Maximum privacy without coherence, zero-error

Debbie Leung* Nengkun Yu†

03 September, 2015

Abstract

We study the possible difference between the quantum and the private capacities of a quantum channel in the zero-error setting. For a family of channels introduced by [LLSS14], we demonstrate an extreme difference: the zero-error quantum capacity is zero, whereas the zero-error private capacity is maximum given the quantum output dimension.

1 Introduction

Given Alice, a sender, and Bob, a receiver, any communication from Alice to Bob can be modeled by a quantum channel $\mathcal{N}$. Various capacities of the quantum channel $\mathcal{N}$ can be defined to quantify its capability for communicating different types of data. The quantum capacity $Q(\mathcal{N})$, measured in qubits per channel use, establishes the maximum rate for transmitting quantum information and how well we can perform quantum error correction. The private capacity $\mathcal{P}(\mathcal{N})$, in bits per channel use, gives the maximum rate of *private* classical communication. Errors that become negligible as the number of channel uses increases are allowed in the above definitions.

Understanding the relation between the quantum and the private capacities is an essential task in quantum Shannon theory. In [HHHO05], some channels $\mathcal{N}$ are found for which $Q(\mathcal{N}) = 0$ but $P(\mathcal{N}) > 0$, breaking a long-held intuition that coherence is necessary for privacy. In [LLSS14], a class of channels with $Q(\mathcal{N}) \leq 1$ and $P(\mathcal{N}) = \log d$ is presented, where d^2 is the input dimension and log is taken base 2. As d increases, these channels saturate an upper bound for $P(\mathcal{N}) - Q(\mathcal{N})$ thus approximately realizing the largest possible separation between the two capacities.

Introduced by Shannon in 1956 [SHA56], the zero-error capacity characterizes the optimal achievable communication rate of a noisy channel when information must be transmitted without any error. The zero-error capacity has deep connections to combinatorial optimization and it plays an essential role in graph theory and communication complexity theory [LOV79, ALON98]. Quite recently, the notion of zero-error capacity has been introduced for quantum channels [MA05,

*Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada.

†Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, and Department of Mathematics & Statistics, University of Guelph, Guelph, Ontario, Canada

MACA06, BS07], and many further interesting results are found [DUAN09, CCH11, CS12, DSW13, SS14, SS15, S15]. In particular, some channels cannot transmit quantum data perfectly given only one use, but have a large transmission rate with two uses. Also, there exist channels with no zero-error capacity but whose joint zero-error capacity is positive, a phenomenon called superactivation. In fact, quantum channels with no zero-error *classical* capacities are found to have joint zero-error *quantum* capacities (that activates all of zero-error classical, private, and quantum capacities)! Superactivation is impossible for classical channels. Various assisted communication scenarios have also been studied but they are out of the current scope.

We denote the zero-error quantum and private capacities for a quantum channel $\mathcal{N}$ as $Q_0(\mathcal{N})$ and $P_0(\mathcal{N})$ respectively. Zero-error private classical communication requires perfect data transmission such that no one but the receiver gains any information on the data. Clearly $Q_0(\mathcal{N}) \leq Q(\mathcal{N}) \leq \mathcal{P}(\mathcal{N})$ and $Q_0(\mathcal{N}) \leq P_0(\mathcal{N}) \leq \mathcal{P}(\mathcal{N})$.

In this paper, we study the zero-error quantum capacity of the channels introduced in [LLSS14], and demonstrate an exact extreme separation. For these channels, $P_0(\mathcal{N}) = \log d$ and $Q_0(\mathcal{N}) = 0$. In other words, each of these channels has no capacity to transmit quantum information perfectly, even it has full ability to distribute private information perfectly.

2 Preliminaries

In this section, we discuss some background and notation in quantum information and zero error capacities for a quantum channel. Readers familiar with these subjects can proceed to the next section.

A *complex Euclidean space* refers to any finite dimensional inner product space over the complex numbers. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be arbitrary complex Euclidean spaces. A pure quantum state of $\mathcal{H}_A$ is a normalized vector $|\psi\rangle \in \mathcal{H}_A$.

The space of linear operators mapping $\mathcal{H}_A$ to $\mathcal{H}_B$ is denoted by $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$, while $\mathcal{L}(\mathcal{H}_A)$ is the shorthand for $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_A)$. $I_{\mathcal{H}_A}$ is used to denote the identity operator on $\mathcal{H}_A$. The adjoint of $M \in \mathcal{L}(\mathcal{H}_A)$ is denoted by $M^\dagger$. The notation $M \geq 0$ means that M is hermitian, $M = M^\dagger$, and is positive semidefinite.

With respect to a fixed basis, the complex conjugate of a state $|\alpha\rangle$ and a linear operator M are denoted as $|\alpha^c\rangle$ and M^c, respectively.

A general quantum state of $\mathcal{H}_A$ is characterized by its density operator $\rho \in \mathcal{L}(\mathcal{H}_A)$, which is a positive semidefinite operator with trace one on $\mathcal{H}_A$. We denote the set of density matrices as $\mathcal{D}(\mathcal{H}_A)$. The density operator of a pure state $|\psi\rangle$ is simply the projector $\psi := |\psi\rangle\langle\psi|$. The support of ρ, denoted by $supp(\rho)$, is the vector space spanned by the eigenvectors of ρ with positive eigenvalues. More concretely, if ρ has spectral decomposition $\rho = \sum_{k=1}^n p_k |\psi_k\rangle\langle\psi_k|$, where $0 < p_k \leq 1$ and $\sum_{k=1}^n p_k = 1$. Then $supp(\rho) = span\{|\psi_k\rangle : 1 \leq k \leq n\}$. The null space of any $M \geq 0$ is the orthogonal complement of $supp(M)$.

