Quantum Action-Dependent Channels

Michael Korenberg and Uzi Pereg

*Faculty of Electrical and Computer Engineering, Technion
†Helen Diller Quantum Center, Technion
Email: mkorenberg@campus.technion.ac.il, uzipereg@technion.ac.il

Abstract

We introduce the quantum action-dependent channel. The model can be viewed as a quantum analogue of the classical action-dependent channel model. The Gel'fand-Pinsker channel has two inputs, Alice's transmission and the input environment. The action-dependent model allows the transmitter to affect the channel's environment. Specifically, Alice encodes her message into a quantum action, which in turn influences the channel's environment through an action channel. Alice also has side information. In the quantum model, she cannot have a copy of the environment state due to the no-cloning theorem. Instead, she shares entanglement with this environment,as a result, her measurement can lead to a collapse of the environment state. We derive an achievable communication rate for the transmission of messages via the quantum action-dependent channel.

I. Introduction

A fundamental problem in information theory is the characterization of reliable communication over channels affected by *random parameters*, commonly referred to as channel states. Beginning with Shannon's seminal work on channels with side information [1], the study of channels with random parameters has revealed the crucial role of side information at the encoder or decoder. Gel'fand and Pinsker established the capacity for channels with non-causal state information at the encoder [2]. Costa's "writing on dirty paper" result [3] further extended it to Gaussian channels. These works laid the foundation for a rich literature on random-parameter models in both point-to-point and multi-user settings [4–7].

In the random-parameter paradigm, the parameters are typically drawn from nature and cannot be controlled by the communicating parties [2]. The parameters influence the channel by altering its transition law. In the classical setting, the channel is described in terms of a probability function $P_{Y|X,S}(\cdot|x,s)$, where X represents Alice's transmission and Y is Bob's observation at the channel output. The random parameter S has a specified distribution and its variation can significantly affect the channel output. For this reason, side information, i.e., the knowledge of S, has a profound effect on capacity.

Weissman [8] introduced the *action-dependent channel*. In this model, the encoder first selects an action sequence, which in turn, generates the channel parameters in a noisy fashion. The overall channel input then depends on both the message and the induced parameters. This two-stage procedure captures a broad class of practical problems, such as memories with defects, magnetic recording with rewriting, and other scenarios in which the transmitter can probe or partially control the channel before communication, as was demonstrated in [9]. For example, a two-stage coding strategy can steer a defective memory to improve reliability: first, the transmitter writes to the memory and immediately tries to read it back to learn about defects. Then, the transmitter rewrites the defective bits based on that information. The flexibility of this model led to its extension in several directions. For instance, the concept of probing capacity was introduced to quantify the maximum rate at which the channel state can be learned through actions [10], and other works incorporated cost constraints on these actions [11]. The framework has also proven valuable in multi-user communication, with generalizations to broadcast channels [12, 13] and multiple-access channels [14]. Furthermore, its implications for security have been explored in the context of wiretap channels [15, 16] and other secure communication settings [17], where the action channel acts as a broadcast channel influenced by the transmitter's actions.

The ongoing development of quantum information theory is foundational for engineering next-generation communication and computation systems [18–20]. By leveraging the principles of quantum mechanics, this field aims to overcome the limitations of classical technologies. This quantum framework also unlocks entirely new phenomena with no classical parallel, such as entanglement, i.e., the strongest resource of quantum correlation, as well as the no-cloning theorem, which forbids the perfect duplication of unknown quantum information, motivating a deeper study of fundamental communication limits. Action dependence is relevant in quantum communication as well. For example, a quantum measurement by the encoder on the transmission system could result in a state collapse of the channel input environment.

Quantum environment-dependent channels are crucial for studying scenarios that involve not only the transmission of a message, but also parameter estimation, a central task in fields such as quantum metrology. These types of quantum Gel'fand-Pinsker channels have been studied, both with and without entanglement assistance [21] (see also [22]). The security implications have also been explored in the quantum setting through wiretap channels [23] and covert communication [24]. Other variations include scenarios in which the decoder performs parameter estimation [25]. The action-dependent framework has not yet been studied in the quantum literature thus far.

In this paper, we introduce the quantum action-dependent channel. Our action dependence model modifies the environment-dependent paradigm by allowing the transmitter's actions to influence a quantum environment; this environment then generates the channel's governing parameters, giving the message direct influence over the communication conditions. Specifically, an

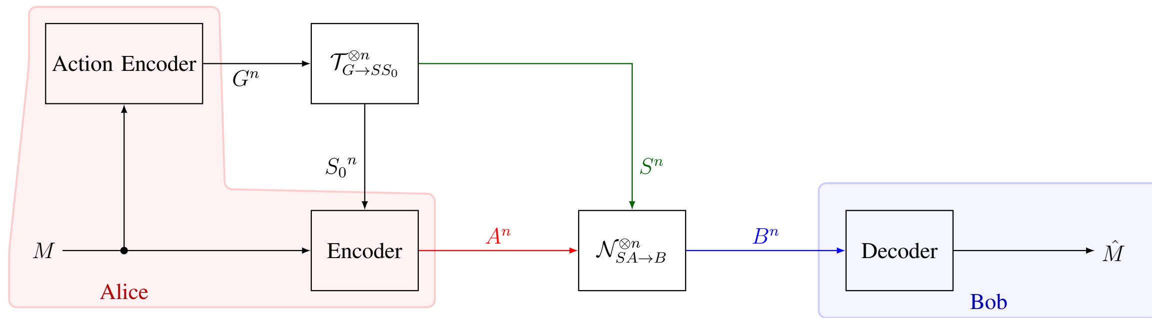

Fig. 1. Coding over a quantum action-dependent channel.

encoder (Alice) first encodes a classical message M into an action sequence G^n, which is fed into a quantum action channel $\mathcal{T}^{\otimes n}_{G\to SS_0}$. This channel produces side information S_0^n, for Alice, and an environment system S^n. Alice then encodes the message and the side information into her transmission A^n, which is sent through the quantum communication channel $\mathcal{N}^{\otimes n}_{SA\to B}$. The receiver (Bob) obtains the output sequence B^n, and performs a measurement in order to estimate Alice's message.

The framework is the quantum counterpart of the classical action-dependent channel introduced by Weissman [8]. However, the generalization is nontrivial due to fundamental quantum principles such as the no-cloning theorem. While a classical channel parameter can be perfectly copied and then sent back to the transmitter, an unknown quantum state cannot. Consequently, the side information is modeled as entanglement shared between two distinct systems, S and S_0, where S represents the environment affecting the channel, and S_0 is the side information available to Alice.

We derive an achievable rate using one-shot information-theoretic methods. These techniques establish non-asymptotic performance bounds by directly analyzing the error probability for a finite number of channel uses, rather than relying on asymptotic arguments. The introduction of action dependence makes this analysis more challenging than in previous environment-dependent channel models [23, 25]. In previous settings, the shared quantum state between the transmitter and the environment is set by an outside source. Whereas here, the transmitter's action *induces* the shared entangled state. Consequently, our analysis must account for this additional layer of control. The formula of our capacity bound thus includes optimization over not only the input state, but also the a quantum ensemble for the sender's action.

II. Notation and Basic Definitions

We use standard notation from quantum information theory. Quantum systems are denoted by uppercase letters (e.g., A, B) and their corresponding finite-dimensional Hilbert spaces by $\mathcal{H}_A, \mathcal{H}_B$. The set of density operators on $\mathcal{H}_A$ is $\mathscr{D}(\mathcal{H}_A)$. Quantum states (density operators) are denoted by greek letter, e.g., ρ, σ. A POVM is a set of positive semi-definite operators $\{D_m\}$ that satisfy $\sum_m D_m = \mathbb{1}$, where $\mathbb{1}$ denotes the identity operator. If the quantum state before the measurement is ρ, then the probability of an outcome m is $\Pr(m) = \mathrm{Tr}(D_m\rho)$.

