Usefulness of adaptive strategies in asymptotic quantum channel discrimination

Farzin Salek,[1,*] Masahito Hayashi,[2,3,4,†] and Andreas Winter[5,6,‡]

[1]*Zentrum Mathematik, Technische Universität München, 85748 München, Germany*
[2]*Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Nanshan District, Shenzhen, 518055, China*
[3]*International Quantum Academy (SIQA), Futian District, Shenzhen 518048, China*
[4]*Graduate School of Mathematics, Nagoya University, Nagoya, 464-8602, Japan*
[5]*Institució Catalana de Recerca i Estudis Avançats (ICREA), Pg. Lluis Companys, 23, 08010 Barcelona, Spain*
[6]*Grup d'Informació Quàntica, Departament de Física, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain*

(Received 10 June 2021; revised 30 November 2021; accepted 25 January 2022; published 14 February 2022)

Adaptiveness is a key principle in information processing including statistics and machine learning. We investigate the usefulness adaptive methods in the framework of asymptotic binary hypothesis testing, when each hypothesis represents asymptotically many independent instances of a quantum channel, and the tests are based on using the unknown channel and observing outputs. Unlike the familiar setting of quantum states as hypotheses, there is a fundamental distinction between adaptive and nonadaptive strategies with respect to the channel uses, and we introduce a number of further variants of the discrimination tasks by imposing different restrictions on the test strategies. The following results are obtained: (1) We prove that for classical-quantum channels, adaptive and nonadaptive strategies lead to the same error exponents both in the symmetric (Chernoff) and asymmetric (Hoeffding, Stein) settings. (2) The first separation between adaptive and nonadaptive symmetric hypothesis testing exponents for quantum channels, which we derive from a general lower bound on the error probability for nonadaptive strategies; the concrete example we analyze is a pair of entanglement-breaking channels. (3) We prove, in some sense generalizing the previous statement, that for general channels adaptive strategies restricted to classical feed-forward and product state channel inputs are not superior in the asymptotic limit to nonadaptive product state strategies. (4) As an application of our findings, we address the discrimination power of an arbitrary quantum channel and show that adaptive strategies with classical feedback and no quantum memory at the input do not increase the discrimination power of the channel beyond nonadaptive tensor product input strategies.

DOI: 10.1103/PhysRevA.105.022419

I. INTRODUCTION

Adaptiveness is a key principle in information processing including statistics and machine learning [1], which can entail great advantage over nonadaptive methods. Because of the higher complexity of adaptive methods, we thus are motivated to clarify in which situations they offer a significant improvement. Here, we address this question in the setting of binary hypothesis testing for quantum channels. Hypothesis testing is one of the most fundamental primitives both in classical and quantum information processing because a variety of other information processing problems can be cast in the framework of hypothesis testing; both direct coding theorems and converses can be reduced to it. It is expected that this analysis for adaptiveness reveals the role of adaptive methods in various types of quantum information processing. In binary hypothesis testing, the two hypotheses are usually referred to as null and alternative hypotheses and, accordingly, two error probabilities are defined: type-I error due to a wrong decision in favor of the alternative hypothesis (while the truth corresponds to the null hypothesis) and type-II error due to the alternative hypothesis being rejected despite being correct. The overall objective of the hypothesis testing is to minimize the error probability in identifying the hypotheses. Depending on the significance attributed to the two types of errors, several settings can be distinguished. A historical distinction is between the *symmetric* and the *asymmetric* hypothesis testing: in symmetric hypothesis testing, the goal is to minimize both error probabilities simultaneously, while in asymmetric hypothesis testing, the goal is to minimize one type of error probability subject to a constraint on the other type of error probability.