A nonzero positive semidefinite operator $E \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is said to be a PPT operator (or simply

PPT) if $E^{\Gamma_{\mathcal{H}_A}} \geq 0$, where $\Gamma_{\mathcal{H}_A}$ denotes the partial transpose with respect to the system $\mathcal{H}_A$, i.e.,

$$(|ij\rangle\langle kl|)^{\Gamma_{\mathcal{H}_A}} = |kj\rangle\langle il|. \tag{1}$$

While $\Gamma_{\mathcal{H}_A}$ is basis dependent, the property being PPT is not. For simplicity, we will specify the system $\mathcal{H}_A$ for $\Gamma_{\mathcal{H}_A}$ in the text and denote the operation with the shorthand Γ.

A quantum channel $\mathcal{N}$ from Alice to Bob is a completely positive trace preserving linear map from the input state space of Alice $\mathcal{D}(\mathcal{H}_A)$ to the output state space of Bob $\mathcal{D}(\mathcal{H}_B)$. There are several characterizations of quantum channels (see [NC00] chapter 8 or [Wat11]). We use the isometric extension for a channel, $\mathcal{N}(\rho) = \mathrm{tr}_{\mathcal{H}_E} U\rho U^\dagger$, where $U \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B \otimes \mathcal{H}_E)$ is an isometry mapping the input to the output space for Bob and some auxilary space called the "environment", and $\mathrm{tr}_{\mathcal{H}_E}$ denote the partial trace over $\mathcal{H}_E$. The isometry U is unique up to left multiplication by another isometry acting on $\mathcal{H}_E$, and this degree of freedom has no physical effect on our analysis, and can be chosen to facilitate it. The complementary channel $\mathcal{N}^c(\rho) = \mathrm{tr}_{\mathcal{H}_B} U\rho U^\dagger$ describes what information leaks to the environment.

The notion of zero-error quantum capacity can be introduced as follows. Let $\alpha^q(\mathcal{N})$ be the maximum integer k such that there is a k-dimensional subspace $\mathcal{H}'_A$ of $\mathcal{H}_A$ that can be perfectly transmitted through $\mathcal{N}$. That is, there is a recovery quantum channel $\mathcal{R}$ from $\mathcal{D}(\mathcal{H}_B)$ to $\mathcal{D}(\mathcal{H}_{A'})$ so that $(\mathcal{R} \circ \mathcal{N})(\psi) = \psi$ for any $|\psi\rangle \in \mathcal{H}_{A'}$ (recall $\psi = |\psi\rangle\langle\psi|$). Then, $\log_2 \alpha^q(\mathcal{N})$ represents the maximum number of qubits one can send perfectly by one use of $\mathcal{N}$. The *zero-error quantum capacity* of $\mathcal{N}$, $Q_0(\mathcal{N})$, is defined as:

$$Q_0(\mathcal{N}) = \sup_{n \geq 1} \frac{\log_2 \alpha^q(\mathcal{N}^{\otimes n})}{n}. \tag{2}$$

The main difficulty of evaluating the zero-error capacity of a quantum channel is that there is no upper bound on the required number of uses n in evaluating the above expression. This remains the case even for the simpler problem of determining whether $Q_0(\mathcal{N}) = 0$. For example, in [SS14], for any integer k, the authors found a channel $\mathcal{N}$ for which $\alpha^q(\mathcal{N}) = 1$ but $\alpha^q(\mathcal{N}^{\otimes 2}) \geq k$. They also found a channel $\mathcal{N}$ for which the k-shot capacity vanishes but $Q_0(\mathcal{N}) > 0$. Furthermore, superactivation is possible (see section 1) and [CS12] exhibits an extreme example in which channels $\mathcal{N}_1$, $\mathcal{N}_2$ have no zero-error classical capacity but $Q_0(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$. Fortunately, for our purpose, we can invoke the following lemma from [CS12].

Lemma 1. *Let $\mathcal{N} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$ be a quantum channel. One can transmit quantum information without error through a single use of $\mathcal{N}$ if and only if there are states $|\alpha\rangle$ and $|\beta\rangle$ such that*

$$\mathrm{tr}\left[\mathcal{N}(|\alpha\rangle\langle\alpha|)\,\mathcal{E}(|\beta\rangle\langle\beta|)\right] = 0 \tag{3}$$

and

$$\mathrm{tr}\left[\mathcal{N}(|\alpha+\beta\rangle\langle\alpha+\beta|)\,\mathcal{N}(|\alpha-\beta\rangle\langle\alpha-\beta|)\right] = 0. \tag{4}$$

where $|\alpha \pm \beta\rangle = 1/\sqrt{2}(|\alpha\rangle \pm |\beta\rangle)$.

Private communication via a memoryless classical channel and quantum key distribution are well established subjects. Private classical communication of a quantum channel has more recently been formally introduced in [Dev05]. The private capacity of $\mathcal{N}$ measures the maximum rate of reliable classical data transmission via $\mathcal{N}$ while keeping the output of the complementary channel independent of the data. In [Dev05], an expression for the private capacity is derived,

$$\mathcal{P}(\mathcal{N}) = \max_{\mathcal{E}} \frac{1}{n} \left[I(X : B_1 \cdots B_n) - I(X : E_1 \cdots E_n) \right] \tag{5}$$

where B_i, E_i are the output and environment spaces for the i^{th} channel use, $I(C : D) = S(C) + S(D) - S(CD)$ is the quantum mutual information between C and D evaluated on the state of CD, $S(\cdot)$ denotes the von Neumann entropy, and $\mathcal{E} = \{p_x, \rho_x\}$ is a general ensemble of possibly mixed states ρ_x on the n input spaces $A_1 \cdots A_n$. The expressions $I(X : B_1 \cdots B_n)$, $I(X : E_1 \cdots E_n)$ are evaluated on $\sum_x p_x |x\rangle\langle x|_X \otimes \mathcal{N}^{\otimes n}(\rho_x)$ and $\sum_x p_x |x\rangle\langle x|_X \otimes \mathcal{N}^{c \otimes n}(\rho_x)$ respectively. Once again, the requirement to optimize over n in the capacity expression Eq. (5) is an obstacle for evaluating the private capacity in general. However, useful lower bounds and properties of the private capacity can still be inferred from Eq. (5).