A quantum channel $\mathcal{N}_{A\to B}$ is a completely positive trace-preserving (CPTP) map. Here, we consider a quantum channel $\mathcal{N}_{SA\to B}$, where A, S, and B are associated with the transmitter (Alice), the channel environment ("channel state"), and the receiver (Bob). The channel can be represented through its Stinespring dilation, in terms of an isometry $V_{SA\to BE}$ that couples the output system to an auxiliary environment E. Namely, $\mathcal{N}_{SA\to B}(\rho_{SA}) = \mathrm{Tr}_E\left[V\rho_{SA}V^\dagger\right]$. We assume that the channel is memoryless. That is, if an input sequence $(S^n, A^n) \equiv (S_1, A_1), \dots, (S_n, A_n)$ is transmitted through the channel, then the input state $\rho_{S^nA^n}$ undergoes the tensor-product map $\mathcal{N}^{\otimes n}_{SA\to B}$. We will see that in the action-dependent model, the channel environment S^n is affected by the encoding operation. See Section V.

For a quantum state ρ, the von Neumann entropy is $H(\rho) = -\mathrm{Tr}(\rho\log\rho)$. For a bipartite state $\rho_{AB} \in \mathscr{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, the quantum mutual information is defined as $I(A;B)_\rho = H(\rho_A) + H(\rho_B) - H(\rho_{AB})$, and the conditional entropy as $H(A|B)_\rho = H(\rho_{AB}) - H(\rho_B)$. Unlike its classical counterpart, the quantum conditional entropy can be negative.

The quantum relative entropy between two states ρ and σ in $\mathscr{D}(\mathcal{H})$ is defined as $D(\rho\|\sigma) = \mathrm{Tr}\left(\rho\left(\log\rho - \log\sigma\right)\right)$ if $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$, and $D(\rho\|\sigma) = +\infty$ otherwise. The Sandwiched Rényi Divergence [26] is defined as $\tilde{D}_\alpha\left(\rho\|\sigma\right) := \frac{1}{\alpha-1}\log\mathrm{Tr}\left[\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right]^\alpha$.

Other key definitions are given below [27]:

1) **Pinching**: For a Hermitian operator $A = \sum_i a_i\Pi_i$ with projectors Π_i onto its eigenspaces, the pinching map is $\mathcal{E}_A(B) := \sum_i \Pi_i B\Pi_i$.
2) **Fidelity**: $F(\rho,\sigma) := \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2$.
3) **Purified Distance**: $P(\rho,\sigma) := \sqrt{1 - F^2(\rho,\sigma)}$.

III. Action-Dependent Coding

Before presenting our main results, we introduce a code for the transmission of messages via a quantum action-dependent channel, where the encoder selects an action that affects the channel environment. Specifically, Alice has two roles: she encodes both the action G and the transmission A through the channel. Her action encoder sends G through an action channel $\mathcal{T}_{G\to SS_0}$ that produces Alice's side information S_0 and the channel environment S.

Definition 1 (Action-Dependent Code). An (M, n) code for communication over a quantum action-dependent channel $\mathcal{N}_{SA\to B}$, that is governed by an action channel $\mathcal{T}_{G\to SS_0}$, consists of:

1) An *encoder* that comprises two stages:
   - action encoder that prepares a quantum action state $\rho^{(m)}_{G^n} \in \mathscr{D}(\mathcal{H}_G^{\otimes n})$, for $m \in \{1, \dots, M\} = \mathsf{M}$.
   - transmission encoder $\mathcal{E}^{(m)}_{S_0^n \to A^n}$ that receives the side-information S_0^n and prepares the channel input A^n.
2) A *decoding measurement*, i.e., a POVM $\{D_m\}_{m=1}^M$ on the output Hilbert space $\mathcal{H}_B^{\otimes n}$.

The coding scheme works as shown in Figure 1. Alice selects a uniform message $m \in \mathsf{M}$. She first prepares the action state $\rho^{(m)}_{G^n}$. The action system G^n which is then sent through the action channel, producing

$$\rho^{(m)}_{S^n S_0^n} = \mathcal{T}^{\otimes n}_{G\to SS_0}(\rho^{(m)}_{G^n}). \tag{1}$$

Given the side information S_0^n, Alice applies the transmission encoder:

$$\rho^{(m)}_{S^n A^n} = \mathrm{id}_{S^n} \otimes \mathcal{E}^{(m)}_{S_0^n\to A^n}(\rho^{(m)}_{S^n S_0^n}). \tag{2}$$

Both the input environment S^n and Alice's transmission A^n are fed into the channel $\mathcal{N}^{\otimes n}_{SA\to B}$, hence

$$\rho^{(m)}_{B^n} = \mathcal{N}^{\otimes n}_{SA\to B}(\rho^{(m)}_{S^n A^n}). \tag{3}$$

Bob receives B^n. He performs the measurement $\{D_m\}$ to obtain an estimate of Alice's message.

For an $(\mathsf{M}, n, \varepsilon)$ code, *average probability of error* is bounded by ε, i.e.,

$$\bar{p}_e^{(n)} := 1 - \frac{1}{M}\sum_{m\in\mathsf{M}} \mathrm{Tr}\Big[D_m\, \rho^{(m)}_{B^n}\Big] \le \varepsilon. \tag{4}$$

Definition 2 (Achievable Rate). A communication rate R is said to be achievable for the quantum action-dependent channel $\mathcal{N}_{SA\to B}$, with respect to the action channel $\mathcal{T}_{G\to SS_0}$, if for every $\varepsilon, \delta > 0$ and sufficiently large n, there exists a $(2^{n(R-\delta)}, n, \varepsilon)$ code. The channel capacity C_{QAD} is defined as the supremum of all achievable rates, where the subscript 'QAD' indicates the quantum action dependence.

IV. Main Result

We now state our main result, an achievable rate for the quantum action-dependent channel.

Theorem 1 (Achievable Rate). The following rate is achievable for the quantum action-dependent channel:

$$\mathsf{R}_{\text{low}} = I(VU; B)_\rho - I(V; S|U)_\rho, \tag{5}$$

with respect to a classical auxiliary pair $(V, U) \sim p_{VU}$, a state collection $\{\sigma_G^u\}$, and an encoding channel $\mathcal{F}^v_{S_0\to A}$, such that

$$\sigma^u_{SS_0} = \mathcal{T}_{G\to SS_0}(\sigma^u_G), \tag{6}$$

$$\rho^{v,u}_{SA} = \mathrm{id}_S \otimes \mathcal{F}^v_{S_0\to A}(\sigma^u_{SS_0}), \tag{7}$$

$$\rho_{VUSA} = \sum_{u,v} p_{V,U}(v,u)\, |v\rangle\langle v|_V \otimes |u\rangle\langle u|_U \otimes \rho^{v,u}_{SA}, \tag{8}$$

where $\rho_V^u = \sum_{v\in\mathcal{V}} p_{V|U}(v|u)\, |v\rangle\langle v|$. Hence, $\rho_{VUB} = \mathrm{id}_{VU} \otimes \mathcal{N}_{SA\to B}(\rho_{VUSA})$. Equivalently, the capacity of the quantum action-dependent channel $\mathcal{N}_{SA\to B}$ satisfies

$$C_{\text{QAD}} \ge \max_{p_{VU},\, \sigma^u_G,\, \mathcal{F}^v_{S_0\to A}} [I(VU; B)_\rho - I(V; S|U)_\rho]. \tag{9}$$

Remark 1. Previous work has considered side information when the quantum state σ_{SS_0} is fixed and dictated by the model [23–25]. This fixed state represents the entanglement between the environment subsystem S and the side-information subsystem S_0, which is accessible to Alice. By utilizing the side information S_0, Alice's encoder can generate entanglement between the channel input and its environment S. In this sense, we can regard Alice as being entangled with the channel, and this is a key feature of quantum side information at the transmitter. In our model, however, the state $\sigma^u_{SS_0}$ depends on the action encoding u chosen by Alice. This added degree of freedom allows Alice to influence the channel environment S by selecting different actions. This is analogous to the classical action-dependent channel model in [8], where the channel parameter is a noisy version of Alice's action.

