be $Q(\mathcal{A}_{y,N}^F) \leq (1-N)I_c(A_y,\rho) + NI_c(X \circ A_y \circ X, \rho) = Q(A_y)$. This simple bound seem to not have been pointed out previously, and the actual quantum capacity $Q(\mathcal{A}_{y,N}^F)$ is very close to it. Moreover, the structure of the generalized amplitude damping is such that one can get better bounds from different degradable extensions, where we adapt the argument by [Smi08] on the depolarizing channel:

Proposition 6.1 (Combining bounds of degradable extensions of generalized amplitude damping). For any collection of degradable extensions $\mathcal{A}_{y,N}^{ext,i}$, i = 1, ..., l, for any y_0 the quantum capacity of $\mathcal{A}_{y_0,N}$ is upper bounded by the convex hull of $Q(\mathcal{A}_{y_0,N}^{ext,i})$, i = 1, ..., l, as functions of the variable N.

Proof. For any N_1, N_2 such that $N = qN_1 + (1-q)N_2$, $1 - N = 1 - qN_1 + (1-q)N_2 = q(1-N_1) + (1-q)(1-N_2)$, we have

$$\mathcal{A}_{y,N}[\rho] = q(N_1 \mathcal{A}_y[\rho] + (1 - N_1) X \circ \mathcal{A}_y \circ X[\rho]) + (1 - q)(N_2 \mathcal{A}_y[\rho] + (1 - N_2) X \circ \mathcal{A}_y \circ X[\rho])$$
(58)

If $\mathcal{A}_{y,N_1}^{ext,i}$ and $\mathcal{A}_{y,N_2}^{ext,j}$ are degradable extensions of \mathcal{A}_{y,N_1} and \mathcal{A}_{y,N_2} respectively, then $q\mathcal{A}_{y,N_1}^{ext,i} \otimes |0\rangle\langle 0| + (1-q)\mathcal{A}_{y,N_2}^{ext,j} \otimes |1\rangle\langle 1|$ is a degradable extension of $\mathcal{A}_{y,N}$ with quantum capacity less than $qQ(\mathcal{A}_{y,N_1}^{ext,i}) + (1-q)Q(\mathcal{A}_{y,N_2}^{ext,j})$.

In addition to the extension proposed by [Wan21], we find two other degradable extensions using the results of this paper. The first is obtained observing that the following set is also a good choice of Kraus operators

$$A_{1} = \sqrt{N(1-N)}(\sqrt{1-y} + 1)(|0\rangle\langle 0| + |1\rangle\langle 1|) = \sqrt{N(1-N)}(\sqrt{1-y} + 1)I$$
(59)

$$A_2 = \sqrt{(1-N)y} \left| 1 \right\rangle \! \left\langle 0 \right| \tag{60}$$

$$A_3 = ((1-N) - N\sqrt{1-y}) |0\rangle\langle 0| + ((1-N)\sqrt{1-y} - N) |1\rangle\langle 1|$$
(61)

$$A_4 = \sqrt{Ny} \left| 0 \right\rangle \! \left\langle 1 \right| \tag{62}$$

We notice that A_1 is a rescaled unitary operator, therefore we can directly apply the bound of Eq. (21) with $(1-p) = N(1-N)(\sqrt{1-y}+1)^2$. This bound is applicable if $N(1-N)(\sqrt{1-y}+1)^2 > 1/2$. Moreover, at N = 1/2, the generalized amplitude damping becomes a Pauli channel:

$$\mathcal{A}_{y,0.5}(\rho) = \frac{1 - y/2 + \sqrt{1 - y}}{2}\rho + \frac{1 - y/2 - \sqrt{1 - y}}{2}Z\rho Z + \frac{y}{4}(Y\rho Y + X\rho X)$$
(63)

and we get a more refined bound $Q_{\text{fmin}}(y)$, using the techniques of the previous sections, in particular with the same flag structure of BB84 Eq. (54). Putting all together, we observe that the bound by [Wan21] remains the best one at high y, but at low y it is beaten by the following bound allowed by the convex hull argument:

$$Q_{\text{conv}}(y,N) = 2NQ_{\text{fmin}}(y) + (1-2N)Q(\mathcal{A}_y)$$
(64)

and using the full convex hull bound does not give substantial improvements. We plot the results in Figure 4.