Consider any quantum channel $\mathcal{N}$ with a quantum output B and a classical output C. We use Eq. (5) to show that $\mathcal{P}(\mathcal{N}) \leq \log_2 \dim(B)$. We first consider the one shot case.

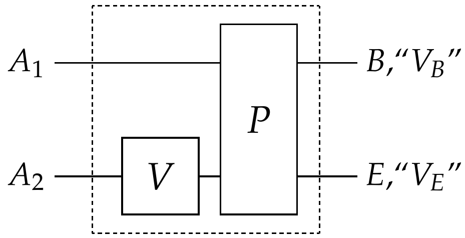
$$I(X : BC) - I(X : E) = I(X : BC) - I(X : EC) = \sum_c p_c [I(X : B|C = c) - I(X : E|C = c)] \,. \tag{6}$$

The first equality comes from the classicality of C, that the environment E already has a copy of the information. The second equality follows from decomposing the von Neuman entropy of a quantum-classical system [NC00]. If we optimize the expression in the square brackets, we obtain the one-shot private capacity for $\mathcal{N}$ conditioned on $C = c$, which is upper bounded by $\log_2 \dim(B)$. The argument for the n-shot case is identical, with B, C, E replaced by n-tuples.

3 Zero-error Quantum Capacity of $\mathcal{N}_d$

In this section, we first describe the family of channels that will exhibit the extreme separation between the zero-error quantum and private capacities. Then, we derive those capacities.

The family of channels $\mathcal{N}_d$ introduced in [LLSS14] can be schematically summarized as follows:



(7)

For each integer $d \geq 2$, we define the channel $\mathcal{N}_d$ which has two input registers A_1 and A_2, each of dimension d. A unitary operation V is applied to A_2, followed by a controlled phase gate $P = \sum_{i,j} \omega^{ij} |i\rangle\langle i| \otimes |j\rangle\langle j|$ acting on $A_1 A_2$, where ω is a primitive d^{th} root of unity. Bob receives only A_1 (now relabeled as B) and "V_B", which denotes a classical register with a description of V. The

A_2 register is discarded. The complementary channel has outputs A_2 (relabeled as E) and "V_E" which also contains a description of V. The isometric extension is given by

$$U_d \left|\psi\right\rangle_{A_1A_2} = \sum_V \sqrt{\mathrm{pr}(V)}\, \left(P\,(I\otimes V)\left|\psi\right\rangle_{A_1A_2}\right) \otimes \left|V\right\rangle_{V_B} \otimes \left|V\right\rangle_{V_E}\,.$$

Here, V is drawn from any exact unitary 2-design $\mathcal{G} = \{g_1, g_2, \cdots, g_m\}$ (such as the Clifford group, see [CLLW15] and the references therein).

It was shown in [LLSS14] that $P(\mathcal{N}_d) = \log d$. The method given by [LLSS14] to transmit private classical data has no error and has perfect secrecy so $P_0(\mathcal{N}_d) = \log d$. To be self-contained, we provide a quick argument here. Suppose the input into A_2 is half of a maximally entangled state $|\Phi\rangle = \frac{1}{\sqrt{d}}\sum_i |i\rangle_{A_2}|i\rangle_{A_3}$ where A_3 stays in Alice's possession. By the transpose trick, the unitary operations V and P can be replaced by unitary operations acting on A_1 and A_3 without changing the final state on B, E, A_3, V_B, V_E. So, the output of the complementary channel (E, V_E) is independent of the input. Moreover, $\mathcal{N}_d(|i\rangle\langle i| \otimes I/d) = |i\rangle\langle i|$. So $\log d$ bits can be transmitted perfectly and secretly.

Furthermore, [LLSS14] also shows that $Q(\mathcal{N}_d) \leq 1$. Intuitively, superposition of states in system A_1 will be heavily decohered by the P gate, because error correction is ineffective due to the random unitary V. However, [LLSS14] finds that $Q(\mathcal{N}_d) \geq 0.61$ for large d.

This motivates the current study, to demonstrate an extreme separation of P_0 and Q_0 using the channels $\mathcal{N}_d$. Our main result is that, no finite number of uses of $\mathcal{N}_d$ can be used to transmit one qubit with zero error. This implies in particular $Q_0(\mathcal{N}_d) = 0$, while $P_0(\mathcal{N}_d) = \log d$, attaining the extremes allowed by the quantum output dimension (see end of section 2.)

In [DUAN09, DSW13, SS14], the non-commutative graph of a quantum channel is defined and used to study several different zero-error capacities. In particular, [SS14] derived sufficient conditions for the impossibility of superactivation of zero-error quantum capacity of a channel in terms of properties of the single-copy non-commutative graph. If a channel satisfies any of these conditions, and has no one-shot zero error quantum capacity, then it has no zero-error quantum capacity by induction. However, we show in the appendix that the non-commutative graph of $\mathcal{N}_d$ does not satisfy any of these conditions, along with a discussion of its non-commutative graph.

Our main technical result is a characterization of pairs of input states whose orthogonality is preserved by n uses of the channel.

Theorem 2. Let n be any positive integer, $|\psi_1\rangle = \sum_{i_1,\cdots,i_n} |i_1,\cdots,i_n\rangle\,|\alpha_{i_1,\cdots,i_n}\rangle$, and $|\psi_2\rangle = \sum_{i_1,\cdots,i_n} |i_1,\cdots,i_n\rangle\,|\beta_{i_1,\cdots,i_n}\rangle$ be two arbitrary pure state inputs for $\mathcal{N}_d^{\otimes n}$. Then, $\mathrm{tr}[\mathcal{N}_d^{\otimes n}(\psi_1)\mathcal{N}_d^{\otimes n}(\psi_2)] = 0$ if and only if at most one of $|\alpha_{i_1,\cdots,i_n}\rangle$ and $|\beta_{i_1,\cdots,i_n}\rangle$ is nonzero for each tuple $(i_1,\cdots,i_n)$.