V. One-Shot Code Construction

In this section, we introduce a coding scheme for the one-shot setting, of $n = 1$, over the quantum action-dependent channel (see Figure 1). Let $\mathcal{N}_{SA\to B}$ be a quantum action-dependent channel. Let $\mathcal{T}_{G\to SS_0}$ be the action channel, that generates Alice's side information subsystem S_0 and the environment subsystem S. Consider the quantum states defined in Theorem 1: $\sigma^u_{SS_0}$ is the entangled state produced by the action channel $\mathcal{T}_{G\to SS_0}$, hence, ρ_{VUSA} is the channel input, and the corresponding output is $\rho_{UVB} = \mathrm{id}_{UV} \otimes \mathcal{N}_{SA\to B}(\rho_{UVSA})$.

We now describe the one-shot coding scheme.

A. Codebook

Let $R,\ R_S > 0$ denote the coding rates corresponding to the information and action encodings. First, the action-encoding codebook $\mathcal{C}_U := \{u(m)\}_{m\in\{1,\dots,2^R\}}$ is sampled from a random set of i.i.d. codebooks $\mathbf{C}_U$, distributed according to p_U. Then, let $\mathcal{C}_V(m) := \{v(m,1), v(m,2),\dots,v(m,2^{R_S})\}$ be 2^R sub-codebooks such that $v(m,\ell)$ are drawn independently according to $p_{V|U}(\cdot|u(m))$. Both are revealed to Alice and Bob. The overall codebook is $\mathcal{C} := \mathcal{C}_U \cup \{\mathcal{C}_V(m)\}$. We use the notation $\mathcal{C}$ for a deterministic codebook and $\mathbf{C}$ for a random codebook.

B. Encoder

Our encoding scheme consists of two parts, action encoding and message encoding:

1) **Action Encoding:** For each value u, let $\left|\sigma^u_{GK_0}\right\rangle$ be a purification of the state σ^u_G, with K_0 as a reference.
Given a message m, prepare $\left|\sigma^{u(m)}_{GK_0}\right\rangle$, and transmit G through the action channel.
Consider a Stinespring dilation of the action channel, with an isometry $T_{G\to SS_0K_1}$, where K_1 is appended the channel environment S and the side information S_0. Upon the action encoding above, this channel acts on $\left|\sigma^{u(m)}_{GK_0}\right\rangle$ to produce the joint state $\left|\psi^{u(m)}_{SS_0K_1K_0}\right\rangle$:

$$\left|\psi^{u(m)}_{SS_0K_1K_0}\right\rangle = T_{G\to SS_0K_1} \otimes \mathbb{1}_{K_0} \left|\sigma^{u(m)}_{GK_0}\right\rangle. \tag{10}$$

2) **Message Encoding:** Alice implements the encoding map $\mathcal{E}^{v(m,\ell)}_{S_0\to A}$ on the side-information subsystem S_0. Consider a Stinespring dilation with an isometry $E^{v(m,\ell)}_{S_0\to AT}$. This produces the channel input state

$$\left|\rho^{v(m,\ell),u(m)}_{SATK_1K_0}\right\rangle = (\mathbb{1}_S \otimes E^{v(m,\ell)}_{S_0\to AT} \otimes \mathbb{1}_{K_1K_0}) \left|\psi^{u(m)}_{SS_0K_1K_0}\right\rangle \tag{11}$$

Overall, Alice's state is

$$\left|\phi^m_{SATK_1K_0L}\right\rangle = \frac{1}{\sqrt{2^{R_S}}} \sum_{\ell=1}^{2^{R_S}} \left|\rho^{v(m,\ell),u(m)}_{SATK_1K_0}\right\rangle \otimes |\ell\rangle. \tag{12}$$

According to Uhlmann's Theorem [27], for every pair of purifications $|\psi\rangle_{AB}$ and $|\phi\rangle_{AC}$ of ρ_A and σ_A, respectively, there exists an isometry $W_{C\to B}$ such that $F(\rho_A,\sigma_A) = F(|\psi\rangle\langle\psi|_{AB}, W(|\phi\rangle\langle\phi|_{AC})W^\dagger)$. Then, in our case, it follows that there exists a set of isometries,

$$\{W^m_{S_0\to ATL}\}_{m\in\mathsf{M}} \in \mathscr{L}\left(\mathcal{H}_{S_0} \to \mathcal{H}_A \otimes \mathcal{H}_T \otimes \mathcal{H}_L\right) \tag{13}$$

that map from $\left|\psi^{u(m)}_{SS_0K_1K_0}\right\rangle$ to $\left|\phi^m_{SATK_1K_0L}\right\rangle$, or equivalently, from $\left|\psi^{u(m)}_{SS_0K_1K_0}\right\rangle$ to $\left|\rho^{v(m,\ell),u(m)}_{SATK_1K_0}\right\rangle$.
Using the short notation $\tilde{W}^m = \mathbb{1}_S \otimes W^m_{S_0\to ATL} \otimes \mathbb{1}_{K_1K_0}$,

$$P\left(\phi^m_{SATK_1K_0L}, \tilde{W}^m(\psi^{u(m)}_{SS_0K_1K_0})\tilde{W}^{\dagger m}\right) = P\left(\frac{1}{2^{R_S}} \sum_{\ell\in\mathsf{L}} \rho^{v(m,\ell),u(m)}_S, \sigma^{u(m)}_S\right). \tag{14}$$

Given a message m, Alice applies the isometry $W^m_{S_0\to ATL}$ on $\left|\psi^{u(m)}_{SS_0K_1K_0}\right\rangle$ and transmits A over the action-dependent channel.

C. Decoding

We would like to design a POVM measurement $\{D_m\}$ on the system B that distinguishes between the states $\{\rho_B^{(m)}\}_{m\in\mathsf{M}}$ with high probability. Let $\mathcal{E}_1$ be the pinching map associated with $\rho_{VU}\otimes\rho_B$ such that: $\rho_{VU}\otimes\rho_B=\sum_\lambda \lambda\Pi_\lambda$ is the spectral decomposition of $\rho_{VU}\otimes\rho_B$. The pinching map $\mathcal{E}_1$ is defined as: $\mathcal{E}_1(\rho)=\sum_\lambda \Pi_\lambda\rho\Pi_\lambda$, where $\{\Pi_\lambda\}$ are the orthogonal projectors onto the eigenspace of $\rho_{VU}\otimes\rho_B$. We define ν_1 as the number of distinct nonnegative eigenvalues of $\rho_{VU}\otimes\rho_B$. Now $\mathcal{E}_1(\rho_{VUB})$ is block-diagonal in the eigenbasis of $\rho_{VU}\otimes\rho_B$, thus it commutes with $\rho_{VU}\otimes\rho_B$. The pinching of ρ_{VUB} with respect to $\rho_{VU}\otimes\rho_B$ is defined as:

$$\mathcal{E}_1(\rho_{VUB})=\sum_{\lambda=1}^{\nu_1}\Pi_\lambda\left(\sum_{v,u}p_{VU}(v,u)\,|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\otimes\rho_B^{v,u}\right)\Pi_\lambda \tag{15}$$

For two Hermitian matrices A and B, we define the projection $\{A\geq B\}$ as $\sum_{\lambda\geq 0}\lambda P_\lambda$, where the spectral decomposition of $A-B$ is given as $\sum_\lambda \lambda P_\lambda$. In this notation, P_λ is the projection to the eigenspace corresponding to the eigenvalue λ. Then, let

$$\Pi_{VUB}=\{\mathcal{E}_1\left(\rho_{VUB}\right)\geq 2^{R+R_S}\rho_{VU}\otimes\rho_B\}. \tag{16}$$

For every $m\in\mathsf{M},\ell\in\mathsf{L}$, we define:

$$\gamma(m,\ell)=\mathrm{Tr}_{VU}\left[\Pi_{VUB}\left(|v(m,\ell)\rangle\langle v(m,\ell)|\otimes|u(m)\rangle\langle u(m)|\otimes\mathbb{1}_B\right)\right]. \tag{17}$$

Our set of POVM operators are then normalized as

$$\beta(m,\ell)=\left(\sum_{m',\ell'}\gamma(m',\ell')\right)^{-\frac{1}{2}}\gamma(m,\ell)\left(\sum_{m',\ell'}\gamma(m',\ell')\right)^{-\frac{1}{2}} \tag{18}$$

for $(m,\ell)\in\mathsf{M}\times\mathsf{L}$.