In classical information theory, discriminating two distributions has been studied by many researchers; Stein, Chernoff [2], Hoeffding [3], and Han-Kobayashi [4] formulated asymptotic hypothesis testing of two distributions as optimization problems and subsequently found optimum error exponents. As generalizations of these settings to quantum realm, discrimination of two quantum states has been studied extensively in quantum information theory, albeit the complications stemming from the noncommutativity of quantum mechanics appear in the most visible way among these problems. The

*farzin.salek@gmail.com
†hayashi@sustech.edu.cn
‡andreas.winter@uab.cat

first study in this direction was done by Hiai and Petz [5], which showed the possibility part of the quantum extension of Stein's lemma. That is, it showed that the error exponent of type-II error probability attains the relative entropy registered between the states under the constant constraint for type-I error probability. Also, it shows the impossibility to exceed the above error exponent when type-I error probability goes to zero. Subsequently, Ogawa and Nagaoka [6] strengthened the above impossibility, i.e., it showed the same fact under the constant constraint for type-I error probability. As the quantum extension of the Chernoff bound, Audenaert *et al.* [7] derived a lower bound for the exponent of the sum of type-I and type-II error probabilities, and Nussbaum and Szkoła [8] showed its tightness. (See [9] for earlier significant progress.) Concerning the quantum extension of the Hoeffding bound, the paper [10] derived a lower bound of the exponent of the type-II error probability under the exponential constraint for type-I error probability, but it suggested the existence of a tighter lower bound. Later, Ref. [11] proved the suggested tighter lower bound and, subsequently, Nagaoka [12] showed its optimality.

To study the effect of adaptiveness in the viewpoint of the binary hypothesis testing, we focus on the discrimination of (quantum) channels, which is a natural extension of the state discrimination problem. Channel discrimination is a fundamental question not only in quantum information, but also in other disciplines including theoretical computer science where, under the name of oracle identification, discrimination of unitary operations as oracles in quantum algorithms becomes relevant [13]. Despite inherent mathematical links between the channel and state discrimination problems, due to the additional degrees of freedom introduced by the adaptive strategies, discrimination of channels is more complicated. Many papers have been dedicated to study the potential advantages of adaptive strategies over nonadaptive strategies in channel discrimination, such as [14,15].

The seminal classical work [16] showed that in the asymptotic regime, the exponential error rate for classical channel discrimination cannot be improved by adaptive strategies for any of the symmetric or asymmetric settings, i.e., the channel versions of Stein's lemma, Chernoff bound, and Hoeffing bound. Since the publication of [16], significant amount of research has focused on showing the potential advantages of adaptive strategies in discrimination of quantum channels. Significant progress was reported in [17] concerning classical quantum channels, i.e., the case when the channel has a classical input and a quantum output. There are other pairs of channels, for which it could be shown that adaptive strategies do not outperform nonadaptive ones for any finite number of copies, such as pairs of von Neumann measurements [18,19] and teleportation-covariant channels (which are programmed by their Choi states) [20]. Wilde *et al.* [17] showed that the classical-quantum (cq) channel extension of Stein's lemma has no improvement by use of adaptive strategy. However, for Chernoff and Hoeffding bounds, they derived upper and lower bounds. These bounds do not coincide when the cq channel has a certain noncommutativity. Therefore, it remained an open problem whether an adaptive method improves Chernoff and Hoeffding bounds in the classical-quantum channel discrimination.

Concerning quantum-quantum (qq) channels, i.e., channels having quantum input and quantum outputs, it is known that adaptive strategies offer an advantage in the nonasymptotic regime for discrimination in the symmetric Chernoff setting [14,21–23]. In particular, Harrow *et al.* [14] demonstrated the advantage of adaptive strategies in discriminating a pair of entanglement-breaking channels that requires just two channel evaluations to distinguish them perfectly, but such that no nonadaptive strategy can give perfect distinguishability using any finite number of channel evaluations. However, it was open whether the same holds in the asymptotic setting.

This question in the asymmetric regime was recently settled by Wang and Wilde: In [24, Theorem 3], they found an exponent in Stein's setting for nonadaptive strategies in terms of channel max-relative entropy, also in the same paper [24, Theorem 6], they found an exponent in Stein's setting for the adaptive strategies in terms of amortized channel divergence, a quantity introduced in [17] to quantify the largest distinguishability between two channels. However, the fact that adaptive strategies do not offer an advantage in the setting of Stein's lemma for quantum channels, i.e., the equality of the aforementioned exponents of Wang and Wilde, was later shown in [25] via a chain rule for the quantum relative entropy proven therein. Cooney *et al.* [26] proved the quantum Stein's lemma for discriminating between an arbitrary quantum channel and a "replacer channel" that discards its input and replaces it with a fixed state. This work led to the conclusion that at least in the asymptotic regime, a nonadaptive strategy is optimal in the setting of Stein's lemma. However, in the Hoeffding and Chernoff settings, the question of potential advantages of adaptive strategies involving replacer channels remains open.