In other words, states suitable for transmitting classical information through $\mathcal{N}_d^{\otimes n}$ without any error have no "overlap" in the computational basis of $A_1^{\otimes n}$.

We first state the consequence of Theorem 2 and then we will return to prove it.

Theorem 3. For any positive integer n, $\mathcal{N}_d^{\otimes n}$ cannot transmit a qubit with zero error. In particular, this implies $Q_0(\mathcal{N}_d) = 0$.

Proof (theorem 3). Suppose by contradiction, some n uses of $\mathcal{N}_d$ can be used to transmit a 2-dimensional subspace spanned by a basis $\{|\psi_1\rangle, |\psi_2\rangle\}$, where $|\psi_1\rangle = \sum_{i_1,\cdots,i_n} |i_1,\cdots,i_n\rangle |\alpha_{i_1,\cdots,i_n}\rangle$, and $|\psi_2\rangle = \sum_{i_1,\cdots,i_n} |i_1,\cdots,i_n\rangle |\beta_{i_1,\cdots,i_n}\rangle$. According to Lemma 1,

$$\operatorname{tr}\left[\mathcal{N}_d^{\otimes n}(\psi_1)\,\mathcal{N}_d^{\otimes n}(\psi_2)\right] = 0 \tag{8}$$

and

$$\operatorname{tr}\left[\mathcal{N}_d^{\otimes n}(|\psi_1{+}\psi_2\rangle\langle\psi_1{+}\psi_2|)\,\mathcal{N}_d^{\otimes n}(|\psi_1{-}\psi_2\rangle\langle\psi_1{-}\psi_2|)\right] = 0. \tag{9}$$

Invoking Theorem 2 on the conditions above, for each $i_1,\cdots,i_n$, at most one of $|\alpha_{i_1,\cdots,i_n}\rangle = 0$ and $|\beta_{i_1,\cdots,i_n}\rangle$ is nonzero, and at most one of $(|\alpha_{i_1\cdots i_n}\rangle + |\beta_{i_1,\cdots,i_n}\rangle)$ and $(|\alpha_{i_1\cdots i_n}\rangle - |\beta_{i_1,\cdots,i_n}\rangle)$ is nonzero, which implies $|\alpha_{i_1\cdots i_n}\rangle = |\beta_{i_1,\cdots,i_n}\rangle = 0$. Then, $|\psi_1\rangle = |\psi_2\rangle = 0$ a contradiction. ■

We now turn to a proof for Theorem 2. We first consider the simpler one-shot case to illustrate the main ideas without the burden of the n-shot notations. Then, we prove Theorem 2 with similar techniques.

Lemma 4. Let $|\psi_1\rangle = \sum_i |i\rangle |\alpha_i\rangle$ and $|\psi_2\rangle = \sum_i |i\rangle |\beta_i\rangle$ be two possible pure input states for $\mathcal{N}_d$. Then, $\operatorname{tr}[\mathcal{N}_d(\psi_1)\mathcal{N}_d(\psi_2)] = 0$ if and only if at most one of $|\alpha_i\rangle$ and $|\beta_i\rangle$ is nonzero for each i.

Proof (lemma 4). We first rephrase the condition $\operatorname{tr}[\mathcal{N}_d(\psi_1)\mathcal{N}_d(\psi_2)] = 0$.

Recall that V is chosen from an exact unitary 2-design $\mathcal{G} = \{g_1, g_2, \cdots, g_m\}$. We rewrite the gate $P = \sum_i |i\rangle\langle i| \otimes Z_i$ where $Z = \sum_k \omega^k |k\rangle\langle k|$, and $Z_l = Z^l$. So, for $V = g_j$,

$$P(I\otimes V)|\psi_1\rangle = \sum_i |i\rangle \left(Z_i g_j |\alpha_i\rangle\right),$$
$$P(I\otimes V)|\psi_2\rangle = \sum_i |i\rangle \left(Z_i g_j |\beta_i\rangle\right),$$

where the first and second systems are B and E respectively. Then reducing the above states to B gives respectively

$$\rho^{(j)} = \sum_{i,k} \rho^{(j)}_{i,k} |k\rangle\langle i| \quad \text{with} \quad \rho^{(j)}_{i,k} = \langle \alpha_i | g_j^\dagger Z_{k-i} g_j | \alpha_k\rangle,$$
$$\sigma^{(j)} = \sum_{i,k} \sigma^{(j)}_{i,k} |k\rangle\langle i| \quad \text{with} \quad \sigma^{(j)}_{i,k} = \langle \beta_i | g_j^\dagger Z_{k-i} g_j | \beta_k\rangle.$$

Their trace inner product can be rephrased:

$$\begin{aligned}
\operatorname{tr}(\rho^{(j)\dagger}\sigma^{(j)}) &= \operatorname{tr}(\rho^{(j)}\sigma^{(j)}) = \sum_{i,k} \rho^{(j)}_{i,k}\sigma^{(j)}_{k,i} = \sum_{i,k} \rho^{(j)}_{i,k}\sigma^{(j)*}_{i,k} \\
&= \sum_{i,k} \langle\alpha_i|g_j^\dagger Z_{k-i} g_j|\alpha_k\rangle\langle\beta_i^c|g_j^{\dagger c} Z_{k-i}^c g_j^c|\beta_k^c\rangle \\
&= \sum_{i,k} \langle\alpha_i|\langle\beta_i^c|(g_j^\dagger Z_{k-i} g_j)\otimes(g_j^{\dagger c} Z_{k-i}^c g_j^c)|\alpha_k\rangle|\beta_k^c\rangle \\
&= \langle x|A^{(j)}|x\rangle,
\end{aligned}$$

where

$$\begin{aligned}
A^{(j)} &= \sum_{i,k} |i\rangle\langle k| \otimes (g_j^\dagger Z_{k-i} g_j) \otimes (g_j^{\dagger c} Z_{k-i}^c g_j^c), \text{ and} \\
|x\rangle &= \sum_i |i\rangle\,|\alpha_i\rangle\,|\beta_i^c\rangle.
\end{aligned}$$