We are now ready to state our one-shot result.

Proposition 2 (One-shot error probability). Let $\alpha\in\left(0,\frac{1}{2}\right)$. Then, the average error probability is bounded by:

$$\mathbb{E}_{\mathbf{C}}[\bar{p}_e^{(1)}]\leq 12\cdot\nu_1^\alpha 2^{\alpha\left[R+R_S-\tilde{D}_{1-\alpha}(\rho_{VUB}||\rho_{VU}\otimes\rho_B)\right]}+\frac{2}{\alpha\ln 2}\frac{\nu_2^\alpha}{2^{\alpha R_S}}2^{\alpha\tilde{D}_{1+\alpha}(\rho_{VUS}\|\rho_{V-U-S})} \tag{19}$$

with

$$\rho_{V-U-S}=\sum_u p_U(u)\,|u\rangle\langle u|\otimes\rho_V^u\otimes\rho_S^u \tag{20}$$

where ν_1 is the number of distinct eigenvalues of $\rho_{VU}\otimes\rho_B$, and ν_2 is the maximum number of distinct eigenvalues of $\{\rho_S^{u(m)}\}_{\forall m\in\mathsf{M}}$.

The proof of Proposition 2 is given in Appendix A.

VI. Proof of Theorem 1

We consider the average error probability as the number of channel uses n goes to infinity. Let d_{VUB} be the dimension of $\mathcal{H}_V\otimes\mathcal{H}_U\otimes\mathcal{H}_B$, and d_S be the dimension of $\mathcal{H}_S$. As shown in [28, Lemma 3.9], we can bound ν_1 and ν_2 as follows:

$$\begin{aligned}\nu_1&\leq(n+1)^{d_{VUB}-1},\\ \nu_2&\leq(n+1)^{d_S-1}.\end{aligned} \tag{21}$$

Based on Proposition 2 for n uses of the channel, there exists a (deterministic) codebook $\mathcal{C}$ such that:

$$\begin{aligned}\bar{p}_e^{(n)}\leq&12\,(n+1)^{\alpha(d_{VUB}-1)}\,2^{\alpha\left[n(R+R_S)-\tilde{D}_{1-\alpha}\left(\rho_{VUB}^{\otimes n}||\rho_{VU}^{\otimes n}\otimes\rho_B^{\otimes n}\right)\right]}\\ &+\frac{2}{\alpha\ln 2}\frac{(n+1)^{\alpha(d_S-1)}}{2^{\alpha nR_S}}2^{\alpha\tilde{D}_{1+\alpha}(\rho_{VUS}^{\otimes n}\|\rho_{V-U-S}^{\otimes n})}.\end{aligned} \tag{22}$$

Hence, the error probability tends to zero as $n\to\infty$, provided that

$$R+R_S<\frac{1}{n}\tilde{D}_{1-\alpha}\left(\rho_{VUB}^{\otimes n}||\rho_{VU}^{\otimes n}\otimes\rho_B^{\otimes n}\right)-\alpha(d_{VUB}-1)\frac{1}{n}\log\left(n+1\right), \tag{23}$$

and

$$R_S>\frac{1}{n}\tilde{D}_{1+\alpha}\left(\rho_{VUS}^{\otimes n}||\rho_{V-U-S}^{\otimes n}\right)+\frac{\alpha(d_S-1)}{n}\log\left(n+1\right). \tag{24}$$

In the limit of $n \to \infty$ and $\alpha \to 0$, the bounds reduce to [27]

$$R_S > I(V;S|U)_\rho + \frac{\delta}{3}, \tag{25}$$

$$R + R_S < I(VU;B)_\rho - \frac{\delta}{3}. \tag{26}$$

Where $\delta > 0$ is arbitrarily small. We deduce that the error probability tends to zero for

$$R < I(VU;B)_\rho - I(V;S|U)_\rho - \delta. \qquad \square \tag{27}$$

Appendix A
Proof of Proposition 2

Let $\Theta_B(m)$ be the state Bob receives:

$$\Theta_B(m) = \mathrm{Tr}_{TK_1K_0L}\left[\mathcal{N}_{SA\to B}\left(\tilde{W}^m(\psi^{u(m)}_{SS_0K_1K_0})\tilde{W}^{\dagger m}\right)\right] \tag{28}$$

given that the message m was transmitted. Furthermore, let $\hat{\Theta}_B(m)$ be the average state that Bob receives, when averaged over the sub-codebook of $\mathcal{C}_V(m)$:

$$\hat{\Theta}_B(m) = \frac{1}{2^{R_S}}\sum_{\ell\in\mathsf{L}}\rho_B^{v(m,\ell),u(m)}. \tag{29}$$

By the symmetry of encoding and decoding, we may assume without loss of generality that Alice sent $m = 1$. Consider the pinching-based decoder $\{\beta(m,\ell)\}_{(m,\ell)\in\mathsf{M}\times\mathsf{L}}$ that has been constructed in Subsection V-C. We now bound the average error probability as follows:

$$\begin{aligned}
\mathbb{E}_{\mathbf{C}}[\bar{p}_e^{(1)}] &= \Pr\Big(\hat{M}\neq 1 \mid M=1\Big)\\
&\overset{(a)}{=} \mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[\left(\sum_{m'\neq 1,\ell}\beta(m',\ell)\right)\Theta_B(1)\right]\right]\\
&\overset{(b)}{\leq} 2\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[\left(\sum_{m'\neq 1,\ell}\beta(m',\ell)\right)\hat{\Theta}_B(1)\right]\right] + 2\mathbb{E}_{\mathbf{C}}\left\{\left|\sqrt{\mathrm{Tr}\left[\left(\sum_{m'\neq 1,\ell}\beta(m',\ell)\right)\Theta_B(1)\right]}\right.\right.\\
&\quad\left.\left.-\sqrt{\mathrm{Tr}\left[\left(\sum_{m'\neq 1,\ell}\beta(m',\ell)\right)\hat{\Theta}_B(1)\right]}\right|^2\right\}\\
&\overset{(c)}{\leq} 2\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[\left(\sum_{m'\neq 1,\ell}\beta(m',\ell)\right)\hat{\Theta}_B(1)\right]\right] + 2\mathbb{E}_{\mathbf{C}}\left[P\left(\Theta_B(1),\hat{\Theta}_B(1)\right)^2\right]
\end{aligned} \tag{30}$$

where (a) follows since the error events are disjoint, (b) is obtained by rewriting the left-hand side term as $A = \left(\sqrt{B}+\sqrt{A}-\sqrt{B}\right)^2$ and then applying the inequality for non-commutative x and y: $(x+y)^2 \leq 2(x^2+y^2)$. (c) is obtained by $\sum_{m'\neq 1,\ell}\beta(m',\ell)\leq \mathbb{1}$, and for any two quantum states $\rho,\sigma\in\mathscr{D}(\mathcal{H})$ and an operator $0\leq\Delta\leq\mathbb{1}$ we have the following inequality: $\left|\sqrt{\mathrm{Tr}[\Delta\sigma]}-\sqrt{\mathrm{Tr}[\Delta\rho]}\right|\leq P(\sigma,\rho)$ [23, Fact 7].