7 Discussion

In the examples we provided we did not try to numerically optimize in the whole parameter region allowed by the sufficient conditions for degradability. Indeed, the minimization of the upper bound is not a convex optimization problem and would require brute force search, but there are already many parameters for Pauli channels and d = 2, n = 1. However, we stress the fact that the family of upper bounds for the quantum and private capacity of a channel Λ is even larger in principle, as one can consider the flagged extension of $\Lambda^{\otimes k}$: a degradable flagged extension of Λ gives also a degradable flagged extension of $\Lambda^{\otimes k}$ but the converse is not true. We tried to search for a better upper bound of the quantum capacity of the depolarizing channel with two uses, by restricting brute force search to certain parametrizations of the flags, but the attempts we made did not show anything better than the k = 1 bound. It is desirable to further investigate if k = 1 gives already the best upper bound or a phenomenon similar to superadditivity shows up for flagged extensions. Moreover, the extensions we obtained are explicitly dependent on the Kraus representation chosen, which is not unique. We did not find a way to identify an optimal choice of Kraus operators. Since for any channel the number of Kraus operators can be increased arbitrarily by a suitable isometry, it is conceivable that one needs to look at an unbounded space of flags to optimize the upper bound of degradable extensions. As a side note, we point out that the mixed flags extensions as considered in [FKG20] can be treated in the formalism of this paper, just by splitting the Kraus operators into Kraus operators with proper probabilities.

8 Conclusions

We have introduced a method to construct degradable extension of quantum channels which can be written as the convex sum of other channels. This method is of general applicability, and we showed that it gives state-of-the-art upper bounds on the quantum and private capacity of two important Pauli channels, the depolarizing channel and the BB84 channel, and of the generalized amplitude damping channel. By virtue of its simplicity, we believe it can be used with success for many other channels too. The method could in principle give better bounds by considering different Kraus representations and flagged extensions of several uses of a channel, and it would be interesting to study its limitations.

Note added: after the initial submission of this paper, the authors have also obtained upper bounds for the quantum and private capacities of phase-insensitive Gaussian channels, using an extension of the technique proposed here [FKG21].



Figure 4: Bounds on the quantum capacity of the generalized amplitude damping, for three values of N. Q_1 is the lower bound given by the coherent information of one use of the generalized amplitude damping (see also lower bounds from [BL20], which give improvements mildly visible at this scale). $Q_{\rm conv}$ is the new upper bound from Eq. (64), Q_W is the upper bound obtained by Wang [Wan21], Q_{DP} and Q_R are obtained in [KSW20] respectively from data-processing and Rains information. Previous upper bounds [RMG18; GP+09] are worse and not plotted.

Acknowledgments

We thank Felix Leditzky, Matteo Rosati and Xin Wang for valuable comments. The authors acknowledge support by MIUR via PRIN 2017 (Progetto di Ricerca di Interesse Nazionale): project QUSHIP (2017SRNBRK).

References

- [AC97] C. Adami and N. J. Cerf. "von Neumann capacity of noisy quantum channels". In: *Physical Review A* 56.5 (1997), pp. 3470–3483. DOI: 10.1103/PhysRevA.56.3470. arXiv: quant-ph/9609024.
- [App05] D. M. Appleby. "Symmetric informationally complete-positive operator valued measures and the extended Clifford group". In: Journal of Mathematical Physics 46.5 (2005), p. 052107. DOI: 10.1063/1.1896384. arXiv: quant-ph/0412001.
- [BB14] Charles H Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theor. Comput. Sci.* 560.P1 (2014), pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025. arXiv: arXiv:2003.06557.
- [BKN00] H. Barnum, E. Knill, and M.A. Nielsen. "On quantum fidelities and channel capacities". In: *IEEE Transactions on Information Theory* 46.4 (2000), pp. 1317–1329. DOI: 10.1109/18.850671. arXiv: quant-ph/9809010.
- [BL20] Johannes Bausch and Felix Leditzky. "Quantum codes from neural networks". In: New Journal of Physics 22.2 (2020), p. 023005. DOI: 10.1088/1367-2630/ab6cdd. arXiv: 1806.08781.
- [BL21] Johannes Bausch and Felix Leditzky. "Error thresholds for arbitrary pauli noise". In: *SIAM Journal on Computing* 50.4 (2021), pp. 1410–1460. DOI: 10.1137/20M1337375. arXiv: 1910.00471.
- [Bru+98] Dagmar Bruß, David P. DiVincenzo, Artur Ekert, Christopher A. Fuchs, Chiara Macchiavello, and John A. Smolin. "Optimal universal and state-dependent quantum cloning". In: *Physical Review A* 57.4 (1998), pp. 2368–2378. DOI: 10.1103/Phys-RevA.57.2368. arXiv: quant-ph/9705038.
- [CB08] Luca Chirolli and Guido Burkard. "Decoherence in solid-state qubits". In: Advances in Physics 57.3 (2008), pp. 225–285. DOI: 10.1080/00018730802218067. arXiv: 0809. 4716.
- [Cer00] Nicolas J. Cerf. "Pauli Cloning of a Quantum Bit". In: Physical Review Letters 84.19 (2000), pp. 4497–4500. DOI: 10.1103/PhysRevLett.84.4497. arXiv: quant – ph/9803058.
- [CRS08] Toby S. Cubitt, Mary Beth Ruskai, and Graeme Smith. "The structure of degradable quantum channels". In: *Journal of Mathematical Physics* 49.10 (2008). DOI: 10.1063/1.2953685. arXiv: 0802.1360.
- [Cub+15] Toby Cubitt, David Elkouss, William Matthews, Maris Ozols, David Pérez-García, and Sergii Strelchuk. "Unbounded number of channel uses may be required to detect quantum capacity". In: *Nature Communications* 6.1 (2015), p. 6739. DOI: 10.1038/ncomms7739. arXiv: 1408.5115.
- [CWY04] N. Cai, A. Winter, and R. W. Yeung. "Quantum privacy and quantum wiretap channels". In: *Problems of Information Transmission* 40.4 (2004), pp. 318–336. DOI: 10.1007/s11122-005-0002-x.