Let $A := \mathbb{E}_j A^{(j)}$. By the construction of $\mathcal{N}_d$,

$$\operatorname{tr}[\mathcal{N}_d(\psi_1)\mathcal{N}_d(\psi_2)] = 0 \iff \forall j,\ \operatorname{tr}(\rho^{(j)\dagger}\sigma^{(j)}) = 0 \iff \mathbb{E}_j \operatorname{tr}(\rho^{(j)\dagger}\sigma^{(j)}) = 0 \iff \langle x|A|x\rangle = 0.$$

Having rephrased the condition $\operatorname{tr}[\mathcal{N}_d(\psi_1)\mathcal{N}_d(\psi_2)] = 0$ as $\langle x|A|x\rangle = 0$, we show below that the latter implies $|x\rangle = 0$. This is done by first evaluating A which has very simple structure, then analyzing its null space, and showing that the null space contains no nonzero state of the form given by $|x\rangle$.

One can calculate A directly because $\{g_j\}$ is an exact unitary 2-design [DCEL09, CLLW15]:

$$A = \mathbb{E}_j A^{(j)} \tag{10}$$

$$= \sum_{i,k} |i\rangle\langle k| \otimes \mathbb{E}_j (g_j^\dagger \otimes g_j^{\dagger c})(Z_{k-i} \otimes Z_{i-k})(g_j \otimes g_j^c) \tag{11}$$

$$= \sum_{i,i} |i\rangle\langle i| \otimes I + \sum_{i \neq k} |i\rangle\langle k| \otimes \mathbb{E}_j (g_j^\dagger \otimes g_j^{\dagger c})(Z_{k-i} \otimes Z_{i-k})(g_j \otimes g_j^c)\,. \tag{12}$$

Here, for $i \neq k$, we have $\mathbb{E}_j (g_j^\dagger \otimes g_j^{\dagger c})(Z_{k-i} \otimes Z_{i-k})(g_j \otimes g_j^c) = -\frac{1}{d^2-1}(I - \Phi) + \Phi$, where $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle\,|i\rangle$ is the maximally entangled state, $\{\Phi, I - \Phi\}$ form a maximal set of invariances for the averaging, and the coefficients $-\frac{1}{d^2-1}$ and 1 come from evaluating $\frac{1}{d^2-1} \operatorname{tr}[Z_{k-i} \otimes Z_{i-k}(I-\Phi)]$ and $\operatorname{tr}[Z_{k-i} \otimes Z_{i-k}\Phi]$ respectively. Therefore,

$$A = \sum_{i,i} |i\rangle\langle i| \otimes I + \sum_{i \neq k} |i\rangle\langle k| \otimes \left(-\frac{1}{d^2-1}(I - \Phi) + \Phi\right) \tag{13}$$

$$= \sum_{i,k} |i\rangle\langle k| \otimes (a_{i,k}(I - \Phi) + \Phi), \tag{14}$$

where $a_{i,i} = 1$ and $a_{i,k} = -\frac{1}{d^2-1}$ for $i \neq k$.

Having found an explicit expression for A, we analyze the support of A as follows:

$$\begin{aligned} A &= \sum_{i,k} |i\rangle\langle k| \otimes (a_{i,k}(I - \Phi) + \Phi) \\ &= \left(\sum_{i,k} a_{i,k} |i\rangle\langle k|\right) \otimes (I - \Phi) + d\ |\nu\rangle\langle\nu| \otimes \Phi\,, \end{aligned}$$

where $|\nu\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle$. Notice that $\sum_{i,k} a_{i,k} |i\rangle\langle k| \geq 0$, so the projector onto the support of A is

$$I \otimes (I - \Phi) + |\nu\rangle\langle\nu| \otimes \Phi.$$

So the null space of A is spanned by $|\mu\rangle \otimes |\Phi\rangle$ where $|\mu\rangle$ is any vector orthogonal to $|\nu\rangle$.

We now show that $|x\rangle = 0$. Suppose by contradiction that $|x\rangle \neq 0$. Since $\langle x|A|x\rangle = 0$, we have $|x\rangle = |\mu\rangle \otimes |\Phi\rangle$ for some $|\mu\rangle \neq 0$. But $|x\rangle = \sum_i |i\rangle\,|\alpha_i\rangle\,|\beta_i^c\rangle$. For each $l \in \{1, \cdots, d\}$,

$$(\langle l| \otimes I \otimes I)|x\rangle = |\alpha_l\rangle\,|\beta_l^c\rangle = \langle l|\mu\rangle|\Phi\rangle,$$

which is a contradiction unless $\langle l|\mu\rangle = 0$. But now $|\mu\rangle = 0$ which is a contradiction.

Putting the above together, $\operatorname{tr}[\mathcal{N}_d(\psi_1)\mathcal{N}_d(\psi_2)] = 0$ if and only if $\langle x|A|x\rangle = 0$ if and only if at most one of $|\alpha_i\rangle$ and $|\beta_i^c\rangle$ is nonzero for each i. ■

We are now going to prove Theorem 2, using similar techniques.