The first term on the right-hand side of (30) can be written as

$$\begin{aligned}
\sum_{m'\neq 1,\ell}\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[(\beta(m',\ell))\,\hat{\Theta}_B(1)\right]\right] &= \frac{1}{R_S}\sum_{\ell'}\sum_{m'\neq 1,\ell}\mathbb{E}_C\left[\mathrm{Tr}\left[(\beta(m',\ell))\,\rho_B^{v(1,\ell'),u(1)}\right]\right]\\
&= \sum_{m'\neq 1,\ell}\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[(\beta(m',\ell))\,\rho_B^{v(1,1),u(1)}\right]\right]\\
&\leq \mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\Big[(\mathbb{1}-\beta(1,1))\,\rho_B^{v(1,1),u(1)}\Big]\right]\\
&\leq 2\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\Big[(\mathbb{1}-\gamma(1,1))\,\rho_B^{v(1,1),u(1)}\Big]\right] + 4\sum_{(m',\ell)\neq(1,1)}\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\Big[(\gamma(m',\ell))\,\rho_B^{v(1,1),u(1)}\Big]\right],
\end{aligned} \tag{31}$$

where the last inequality is based on the Hayashi-Nagaoka operator inequality [29]: let $0 \leq S \leq \mathbb{1}, T$ be positive semi-definite operators on a Hilbert space $\mathcal{H}$. then

$$\mathbb{1} - (S+T)^{-\frac{1}{2}} S (S+T)^{-\frac{1}{2}} \leq 2(\mathbb{1} - S) + 4T. \tag{32}$$

In our case, we have $S = \gamma(1,1)$ and $T = \sum_{(m',\ell)\neq(1,1)} \gamma(m',\ell)$. The next steps follow similar lines as in [23, 24]. We obtain an upper bound on each term on the right-hand side of (31) by using the following lemmas.

Lemma 3. For every $\alpha \in \left(0, \frac{1}{2}\right)$, and $R, R_S > 0$ we have:

$$\mathrm{Tr}[(\mathbb{1} - \Pi_{VUB})\,\rho_{VUB}] \leq \nu_1^{\alpha} 2^{\alpha\left[R+R_S-\tilde{D}_{1-\alpha}(\rho_{VUB}||\rho_{VU}\otimes\rho_B)\right]} \tag{33}$$

$$2^{R+R_S}\,\mathrm{Tr}\left[\Pi_{VUB}\,(\rho_{VU}\otimes\rho_B)\right] \leq \nu_1^{\alpha} 2^{\alpha\left[R+R_S-\tilde{D}_{1-\alpha}(\rho_{VUB}||\rho_{VU}\otimes\rho_B)\right]} \tag{34}$$

The proof of Lemma 3 is given in Appendix B.

Lemma 4 (see [23, Lemma 7]). Let $\rho_{VUS} = \mathrm{Tr}\left[\rho_{VUSA}\right]$ be a classical-quantum state. Furthermore, let $\mathcal{C} = \{v(1), \ldots v(2^{R_S}), u\}$ be a collection of random variables such that for every $i \in \{1, \ldots, 2^{R_S}\}$, $(v(i), u) \sim p_{VU}$, $(v(i), v(i')) \sim p_{V(i),U} \cdot p_{V(i'),U}$, We consider the following state:

$$\tau_S^{\mathcal{C}} \triangleq \frac{1}{2^{R_S}} \sum_{\ell\in\mathsf{L}} \rho_S^{v(m,\ell),u(\ell)}. \tag{35}$$

Then, for $\alpha \in (0,1)$, there exists a constant $\nu_2 \geq 0$ such that:

$$\mathbb{E}_{\mathbf{C}}\left[\tilde{D}_{1+\alpha}(\tau_S^{\mathcal{C}}\|\rho_S^{u})\right] \leq \frac{1}{\alpha \ln 2} \frac{\nu_2^{\alpha}}{2^{\alpha R_S}} 2^{\alpha \tilde{D}_{1+\alpha}(\rho_{VUS}\|\rho_{V-U-S})} \tag{36}$$

Where $\rho_{V-U-S} \triangleq \sum_u p_U(u)|u\rangle\langle u|_U \otimes \rho_{V|u} \otimes \rho_{S|u}$, ν_2 is the maximum number of distinct eigenvalues of the states $\{\rho_{S|u}\}_u$.

In the next step, we will bound each of the terms in (31), starting with the first one on the left:

$$\begin{aligned}
&2\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[(\mathbb{1} - \gamma(1,1))\,\rho_B^{v(1,1),u(1)}\right]\right] \\
&\overset{(a)}{=} 2\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[(\mathbb{1} - \mathrm{Tr}_{VU}[\Pi_{VUB}(|v(1,1)\rangle\langle v(1,1)| \otimes |u(1)\rangle\langle u(1)| \otimes \mathbb{1}_B)])\,\rho_B^{v(1,1),u(1)}\right]\right] \\
&= 2\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[(\mathbb{1} - \mathrm{Tr}_{VU}[\Pi_{VUB}(|v(1,1)\rangle\langle v(1,1)| \otimes |u(1)\rangle\langle u(1)| \otimes \mathbb{1}_B)])\left(\mathrm{id}_{VU} \otimes \rho_B^{v(1,1),u(1)}\right)\right]\right] \\
&\overset{(b)}{=} 2\mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[(\mathbb{1} - \Pi_{VUB}(|v(1,1)\rangle\langle v(1,1)| \otimes |u(1)\rangle\langle u(1)| \otimes \mathbb{1}_B))\left(\mathrm{id}_{VU} \otimes \rho_B^{v(1,1),u(1)}\right)\right]\right] \\
&= 2\left[\mathrm{Tr}\left[(\mathbb{1} - \Pi_{VUB})\,\mathbb{E}_{\mathcal{C}}\left(|v(1,1)\rangle\langle v(1,1)| \otimes |u(1)\rangle\langle u(1)| \otimes \rho_B^{v(1,1),u(1)}\right)\right]\right] \\
&= 2\left[\mathrm{Tr}\left[(\mathbb{1} - \Pi_{VUB})\left(\sum_{v,u} p_{VU}(v,u)\,|v\rangle\langle v| \otimes |u\rangle\langle u| \otimes \rho_B^{v,u}\right)\right]\right] \\
&\overset{(c)}{=} 2\,\mathrm{Tr}[(\mathbb{1} - \Pi_{VUB})\,\rho_{VUB}] \\
&\overset{(d)}{\leq} 2 \cdot \nu_1^{\alpha} 2^{\alpha\left[R+R_S-\tilde{D}_{1-\alpha}(\rho_{VUB}||\rho_{VU}\otimes\rho_B)\right]}.
\end{aligned} \tag{37}$$

Where

- (a) is obtained by the definition of $\gamma(1,1)$ as in (17),
- (b) is obtained from the linearity of the trace,
- (c) is obtained by taking the expectation with respect to the random codebook C,
- (d) is obtained by Lemma 3.