Hirche *et al.* [27] studied the maximum power of a fixed quantum detector, i.e., a positive-operator-valued measurement (POVM), in discriminating two possible states. This problem is dual to the state discrimination scenario considered so far in that, while in the state discrimination problem the state pair is fixed and optimization is over all measurements, in this problem a measurement POVM is fixed and the question is how powerful this discriminator is, and then whatever criterion considered for quantifying the power of the given detector, it should be optimized over all input states. In particular, if $n \geqslant 2$ uses of the detector are available, the optimization takes place over all n-partite entangled states and also all adaptive strategies that may help improve the performance of the measurement. The main result of [27] states that when asymptotically many uses (i.e., $n \to \infty$) of a given detector are available, its performance does not improve by considering general input states or using an adaptive strategy in any of the symmetric or asymmetric settings described before.

In this paper, we tackle and solve all the aforementioned open problems as we explain next: (i) We prove that for cq channels, adaptive and nonadaptive strategies lead to the same error exponents both in the symmetric (Chernoff) and asymmetric (Hoeffding, Stein) settings. (ii) We derive the first separation between adaptive and nonadaptive symmetric hypothesis testing exponents for qq channels, which we derive from a general lower bound on the error probability for nonadaptive strategies. The two concrete examples we analyze are pairs of entanglement-breaking channels. (iii) When two qq channels are given as entanglement-breaking channel with the same measurement, we prove that adaptive and nonadaptive strategies lead to the same error exponents both in the symmetric (Chernoff) and asymmetric (Hoeffding, Stein) settings. (iv) As an application of our findings, we address the discrimination power of an arbitrary quantum channel and show that adaptive strategies with classical feedback and no quantum memory at the input do not increase the discrimination power of the channel beyond nonadaptive tensor product input strategies.

The rest of the paper is organized as follows. Section II presents our results of cq-channel discrimination with discrete feedback variables. Section III gives a general formulation for adaptive discrimination for qq channels. In Sec. IV we show two examples of qq channels, of the entanglement breaking form, that have the first asymptotic separation between adaptive and nonadaptive strategies via proving a lower bound on the Chernoff error for nonadaptive strategies and analyzing an example where adaptive strategies achieve error zero even with two copies of the channels. In Sec. V, we study the discrimination of quantum channels when restricting to a subclass of $\mathbb{A}_n$ allowing only strategies with classical feed forward and without quantum memory at the input. Also, Sec. V addresses the discrimination of two qq channels under a special class of pairs of two qq channels. In Sec. VI we apply our results to the discrimination power of an arbitrary quantum channel. We conclude in Sec. VII. Appendixes are denoted to prove the results for cq-channel discrimination, which are stated in Sec. II.

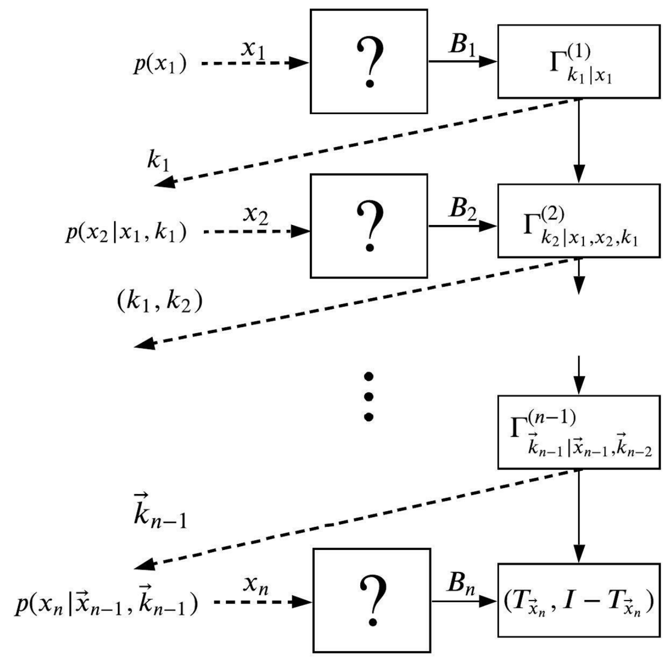

FIG. 1. Adaptive strategy for cq-channel discrimination. Solid and dashed lines denote flow of classical and quantum information, respectively. The classical outputs of instruments $\{\Gamma^{(m)}_{k_m|\vec{x}_m,\vec{k}_{m-1}}\}_{k_m\in\mathcal{K}_m}$ are employed to decide the inputs adaptively, and leave a post-measurement state that can be accessed together with the next channel output.