Proof (theorem 2). Consider two arbitrary pure input states for n uses of $\mathcal{N}_d$, $|\psi_1\rangle = \sum_{i_1,\cdots,i_n} |i_1\cdots i_n\rangle\,|\alpha_{i_1\cdots i_n}\rangle$ and $|\psi_2\rangle = \sum_{i_1,\cdots,i_n} |i_1\cdots i_n\rangle\,|\beta_{i_1,\cdots,i_n}\rangle$. For $V_1\otimes\cdots\otimes V_n = g_{j_1}\otimes\cdots\otimes g_{j_n}$, we have

$$
\begin{aligned}
P^{\otimes n}(I^{\otimes n}\otimes V_1\otimes\cdots\otimes V_n)\,|\psi_1\rangle &= \sum_{i_1,\cdots i_n} |i_1\cdots i_n\rangle\,(Z_{i_1}\otimes\cdots\otimes Z_{i_n})(g_{j_1}\otimes\cdots\otimes g_{j_n})\,|\alpha_{i_1\cdots i_n}\rangle\,,\\
P^{\otimes n}(I^{\otimes n}\otimes V_1\otimes\cdots\otimes V_n)\,|\psi_2\rangle &= \sum_{i_1,\cdots i_n} |i_1\cdots i_n\rangle\,(Z_{i_1}\otimes\cdots\otimes Z_{i_n})(g_{j_1}\otimes\cdots\otimes g_{j_n})\,|\beta_{i_1\cdots i_n}\rangle\,.
\end{aligned}
$$

Then the corresponding output states on $B_1\cdots B_n$ are

$$
\begin{aligned}
\rho^{(j_1,\cdots,j_n)} &= \sum_{i_1\cdots i_n,k_1\cdots k_n} |k_1\cdots k_n\rangle\langle i_1\cdots i_n|\;\rho^{(j_1,\cdots,j_n)}_{i_1\cdots i_n,k_1\cdots k_n}\\
\sigma^{(j_1,\cdots,j_n)} &= \sum_{i_1\cdots i_n,k_1\cdots k_n} |k_1\cdots k_n\rangle\langle i_1\cdots i_n|\;\sigma^{(j_1,\cdots,j_n)}_{i_1\cdots i_n,k_1\cdots k_n}\,,
\end{aligned}
$$

where

$$
\begin{aligned}
\rho^{(j_1,\cdots,j_n)}_{i_1\cdots i_n,k_1\cdots k_n} &= \langle\alpha_{i_1\cdots i_n}|(g^\dagger_{j_1}\otimes\cdots\otimes g^\dagger_{j_n})(Z_{k_1-i_1}\otimes\cdots\otimes Z_{k_n-i_n})(g_{j_1}\otimes\cdots\otimes g_{j_n})|\alpha_{k_1\cdots k_n}\rangle,\\
\sigma^{(j_1,\cdots,j_n)}_{i_1\cdots i_n,k_1\cdots k_n} &= \langle\beta_{i_1\cdots i_n}|(g^\dagger_{j_1}\otimes\cdots\otimes g^\dagger_{j_n})(Z_{k_1-i_1}\otimes\cdots\otimes Z_{k_n-i_n})(g_{j_1}\otimes\cdots\otimes g_{j_n})|\beta_{k_1\cdots k_n}\rangle.
\end{aligned}
$$

As in the one-shot case,

$$
\operatorname{tr}[\mathcal{N}_d^{\otimes n}(\psi_1)\mathcal{N}_d^{\otimes n}(\psi_2)] = 0 \iff \mathbb{E}_{j_1,\cdots,j_n}\operatorname{tr}(\rho^{(j_1,\cdots,j_n)\dagger}\sigma^{(j_1,\cdots,j_n)}) = 0 \iff \langle x|A^{\otimes n}|x\rangle = 0\,,
$$

where $|x\rangle = \sum_{i_1,\cdots,i_n} |i_1\cdots i_n\rangle\,|\alpha_{i_1\cdots i_n}\rangle\,\left|\beta^c_{i_1\cdots i_n}\right\rangle$ and A is as defined in the one-shot case. To verify the last equivalence:

$$
\begin{aligned}
&\mathbb{E}_{j_1,\cdots,j_n}\operatorname{tr}(\rho^{(j_1,\cdots,j_n)\dagger}\sigma^{(j_1,\cdots,j_n)})\\
={}& \mathbb{E}_{j_1,\cdots,j_n}\sum_{i_1\cdots i_n,k_1\cdots k_n}\rho^{(j_1,\cdots,j_n)}_{i_1\cdots i_n,k_1\cdots k_n}\sigma^{(j_1,\cdots,j_n)*}_{i_1\cdots i_n,k_1\cdots k_n}\\
={}& \mathbb{E}_{j_1,\cdots,j_n}\sum_{i_1\cdots i_n,k_1\cdots k_n}\langle\alpha_{i_1\cdots i_n}|(g^\dagger_{j_1}\otimes\cdots\otimes g^\dagger_{j_n})(Z_{k_1-i_1}\otimes\cdots\otimes Z_{k_n-i_n})(g_{j_1}\otimes\cdots\otimes g_{j_n})|\alpha_{k_1\cdots k_n}\rangle\\
&\qquad\qquad\langle\beta^c_{i_1\cdots i_n}|(g^{\dagger c}_{j_1}\otimes\cdots\otimes g^{\dagger c}_{j_n})(Z_{i_1-k_1}\otimes\cdots\otimes Z_{i_n-k_n})(g^c_{j_1}\otimes\cdots\otimes g^c_{j_n})|\beta^c_{k_1\cdots k_n}\rangle\\
={}& \sum_{i_1\cdots i_n,k_1\cdots k_n}\langle\alpha_{i_1\cdots i_n}|\langle\beta^c_{i_1\cdots i_n}|\mathbb{E}_{j_1}[(g^\dagger_{j_1}Z_{k_1-i_1}g_{j_1})\otimes(g^{\dagger c}_{j_1}Z^c_{k_1-i_1}g^c_{j_1})]\otimes\cdots\\
&\qquad\qquad\cdots\otimes\mathbb{E}_{j_n}[(g^\dagger_{j_n}Z_{k_n-i_n}g_{j_n})\otimes(g^{\dagger c}_{j_n}Z^c_{k_n-i_n}g^c_{j_n})]\,|\alpha_{k_1\cdots k_n}\rangle|\beta^c_{k_1\cdots k_n}\rangle\\
={}& \langle x|A^{\otimes n}|x\rangle\,.
\end{aligned}
$$

As in the one-shot case, it suffices to show that $\langle x|A^{\otimes n}|x\rangle = 0$ implies $|x\rangle = 0$.