As for the second term in (31):

$$\begin{aligned}
&4\sum_{(m',\ell)\neq(1,1)} \mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[(\gamma(m',\ell))\,\rho_B^{v(1,1),u(1)}\right]\right] \\
&\overset{(a)}{=} 4\sum_{(m',\ell)\neq(1,1)} \mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[(\mathrm{Tr}_{VU}[\Pi_{VUB}(|v(m',\ell)\rangle\langle v(m',\ell)| \otimes |u(m')\rangle\langle u(m')| \otimes \mathbb{1}_B)])\,\rho_B^{v(1,1),u(1)}\right]\right] \\
&= 4\sum_{(m',\ell)\neq(1,1)} \mathbb{E}_{\mathbf{C}}\left[\mathrm{Tr}\left[\left(\Pi_{VUB}(|v(m',\ell)\rangle\langle v(m',\ell)| \otimes |u(m')\rangle\langle u(m')| \otimes \rho_B^{v(1,1),u(1)}\right)\right]\right] \\
&\overset{(b)}{=} 4\sum_{(m',\ell)\neq(1,1)} \mathrm{Tr}\left[\mathbb{E}_{\mathbf{C}}\left[\left(\Pi_{VUB}(|v(m',\ell)\rangle\langle v(m',\ell)| \otimes |u(m')\rangle\langle u(m')| \otimes \rho_B^{v(1,1),u(1)}\right)\right]\right]
\end{aligned}$$

$$
\begin{aligned}
&= 4 \sum_{(m',\ell)\neq(1,1)} \mathrm{Tr}\ \Pi_{VUB} \left(\sum_{v,v',u,u'} \Pr\left(v(1,1)=v, v(m',\ell)=v', u(1)=u, u(m')=u'\right) |v'\rangle\langle v'| \otimes |u'\rangle\langle u'| \otimes \rho_B^{v,u} \right) \\
&= 4 \sum_{(m',\ell)\neq(1,1)} \mathrm{Tr} \left[\Pi_{VUB} \left(\sum_{v,v',u,u'} p_{VU}(v,u) p_{VU}(v',u') |v'\rangle\langle v'| \otimes |u'\rangle\langle u'| \otimes \rho_B^{v,u} \right) \right] \\
&= 4 \sum_{(m',\ell)\neq(1,1)} \mathrm{Tr} \left[\Pi_{VUB} \left(\sum_{v',u'} p_{VU}(v',u') |v'\rangle\langle v'| \otimes |u'\rangle\langle u'| \right) \otimes \left(\sum_{v,u} p_{VU}(v,u) \rho_B^{v,u} \right) \right] \\
&\overset{(c)}{=} 4 \sum_{(m',\ell)\neq(1,1)} \mathrm{Tr}\left[\Pi_{VUB}\left(\rho_{VU} \otimes \rho_B\right)\right] \\
&\overset{(d)}{\leq} 4 \cdot 2^{R+R_S}\, \mathrm{Tr}\left[\Pi_{VUB}\left(\rho_{VU} \otimes \rho_B\right)\right] \\
&\overset{(e)}{\leq} 4 \cdot \nu_1^{\alpha} 2^{\alpha\left[R+R_S-\tilde{D}_{1-\alpha}(\rho_{VUB}||\rho_{VU}\otimes\rho_B)\right]}.
\end{aligned} \tag{38}
$$

where

- (a) is obtained by the definition of $\gamma(m,\ell)$ as in as in (17),
- (b) is obtained from the linearity of the trace and $\mathbb{E}_C$,
- (c) is obtained by taking the expectation with respect to the random codebook C,
- (d) is obtained due to the fact that $(v(m,\ell), u(m))$ is independent of $(v(m',\ell'), u(m'))$, for $(m,\ell) \neq (m',\ell')$,
- (e) is obtained by Lemma 3.

By combining the two terms in (31) we obtain the following bound:

$$
\sum_{m'\neq 1,\ell} \mathbb{E}_{\mathbf{C}} \left[\mathrm{Tr}\left[\left(\beta(m',\ell)\right) \hat{\Theta}_B(1) \right] \right] \leq 6 \cdot \nu_1^{\alpha} 2^{\alpha\left[R+R_S-\tilde{D}_{1-\alpha}(\rho_{VUB}||\rho_{VU}\otimes\rho_B)\right]} \tag{39}
$$

Now we only have to deal with the second term in (30):

$$
\begin{aligned}
&\mathbb{E}_{\mathbf{C}} \left[P\left(\Theta_B(1), \hat{\Theta}_B(1)\right)^2 \right] \\
&\overset{(a)}{=} \mathbb{E}_{\mathbf{C}} \left[P\left(\mathrm{Tr}_{TK_1K_0L}\left[\mathcal{N}_{SA\to B}\left(\tilde{W}^{(1)} (\psi^{u(1)}_{SS_0K_1K_0}) \tilde{W}^{\dagger(1)} \right) \right], \frac{1}{2^{R_S}} \sum_{\ell\in\mathsf{L}} \rho_B^{v(1,\ell),u(1)} \right)^2 \right] \\
&= \mathbb{E}_{\mathbf{C}} \left[P\left(\mathrm{Tr}_{TK_1K_0L}\left[\mathcal{N}_{SA\to B}\left(\tilde{W}^{(1)} (\psi^{u(1)}_{SS_0K_1K_0}) \tilde{W}^{\dagger(1)} \right) \right], \frac{1}{2^{R_S}} \sum_{\ell\in\mathsf{L}} \mathrm{Tr}_{TK_1K_0}\left[\mathcal{N}_{SA\to B}\left(\rho^{v(1,\ell),u(1)}_{SATK_1K_0} \right) \right] \right)^2 \right] \\
&\overset{(b)}{\leq} \mathbb{E}_{\mathbf{C}} \left[P\left(\phi^{(1)}_{SATK_1K_0L}, \tilde{W}^{(1)} (\psi^{u(1)}_{SS_0K_1K_0}) \tilde{W}^{\dagger(1)} \right)^2 \right] \\
&\overset{(c)}{=} \mathbb{E}_{\mathbf{C}} \left[P\left(\frac{1}{2^{R_S}} \sum_{\ell\in\mathsf{L}} \rho_S^{v(1,\ell),u(1)}, \sigma_S^{u(1)} \right)^2 \right] \\
&\overset{(d)}{=} \mathbb{E}_{\mathbf{C}} \left[P\left(\tau_S^{\mathcal{C}_1}, \rho_S^{u(1)} \right)^2 \right] \\
&\overset{(e)}{\leq} \mathbb{E}_{\mathbf{C}} \left[1 - 2^{-\tilde{D}_{1+\alpha}\left(\tau_S^{\mathcal{C}_1}, \rho_S^{u(1)}\right)} \right] \\
&\overset{(f)}{\leq} \ln 2\, \mathbb{E}_{\mathbf{C}} \left[\tilde{D}_{1+\alpha}\left(\tau_S^{\mathcal{C}_1}, \rho_S^{u(1)} \right) \right] \\
&\overset{(g)}{\leq} \frac{1}{\alpha \ln 2} \frac{\nu_2^{\alpha}}{2^{\alpha R_S}} 2^{\alpha \tilde{D}_{1+\alpha}(\rho_{VUS}\|\rho_{V-U-S})},
\end{aligned} \tag{40}
$$

where

- (a) is obtained by substituting the definition of $\Theta_B(m)$ and $\hat{\Theta}_B(m)$ on the right-hand side of the expression.
- (b) is obtained by the fact that monotonicity of the purified distance does not increase under quantum channel $\mathrm{Tr}_{TK_1K_0}\mathcal{N}_{SA\to B}(\cdot)$.
- (c) is obtained by (14)
- (d) is obtained by using the notation $\tau_S^{\mathcal{C}_1}$ to represent the average state $\frac{1}{2^{R_S}}\sum_{\ell\in\mathcal{L}} \rho_S^{v(1,\ell),u(1)}$, and $\sum_v p_{V|U}(v|u)\left[\mathrm{Tr}_A\, \rho_{SA}^{v,u}\right] = \mathrm{Tr}_{S_0}\, \sigma^u_{SS_0}$.

- (e) is obtained due to the fact that for quantum states $\rho_A, \sigma_A \in \mathscr{D}(A)$, $F^2(\rho,\sigma) = 2^{-D_{1/2}(\rho\|\sigma)} \geq 2^{-D_{1+\alpha}(\rho\|\sigma)}$ [23, Fact 5].
- (f) is obtained using the mathematical inequality $1 - 2^{-x} \leq x \ln 2$.
- (g) is obtained by applying Lemma 4.

The proposition 2 then follows from (39), and (40).