- [dBe13] Niel de Beaudrap. "A linearized stabilizer formalism for systems of finite dimension". In: Quantum Information and Computation 13.1-2 (2013). DOI: 10.26421/qic13.1-2-6.
- [Dev05] Igor Devetak. "The Private Classical Capacity and Quantum Capacity of a Quantum Channel". In: *IEEE Transactions on Information Theory* 51.1 (2005), pp. 44–55. DOI: 10.1109/TIT.2004.839515. arXiv: quant-ph/0304127.
- [DS05] I. Devetak and P. W. Shor. "The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information". In: Communications in Mathematical Physics 256.2 (2005), pp. 287–303. DOI: 10.1007/s00220-005-1317-6. arXiv: quant-ph/0311131.
- [DSS98] David P. DiVincenzo, Peter W. Shor, and John A. Smolin. "Quantum-channel capacity of very noisy channels". In: *Physical Review A* 57.2 (1998), pp. 830–839. DOI: 10.1103/PhysRevA.57.830. arXiv: quant-ph/9706061.
- [FKG20] Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. "Quantum Flags and New Bounds on the Quantum Capacity of the Depolarizing Channel". In: *Physi*cal Review Letters 125.2 (2020), p. 020503. DOI: 10.1103/PhysRevLett.125.020503. arXiv: 1911.01977.
- [FKG21] Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. "Estimating Quantum and Private Capacities of Gaussian Channels via Degradable Extensions". In: *Physical Review Letters* 127.21 (2021), p. 210501. DOI: 10.1103/PhysRevLett.127.210501. arXiv: 2103.09569.
- [FW08] Jesse Fern and K. Birgitta Whaley. "Lower bounds on the nonzero capacity of Pauli channels". In: *Physical Review A* 78.6 (2008), p. 062335. DOI: 10.1103/Phys-RevA.78.062335. arXiv: 0708.1597.
- [GE08] D. Gross and J. Eisert. "Quantum margulis expanders". In: Quantum Information and Computation 8.8-9 (2008), pp. 0722–0733. DOI: 10.26421/qic8.8-9-3. arXiv: 07 10.0651.
- [GF05] Vittorio Giovannetti and Rosario Fazio. "Information-capacity description of spinchain correlations". In: *Physical Review A* 71.3 (2005), p. 032314. DOI: 10.1103/Phys-RevA.71.032314. arXiv: quant-ph/0405110.
- [GNW21] David Gross, Sepehr Nezami, and Michael Walter. "Schur–Weyl Duality for the Clifford Group with Applications: Property Testing, a Robust Hudson Theorem, and de Finetti Representations". In: Communications in Mathematical Physics 385.3 (2021), pp. 1325–1393. DOI: 10.1007/s00220-021-04118-7. arXiv: 1712.08628.
- [GP+09] Raúl García-Patrón, Stefano Pirandola, Seth Lloyd, and Jeffrey H. Shapiro. "Reverse coherent information". In: *Physical Review Letters* 102.21 (2009), p. 210501.
 DOI: 10.1103/PhysRevLett.102.210501. arXiv: arXiv:0808.0210.
- [Gro06] D. Gross. "Hudson's theorem for finite-dimensional quantum systems". In: Journal of Mathematical Physics 47.12 (2006), p. 122107. DOI: 10.1063/1.2393152. arXiv: quant-ph/0602001.
- [Has09] M. B. Hastings. "Superadditivity of communication capacity using entangled inputs". In: *Nature Physics* 5.4 (2009), pp. 255–257. DOI: 10.1038/nphys1224. arXiv: 0809.3972.
- [HHH99] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. "General teleportation channel, singlet fraction, and quasidistillation". In: *Physical Review A* 60.3 (1999), pp. 1888–1898. DOI: 10.1103/PhysRevA.60.1888. arXiv: quant-ph/9807091.