Note that $A \geq I\otimes(I-\Phi)$, so, $A^{\otimes n} \geq I^{\otimes n}\otimes(I-\Phi)^{\otimes n}$. Therefore,

$$
0 = \langle x|A^{\otimes n}|x\rangle \geq \langle x|I^{\otimes n}\otimes(I-\Phi)^{\otimes n}|x\rangle \geq 0
$$

so, $\langle x|I^{\otimes n} \otimes (I-\Phi)^{\otimes n}|x\rangle = 0$. Equivalently, $\forall i_1 \cdots i_n$, $\mathrm{tr}[\alpha_{i_1\cdots i_n} \otimes \beta^c_{i_1\cdots i_n}(I-\Phi)^{\otimes n}] = 0$. Finally, $\alpha_{i_1\cdots i_n} \otimes \beta^c_{i_1\cdots i_n}$ is a matrix with positive partial transpose. According to the following lemma 5, $\alpha_{i_1\cdots i_n} \otimes \beta^c_{i_1\cdots i_n} = 0$. So, at most one of $|\alpha_{i_1\cdots i_n}\rangle$ and $|\beta^c_{i_1\cdots i_n}\rangle$ can be nonzero and $|x\rangle = 0$.

This completes the proof of Theorem 2. ■

Lemma 5. [YDY14] For all positive integer n, there is no non-zero matrix M satisfying $M \geq 0$, $M^\Gamma \geq 0$, and $\mathrm{tr}(M(I-\Phi)^{\otimes n}) = 0$.

This lemma was proved in [YDY14]. We include a proof here to be self-contained.

Proof. Suppose by contradiction, there is such a matrix M satisfying those conditions. Let

$$N = \int_U UMU^\dagger dU, \tag{15}$$

where U ranges over all unitaries of the form $\otimes_{k=1}^n (U_k \otimes U_k^c)$, and U_k ranges over all unitaries for each k, and each $U_k \otimes U_k^c$ acts on the system corresponding to the k^{th} copy of $I-\Phi$. Note that N satisfies the same properties as M, because the operation in Eq. (15) is completely positive (so $N \geq 0$), trace preserving (so $N \neq 0$), PPT preserving (so $N^\Gamma \geq 0$), and finally $\mathrm{tr}(N(I-\Phi)^{\otimes n}) = 0$. Additionally, N satisfies the property that there are non-negative p_k such that

$$N = \sum_{R_k \in \mathcal{R}} p_k R_k,$$

where $\mathcal{R} = \{\Phi, I-\Phi\}^{\otimes n} \setminus \{(I-\Phi)^{\otimes n}\}$.

Since Φ^Γ has both strictly positive and strictly negative eigenvalues, there exists a nonzero Q such that $Q \geq 0$ and $\mathrm{tr}(Q\Phi^\Gamma) = 0$. Thus,

$$r := \mathrm{tr}(Q(I-\Phi)^\Gamma) = \mathrm{tr}(Q) - \mathrm{tr}(Q\Phi^\Gamma) = \mathrm{tr}(Q) > 0.$$

Then the following holds

$$\mathrm{tr}_{1,2\cdots,n-1}[(Q^{\otimes n-1} \otimes I)(\sum_{R_k \in \mathcal{R}} p_k R_k^\Gamma)] \geq 0, \tag{16}$$

where $\mathrm{tr}_{1,2\cdots,n-1}$ denotes the partial trace operation on the first $n-1$ parties (because the above is a completely positive map to $N^\Gamma = \sum_{R_k \in \mathcal{R}} p_k R_k^\Gamma \geq 0$.) Eq. (16) implies that for $R_k = (I-\Phi)^{\otimes n-1} \otimes \Phi$, we have $r^{n-1} p_k \Phi^\Gamma \geq 0$ which implies that $p_k = 0$. Permuting the systems gives $p_l = 0$ for any R_l with $n-1$ tensor factors of $(I-\Phi)$. Finally, we can recursively prove that $p_k = 0$ for any $R_k \in \mathcal{R}$ with $n-2$ tensor factors, $n-3$ tensor factors etc. So, $N = 0$ which is a contradiction. ■

4 Conclusion

In this paper, we show an extreme separation between zero-error quantum capacity and the private capacity by demonstrating for a class of channels that the private capacity is maximum given the output dimension, while there is no ability to transmit even one-qubit with any finite number of channel uses, when no error can be tolerated. We hope techniques from our work can be used to study the zero-error capacity of other channels.

5 Acknowledgements

This work is supported by NSERC, NSERC DAS, CRC, and CIFAR.

References

[LLSS14] D. Leung, K. Li, G. Smith, and J. A. Smolin. Maximal Privacy without Coherence. *Physical Review Letters*, 113:030512, 2014.

[HHHO05] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94, 160502 (2005).

[SHA56] C. E. Shannon. The zero-error capacity of a noisy channel. *IRE Transactions on Information Theory*, 2(3):8–19, 1956.

[LOV79] L. Lovasz. Shannon capacity of the graph. *IEEE Transactions on Information Theory*, 25(1):1–7, 1979.

[ALON98] N. Alon. The Shannon capacity of a union. *Combinatorica.*, 18(3):301–310, 1998.

[MA05] R. A. C. Medeiros, F. M. de Assis. Zero-error capacity of a quantum channel. IJQI, 3(1):135-139, 2005.

[MACA06] R. A. C. Medeiros, R. Alleaume, G. Cohen, and F. M. de Assis. Quantum states characterization for the zero-error capacity. arXiv:quant-ph/0611042 (2006).