Appendix B
Proof of Lemma 3

We start by achieving an upper bound for (33):

$$
\begin{aligned}
\operatorname{Tr}[(\mathbb{I} - \Pi_{VUB})\,\rho_{VUB}] &\overset{(a)}{=} \operatorname{Tr}[\mathcal{E}_1\left((\mathbb{1} - \Pi_{VUB})\,\rho_{VUB}\right)] \\
&\overset{(b)}{=} \operatorname{Tr}[(\mathbb{1} - \Pi_{VUB})\,\mathcal{E}_1(\rho_{VUB})] \\
&= \operatorname{Tr}\big[(\mathbb{1} - \Pi_{VUB})\,\mathcal{E}_1(\rho_{VUB})^{1-\alpha}\mathcal{E}_1(\rho_{VUB})^{\alpha}\big], \quad \forall \alpha \in \left(0, \frac{1}{2}\right) \\
&\overset{(c)}{\leq} 2^{\alpha(R+R_S)} \operatorname{Tr}\big[(\mathbb{1} - \Pi_{VUB})\,\mathcal{E}_1(\rho_{VUB})^{1-\alpha}(\rho_{VU} \otimes \rho_B)^{\alpha}\big] \\
&\overset{(d)}{\leq} 2^{\alpha(R+R_S)} \operatorname{Tr}\big[\mathcal{E}_1(\rho_{VUB})^{1-\alpha}(\rho_{VU} \otimes \rho_B)^{\alpha}\big] \\
&= 2^{\alpha(R+R_S)} \operatorname{Tr}\big[(\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2}}\mathcal{E}_1(\rho_{VUB})^{1-\alpha}(\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2}}\big] \\
&= 2^{\alpha(R+R_S)} \operatorname{Tr}\left[\left((\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\mathcal{E}_1(\rho_{VUB})(\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\right)^{1-\alpha}\right] \\
&= 2^{\alpha(R+R_S)} \operatorname{Tr}\left[\left((\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\,\mathcal{E}_1\left(\rho_{VUB}\right)\left(\rho_{VU} \otimes \rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\right)\right. \\
&\quad \left. \times \left((\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\,\mathcal{E}_1\left(\rho_{VUB}\right)\left(\rho_{VU} \otimes \rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\right)^{-\alpha}\right] \\
&\overset{(e)}{=} 2^{\alpha(R+R_S)} \operatorname{Tr}\left[\left((\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\,\rho_{VUB}\left(\rho_{VU} \otimes \rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\right)\right. \\
&\quad \left. \times \left((\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\,\mathcal{E}_1\left(\rho_{VUB}\right)\left(\rho_{VU} \otimes \rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\right)^{-\alpha}\right] \\
&\overset{(f)}{\leq} 2^{\alpha(R+R_S)}\nu_1^{\alpha} \operatorname{Tr}\left[\left((\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\,\rho_{VUB}\left(\rho_{VU} \otimes \rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\right)\right. \\
&\quad \left. \times \left((\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\,\rho_{VUB}\left(\rho_{VU} \otimes \rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\right)^{-\alpha}\right] \\
&= 2^{\alpha(R+R_S)}\nu_1^{\alpha} \operatorname{Tr}\left[\left((\rho_{VU} \otimes \rho_B)^{\frac{\alpha}{2(1-\alpha)}}\,\rho_{VUB}\left(\rho_{VU} \otimes \rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\right)^{1-\alpha}\right] \\
&= \nu_1^{\alpha} 2^{\alpha\left[R+R_S-\tilde{D}_{1-\alpha}(\rho_{VUB}||\rho_{VU}\otimes\rho_B)\right]}.
\end{aligned} \tag{41}
$$

where

- (a) is obtained due to the trace-preserving property of pinching.
- (b) is obtained from the definition of Π_{VUB} in (16). The projector $\mathbb{1} - \Pi_{VUB}$ can be defined as:

$$
\mathbb{1} - \Pi_{VUB} = \sum_{v\in\mathcal{T}_V}\sum_{u\in\mathcal{T}_U}\sum_{b\in\mathcal{T}_B} |v\rangle\langle v|_V \otimes |u\rangle\langle u|_U \otimes |b\rangle\langle b|_B \,. \tag{42}
$$

Then, by applying the pinching map $\mathcal{E}_1(\rho_{VUB})$, it follows:

$$
\begin{aligned}
\mathcal{E}_1(\rho_{VUB}) &= \sum_{\lambda=1}^{\nu_1} \Pi_\lambda \left(\sum_{v,u} p_{VU}(v,u)\,|v\rangle\langle v|_V \otimes |u\rangle\langle u|_U \otimes \rho_B^{v,u}\right)\Pi_\lambda \\
&= \sum_{\lambda=1}^{\nu_1} |v_\lambda\rangle\langle v_\lambda|_V \otimes |u_\lambda\rangle\langle u_\lambda|_U \otimes |b_\lambda\rangle\langle b_\lambda|_B \left(\sum_{v,u} p_{VU}(v,u)\,|v\rangle\langle v|_V \otimes |u\rangle\langle u|_U \otimes \rho_B^{v,u}\right) |v_\lambda\rangle\langle v_\lambda|_V \otimes |u_\lambda\rangle\langle u_\lambda|_U \otimes |b_\lambda\rangle\langle b_\lambda|_B \\
&= \sum_{\lambda=1}^{\nu_1} p_{VU}(v,u)\,|v_\lambda\rangle\langle v_\lambda|_V \otimes |u_\lambda\rangle\langle u_\lambda|_U \otimes |b_\lambda\rangle\langle b_\lambda|\,\rho_B^{v,u}\,|b_\lambda\rangle\langle b_\lambda|_B \\
&= \sum_{\lambda=1}^{\nu_1} p_{VU}(v,u)\,\langle b_\lambda|\,\rho_B^{v,u}\,|b_\lambda\rangle\,|v_\lambda\rangle\langle v_\lambda|_V \otimes |u_\lambda\rangle\langle u_\lambda|_U \otimes |b_\lambda\rangle\langle b_\lambda|_B
\end{aligned} \tag{43}
$$

Thus:

$$
\begin{aligned}
&\mathcal{E}_1\left((\mathbb{1}-\Pi_{VUB})\,\rho_{VUB}\right)\\
&=\sum_{v,u,b}|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\otimes|b\rangle\langle b|_B\,(\mathbb{1}-\Pi_{VUB})\,\rho_{VUB}\,|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\otimes|b\rangle\langle b|_B\\
&=\sum_{v,u,b}|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\,|b\rangle\langle b|_B\left(\sum_{v'\in\mathcal{T}_V}\sum_{u'\in\mathcal{T}_U}\sum_{b'\in\mathcal{T}_B}|v'\rangle\langle v'|\otimes|u'\rangle\langle u'|\otimes|b'\rangle\langle b'|\right)\rho_{VUB}\,|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\,|b\rangle\langle b|_B\\
&=\sum_{v,u,b}|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\,|b\rangle\langle b|_B\left(\sum_{v'\in\mathcal{T}_V}\sum_{u'\in\mathcal{T}_U}\sum_{b'\in\mathcal{T}_B}p_{VU}(v,u)\,|v'\rangle\langle v'|\otimes|u'\rangle\langle u'|\otimes|b'\rangle\langle b'|\,\rho_B^{v',u'}\right)|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\,|b\rangle\langle b|_B\\
&=\sum_{v\in\mathcal{T}_V}\sum_{u\in\mathcal{T}_U}\sum_{b\in\mathcal{T}_B}p_{VU}(v,u)\,|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\otimes|b\rangle\langle b|\,\rho_B^{v,u}\,|b\rangle\langle b|_B\\
&=\sum_{v\in\mathcal{T}_V}\sum_{u\in\mathcal{T}_U}\sum_{b\in\mathcal{T}_B}p_{VU}(v,u)\,\langle b|\,\rho_B^{v,u}\,|b\rangle\,|v\rangle\langle v|_V\otimes|u\rangle\langle u|_U\otimes|b\rangle\langle b|_B\\
&=(\mathbb{1}-\Pi_{VUB})\,\mathcal{E}_1(\rho_{VUB})
\end{aligned}
\tag{44}
$$