- [Hol19] Alexander S. Holevo. *Quantum Systems, Channels, Information.* De Gruyter, 2019. DOI: 10.1515/9783110642490.
- [KSW20] Sumeet Khatri, Kunal Sharma, and Mark M. Wilde. "Information-theoretic aspects of the generalized amplitude-damping channel". In: *Physical Review A* 102.1 (2020). DOI: 10.1103/PhysRevA.102.012401. arXiv: 1903.07747.
- [LDS18] Felix Leditzky, Nilanjana Datta, and Graeme Smith. "Useful States and Entanglement Distillation". In: *IEEE Transactions on Information Theory*. Vol. 64. 7. 2018, pp. 4689–4708. DOI: 10.1109/TIT.2017.2776907. arXiv: 1701.03081.
- [Li+09] Ke Li, Andreas Winter, Xubo Zou, and Guangcan Guo. "Private capacity of quantum channels is not additive". In: *Physical Review Letters* 103.12 (2009). DOI: 10.1103/PhysRevLett.103.120501. arXiv: 0903.4308.
- [Llo97] Seth Lloyd. "Capacity of the noisy quantum channel". In: *Physical Review A* 55.3 (1997), pp. 1613–1622. DOI: 10.1103/PhysRevA.55.1613. arXiv: quant-ph/9604015.
- [LLS18a] Felix Leditzky, Debbie Leung, and Graeme Smith. "Dephrasure Channel and Superadditivity of Coherent Information". In: *Physical Review Letters* 121.16 (2018), p. 160501. DOI: 10.1103/PhysRevLett.121.160501. arXiv: 1806.08327.
- [LLS18b] Felix Leditzky, Debbie Leung, and Graeme Smith. "Quantum and Private Capacities of Low-Noise Channels". In: *Physical Review Letters* 120.16 (2018). DOI: 10.1103/PhysRevLett.120.160503. arXiv: 1705.04335.
- [NPJ20] Kyungjoo Noh, Stefano Pirandola, and Liang Jiang. "Enhanced energy-constrained quantum communication over bosonic Gaussian channels". In: *Nature Communications* 11.1 (2020), p. 457. DOI: 10.1038/s41467-020-14329-6. arXiv: 1811.06988.
- [Ouy11] Yingkai Ouyang. "Channel covariance, twirling, contraction, and some upper bounds on the quantum capacity". In: *Quantum Information and Computation* (2011). DOI: 10.26421/QIC17.11-12. arXiv: 1106.2337.
- [Rai01] E. M. Rains. "A semidefinite program for distillable entanglement". In: IEEE Transactions on Information Theory 47.7 (2001), pp. 2921–2933. DOI: 10.1109/18.959270. arXiv: quant-ph/0008047.
- [Rai99] E. M. Rains. "Bound on distillable entanglement". In: Physical Review A 60.1 (1999), pp. 179–184. DOI: 10.1103/PhysRevA.60.179.
- [RMG18] Matteo Rosati, Andrea Mari, and Vittorio Giovannetti. "Narrow bounds for the quantum capacity of thermal attenuators". In: *Nature Communications* 9.1 (2018). DOI: 10.1038/s41467-018-06848-0. arXiv: 1801.04731.
- [SG21] Vikesh Siddhu and Robert B. Griffiths. "Positivity and Nonadditivity of Quantum Capacities Using Generalized Erasure Channels". In: *IEEE Transactions on Information Theory* 67.7 (2021), pp. 4533–4545. DOI: 10.1109/TIT.2021.3080819. arXiv: 2003.00583.
- [Sho02] Peter W Shor. "The quantum channel capacity and coherent information". In: *lecture notes*, *MSRI Workshop on Quantum Computation (Quantum Information and Cryptography)*. https://www.msri.org/workshops/203/schedules/1181. 2002.
- [Sid20] Vikesh Siddhu. Leaking information to gain entanglement. 2020. arXiv: 2011.15116.
- [Sid21] Vikesh Siddhu. "Entropic singularities give rise to quantum transmission". In: *Nature Communications* 12.1 (2021), p. 5750. DOI: 10.1038/s41467-021-25954-0. arXiv: 2003.10367.