[BS07] S. Beigi, P. W. Shor. On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels. arXiv:0709.2090 (2007).

[DUAN09] R. Duan. Superactivation of zero-error capacity of noisy quantum channels. *arXiv:0906.2527*, 2009.

[CCH11] T. S. Cubitt, J. Chen, and A. W. Harrow. Superactivation of the asymptotic zero-error classical capacity of a quantum channel. *IEEE Transactions on Information Theory*, 57(12):81148126, 2011.

[CS12] T. S. Cubitt and G. Smith. An Extreme Form of Superactivation for Quantum Zero-Error Capacities. *IEEE Transactions on Information Theory*, 58(3):1953–1961, 2012.

[DSW13] R. Duan, S. Severini and A. Winter. Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovasz theta function. *IEEE Transactions on Information Theory*, 59(2):1164-1174, 2013.

[SS14] M.E. Shirokov, T.V. Shulman. On superactivation of one-shot zero-error quantum capacity and the related property of quantum measurements. Problems of Information Transmission, 2014, 50:3, 232-246.

[SS15] M.E. Shirokov, T.V. Shulman. On superactivation of zero-error capacities and reversibility of a quantum channel. Commun. Math. Phys. V.335, N3, pp.1159-1179 (2015).

[S15] M.E. Shirokov. On channels with positive quantum zero-error capacity having vanishing n-shot capacity. Quantum Information Processing, 2015, 14:8, 3057-3074.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, U.K., 2000.

[Wat11] J. Watrous. https://cs.uwaterloo.ca/∼watrous/LectureNotes.html . Theory of quantum information, fall 2011, lecture 5.

[Dev05] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. IEEE Trans. Inf. Theory 51, 44 (2005) (quant-ph/0304127v6).

[CLLW15] R. Cleve, D. Leung, L. Liu and C. Wang. Near-linear constructions of exact unitary 2-designs. *arXiv:1501.04592*, 2015.

[DCEL09] C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80:012304, Jul 2009.

[YDY14] N. Yu, R. Duan and M. Ying. Distinguishability of Quantum States by Positive Operator-Valued Measures with Positive Partial Transpose. *IEEE Transactions on Information Theory*, 60(4):2069-2079, 2014.

6 Appendix

For a channel $\mathcal{E}$ with Kraus representation $\mathcal{E}(\rho) = \sum E_i \rho E_i^\dagger$ (see [NC00] for example), its noncommutative graph [DUAN09, DSW13] $G(\mathcal{E})$ is defined as the subspace spanned by $\{E_i^\dagger E_j : i, j\}$. In [SS15], superactivation on the zero-error quantum capacity is studied. For a channel $\mathcal{E}$ with no one-shot zero-error quantum capacity, if one of the following conditions hold, $\mathcal{E}$ cannot be superactivated with any other channel.

a) $G(\mathcal{E})$ contains a maximal commutative *-subalgebra whose dimension is the dimension of the input state space. In other words, $G(\mathcal{E})$ contains all matrices which are diagonal with respect to some basis.

b) $G(\mathcal{E})$ is an algebra. In other words, it is closed under matrix production.

In particular, an inductive argument than implies that $\mathcal{E}$ has no zero-error quantum capacity.

In this Appendix, we will show that $G(\mathcal{N}_d)$ violates both conditions, so, our result cannot be inferred from [SS15].

First, we observe that the Kraus space of $\mathcal{N}_d$ is spanned by

$$\{(I \otimes \langle k|)P(I \otimes V) \otimes |V\rangle_{V_B} \otimes |V\rangle_{V_E} : V \in \mathcal{G}, 1 \le k \le d\} = \{Z_k \otimes \langle k|V \otimes |V\rangle_{V_B} \otimes |V\rangle_{V_E} : V \in \mathcal{G}, 1 \le k \le d\},$$

where $\mathcal{G}$ is a two-design as described in the main text. Therefore,

$$G(\mathcal{N}_d) = \text{span}\{Z_{k-l} \otimes V^\dagger |l\rangle\langle k| V : V \in \mathcal{G}, 1 \le k, l \le d\}.$$

For any k, l, we can calculate the span of $\{V^\dagger |l\rangle\langle k| V \,:\, V \in \mathcal{G}\}$ by considering the isomorphism from M to $(I \otimes M)\Phi(I \otimes M^\dagger)$ where $\Phi = |\Phi\rangle\langle\Phi|$ and $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle\, |i\rangle$ and by averaging over V:

$$\begin{aligned}
& \mathbb{E}_{V \in \mathcal{G}} (V^\dagger |l\rangle\langle k| V \otimes I)\ \Phi\ (V^\dagger |l\rangle\langle k| V \otimes I)^\dagger \\
= \ & \mathbb{E}_{V \in \mathcal{G}} (V^\dagger \otimes V^T)(|k\rangle\langle k| \otimes |l\rangle\langle l|)(V^\dagger \otimes V^T)^\dagger \\
= \ & \frac{1 - \delta_{k,l}/d}{d^2 - 1}(I - \Phi) + \frac{\delta_{k,l}}{d}\,\Phi\,.
\end{aligned}$$

Inverting the isomorphism, the span of $\{V^\dagger |l\rangle\langle k| V \,:\, V \in \mathcal{G}\}$ is the whole matrix space when $k = l$, and is the space of all traceless matrices when $k \neq l$. Note that in particular, $G(\mathcal{N}_d)$ does not contain $Z \otimes I$.

Now, if condition (a) holds, then there are d^2 linearly independent commuting matrices in $G(\mathcal{N}_d)$, which together with $Z \otimes I$, gives $d^2 + 1$ linearly independent commuting matrices in $\mathcal{B}(\mathbb{C})$, a contradiction. To see that condition (b) does not hold, note that $I \otimes Z, Z \otimes Z^\dagger \in G(\mathcal{N}_d)$ but their product $Z \otimes I \notin G(\mathcal{N}_d)$.