- (c) is obtained due to the definition of Π_{VUB} in (16), and since $f(x)=x^\alpha$ is a matrix monotone function $\forall\alpha\in(0,1]$
- (d) is obtained because $\mathbb{1}-\Pi_{VUB}\le\mathbb{1}$
- (e) is obtained by by the fact that for two states $\rho,\sigma\in\mathscr{D}(\mathcal{H})$, and $\mathcal{E}_\sigma$ is the pinching map with respect to σ: $\mathrm{Tr}\left[\rho\sigma\right]=\mathrm{Tr}\left[\mathcal{E}_\sigma(\rho)\sigma\right]$
- (f) is obtained by the pinching inequality. For two states $\rho,\sigma\in\mathscr{D}(\mathcal{H})$, and $\mathcal{E}_\sigma$ is the pinching map with respect to σ, then $\rho\le\nu\mathcal{E}_\sigma(\rho)$ [23, Fact 9].

Using similar steps (34), is proven:

$$
\begin{aligned}
2^{R+R_S}\,\mathrm{Tr}\left[\Pi_{VUB}\left(\rho_{VU}\otimes\rho_B\right)\right]&=2^{R+R_S}\,\mathrm{Tr}\left[\Pi_{VUB}\left(\rho_{VU}\otimes\rho_B\right)^{1-\alpha}\left(\rho_{VU}\otimes\rho_B\right)^{\alpha}\right]\quad\forall\alpha\in\left(0,\frac{1}{2}\right)\\
&\overset{(a)}{\le}2^{R+R_S}2^{-(R+R_S)(1-\alpha)}\,\mathrm{Tr}\left[\Pi_{VUB}\mathcal{E}_1\left(\rho_{VUB}\right)^{1-\alpha}\left(\rho_{VU}\otimes\rho_B\right)^{\alpha}\right]\\
&\overset{(b)}{\le}2^{\alpha(R+R_S)}\,\mathrm{Tr}\left[\mathcal{E}_1\left(\rho_{VUB}\right)^{1-\alpha}\left(\rho_{VU}\otimes\rho_B\right)^{\alpha}\right]\\
&=2^{\alpha(R+R_S)}\,\mathrm{Tr}\left[\left(\left(\rho_{VU}\otimes\rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\mathcal{E}_1\left(\rho_{VUB}\right)\left(\rho_{VU}\otimes\rho_B\right)^{\frac{\alpha}{2(1-\alpha)}}\right)^{1-\alpha}\right]\\
&\overset{(c)}{\le}\nu_1^{\alpha}2^{\alpha\left[R+R_S-\tilde{D}_{1-\alpha}(\rho_{VUB}||\rho_{VU}\otimes\rho_B)\right]}.
\end{aligned}
\tag{45}
$$

where

- (a) is obtained due to the definition of Π_{VUB} in (16), and since $f(x)=x^\alpha$ is a matrix monotone function $\forall\alpha\in(0,1]$
- (b) is obtained because $\Pi_{VUB}\le\mathbb{1}$
- (c) is obtained from the first part of the proof.

Acknowledgments

The authors thank Gerhard Kramer (TUM) for useful discussions. MK and UP were supported by ISF, Grants n. 939/23 and 2691/23, DIP n. 2032991, Ollendorff-Minerva Center n. 86160946, and HD Quantum Center n. 2033613. UP was also supported by Chaya Chair n. 8776026, and VATAT Program for Quantum Science and Technology n. 86636903.

References

[1] C. E. Shannon, "Channels with side information at the transmitter," *IBM J. Res. Develop.*, vol. 2, no. 4, Oct. 1958.

[2] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Probl. Control Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[3] M. H. M. Costa, "Writing on dirty paper (corresp.)," *IEEE Trans. Inf. Theory*, vol. 29, pp. 439–441, Jun. 1983.

[4] C. Heegard and A. A. E. Gamal, "On the capacity of computer memory with defects," *IEEE Trans. Inf. Theory*, vol. 29, pp. 731–739, Jul. 1983.

[5] A. Bennatan, D. Burshtein, G. Caire, and S. Shamai, "Superposition coding for side-information channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 1872–1889, May 2006.

[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.

[7] V. Ramachandran, S. R. B. Pillai, and V. M. Prabhakaran, "Joint state estimation and communication over a state-dependent Gaussian multiple access channel," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 6743–6752, Oct. 2019.

[8] T. Weissman, "Capacity of channels with action-dependent states," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5396–5411, Nov. 2010.

[9] K. Kittichokechai, T. J. Oechtering, and M. Skoglund, "Multi-stage coding for channels with a rewrite option and reversible input," in *Proc. IEEE Int. Symp. Inf. Theory*, 2012, pp. 3063–3067.

[10] H. Asnani, H. Permuter, and T. Weissman, "Probing capacity," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7317–7332, Nov. 2011.

[11] K. Kittichokechai, T. J. Oechtering, and M. Skoglund, "Coding with action-dependent side information and additional reconstruction requirements," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6355–6367, Nov. 2015.

[12] Y. Steinberg and T. Weissman, "The degraded broadcast channel with action-dependent states," in *Proc. IEEE Int. Symp. Inf. Theory*, 2012, pp. 596–600.

[13] B. Ahmadi and O. Simeone, "On channels with action-dependent states," in *Proc. IEEE Inf. Theory Workshop*, 2012, pp. 167–171.

[14] L. Dikstein, H. H. Permuter, and S. S. Shamai, "MAC with action-dependent state information at one encoder," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 173–188, Jan. 2015.

[15] B. Dai, A. J. H. Vinck, Y. Luo, and X. Tang, "Wiretap channel with action-dependent channel state information," *Entropy*, vol. 15, no. 2, pp. 445–473, 2013.

[16] B. Dai, C. Li, Y. Liang, Z. Ma, and S. S. Shamai, "Impact of action-dependent state and channel feedback on Gaussian wiretap channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3435–3455, Jun. 2020.

[17] T. Welling, O. Günlü, and A. Yener, "Transmitter actions for secure integrated sensing and communication," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2024, pp. 2580–2585.

[18] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photonics*, vol. 7, no. 5, p. 378, 2013.

[19] A. Orieux and E. Diamanti, "Recent advances on integrated quantum communications," *Journal of Optics*, vol. 18, no. 8, p. 083002, Aug 2016.

[20] L. Petit *et al.*, "Universal quantum logic in hot silicon qubits," *Nature*, vol. 580, no. 7803, pp. 355–359, Apr 2020.

[21] F. Dupuis, "The capacity of quantum channels with side information at the transmitter," in *Proc. IEEE Int. Symp. Inf. Theory*, 2009, pp. 948–952.

[22] U. Pereg, "Entanglement-assisted capacity of quantum channels with side information," 2019, arXiv:1909.09992.

[23] A. Anshu, M. Hayashi, and N. A. Warsi, "Secure communication over fully quantum Gel'fand-Pinsker wiretap channel," *IEEE Trans. Inf. Theory*, vol. 66, no. 9, pp. 5548–5566, Sep. 2020.

[24] H. ZivariFard, R. A. Chou, and X. Wang, "Covert communication with positive rate over state-dependent quantum channels," in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2024, pp. 711–716.

[25] U. Pereg, "Communication over quantum channels with parameter estimation," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 359–383, Jan. 2022.

[26] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," *J. Math. Phys.*, vol. 54, no. 12, p. 122203, Dec. 2013.

[27] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Springer-Verlag, 2015.

[28] M. Hayashi, *Quantum Information Theory: Mathematical Foundation*, 2nd ed. Springer, 2017.

[29] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1753–1768, Jul. 2003.