- [Smi08] Graeme Smith. "Private classical capacity with a symmetric side channel and its application to quantum cryptography". In: *Physical Review A* 78.2 (2008), p. 022306. DOI: 10.1103/PhysRevA.78.022306. arXiv: 0705.3838.
- [SS07] Graeme Smith and John A. Smolin. "Degenerate Quantum Codes for Pauli Channels". In: *Physical Review Letters* 98.3 (2007), p. 030501. DOI: 10.1103/Phys-RevLett.98.030501. arXiv: quant-ph/0604107.
- [SS96] Peter W. Shor and John A. Smolin. *Quantum Error-Correcting Codes Need Not* Completely Reveal the Error Syndrome. 1996. arXiv: quant-ph/9604006.
- [SSW08] Graeme Smith, John A. Smolin, and Andreas Winter. "The quantum capacity with symmetric side channels". In: *IEEE Transactions on Information Theory* 54.9 (2008), pp. 4208–4217. DOI: 10.1109/TIT.2008.928269. arXiv: quant-ph/0607039.
- [SSY11] Graeme Smith, John A. Smolin, and Jon Yard. "Quantum communication with Gaussian channels of zero quantum capacity". In: *Nature Photonics* 5.10 (2011), pp. 624–627. DOI: 10.1038/nphoton.2011.203. arXiv: 1102.4580.
- [Sut+17] David Sutter, Volkher B. Scholz, Andreas Winter, and Renato Renner. "Approximate Degradable Quantum Channels". In: *IEEE Transactions on Information Theory* 63.12 (2017), pp. 7832–7844. DOI: 10.1109/TIT.2017.2754268. arXiv: 1412. 0980.
- [SY08] Graeme Smith and Jon Yard. "Quantum communication with zero-capacity channels". In: Science 321.5897 (2008), pp. 1812–1815. DOI: 10.1126/science.1162242. arXiv: 0807.4935.
- [Wan21] Xin Wang. "Pursuing the fundamental limits for quantum communication". In: *IEEE Transactions on Information Theory* 67.7 (2021), pp. 4524–4532. DOI: 10.1109/TIT.2021.3068818. arXiv: 1912.00931.
- [Wil17] Mark M. Wilde. *Quantum Information Theory*. Cambridge: Cambridge University Press, 2017, pp. 1–757. DOI: 10.1017/9781316809976.
- [Woo87] William K. Wootters. "A Wigner-function formulation of finite-state quantum mechanics". In: Annals of Physics 176.1 (1987). DOI: 10.1016/0003-4916(87)90176-X.
- [WPG07] Michael M. Wolf and David Pérez-García. "Quantum capacities of channels with small environment". In: *Physical Review A* 75.1 (2007), p. 012303. DOI: 10.1103/PhysRevA.75.012303. arXiv: quant-ph/0607070.
- [WY16] Andreas Winter and Dong Yang. "Potential capacities of quantum channels". In: *IEEE Transactions on Information Theory* 62.3 (2016). DOI: 10.1109/TIT.2016.2519920. arXiv: 1505.00907.
- [YHD08] Jon Yard, Patrick Hayden, and Igor Devetak. "Capacity theorems for quantum multiple-access channels: classical-quantum and quantum-quantum capacity regions". In: *IEEE Transactions on Information Theory* 54.7 (2008), pp. 3091–3113. DOI: 10.1109/TIT.2008.924665. arXiv: quant-ph/0501045.
- [Yu+20] Shang Yu, Yu Meng, Raj B. Patel, Yi-Tao Wang, Zhi-Jin Ke, Wei Liu, et al. "Experimental observation of coherent-information superadditivity in a dephrasure channel". In: *Physical Review Letters* 125.6 (2020). DOI: 10.1103/Phys-RevLett.125.060502. arXiv: 2003.13000.

- [Zhu+19] Elton Yechao Zhu, Quntao Zhuang, Min Hsiu Hsieh, and Peter W. Shor. "Superadditivity in Trade-Off Capacities of Quantum Channels". In: *IEEE Transactions on Information Theory* 65.6 (2019), pp. 3973–3989. DOI: 10.1109/TIT.2018.2889082. arXiv: 1708.04314.
- [ZZS17] Elton Yechao Zhu, Quntao Zhuang, and Peter W. Shor. "Superadditivity of the Classical Capacity with Limited Entanglement Assistance". In: *Physical Review Letters* 119.4 (2017). DOI: 10.1103/PhysRevLett.119.040503. arXiv: 1704.06955.