II. DISCRIMINATION OF CLASSICAL-QUANTUM CHANNELS

In this section, the hypotheses are described by two cq channels. To spell out the precise questions, let us introduce a bit of notation. Throughout the paper, A, B, C, etc., denote quantum systems, but also their corresponding Hilbert space. A cq channel is defined with respect to a set $\mathcal{X}$ of input signals and the Hilbert space B of the output states. In this case, the channel from $\mathcal{X}$ to B is described by the map from the set $\mathcal{X}$ to the set of density operators in B; as such, a cq channel is given as $\mathcal{N}: x \to \rho_x$, where ρ_x denotes the output state when the input is $x \in \mathcal{X}$. Our goal is to distinguish between two cq channels, $\mathcal{N}: x \to \rho_x$ and $\overline{\mathcal{N}}: x \to \sigma_x$. Here, we do not assume any condition for the set $\mathcal{X}$, except that it is a measurable space and that the channels are measurable maps (with the usual Borel sets on the state space $\mathcal{S}^B$). In particular, it might be an uncountably infinite set.

The task is to discriminate two hypotheses, the null hypothesis $H_0 : \mathcal{N}$ versus the alternative hypothesis $H_1 : \overline{\mathcal{N}}$ where $n \to \infty$ (independent) uses of the unknown channel are provided. Then, the challenge we face is to make a decision in favor of the true channel based on n inputs $\vec{x}_n = (x_1, \dots, x_n)$ and corresponding output states on $B^n = B_1 \dots B_n$; note that the input $\vec{x}_n = (x_1, \dots, x_n)$ is generated by a very complicated joint distribution of n random variables, which, except for x_1, depend on the actual channel. Hence, they are written with the capitals as $X^n = X_1, \dots, X_n$ when they are treated as random variables.

A. Quantum measurements

To formulate our general adaptive method for the discrimination of cq channels, we prepare a general notation for quantum measurements with state changes. A general quantum state evolution from A to B is written as a completely positive trace-preserving (CPTP) map $\mathcal{M}$ from the space $\mathcal{T}^A$ to the space $\mathcal{T}^B$ of trace class operators on A and B, respectively. When we make a measurement on the initial system A, we obtain the measurement outcome K and the resultant state on the output system B. To describe this situation, we use a set $\{\kappa_k\}_{k\in\mathcal{K}}$ of completely positive (CP) maps from the space $\mathcal{T}^A$ to the space $\mathcal{T}^B$ such that $\sum_{k\in\mathcal{K}} \kappa_k$ is trace preserving. In this paper, since the classical feed-forward information is assumed to be a discrete variable, $\mathcal{K}$ is a discrete (finite or countably infinite) set. Since it is a decomposition of a CPTP map, it is often called a *CP-map valued measure*, and an *instrument* if their sum is CPTP [28]. In this case, when the initial state on A is ρ and the outcome k is observed with probability $\mathrm{Tr}\kappa_k(\rho)$, where the resultant state on B is $\kappa_k(\rho)/\mathrm{Tr}\kappa_k(\rho)$. A state on the composite system of the classical system K and the quantum B is written as $\sum_{k\in\mathcal{K}} |k\rangle\langle k| \otimes \rho_{B|k}$, which belongs to the vector space $\mathcal{T}^{KB} := \sum_{k\in\mathcal{K}} |k\rangle\langle k| \otimes \mathcal{T}^B$. The above measurement process can be written as the following CPTP $\mathcal{E}$ map from $\mathcal{T}^A$ to $\mathcal{T}^{KB}$:

$$\mathcal{E}(\rho) := \sum_{k\in\mathcal{K}} |k\rangle\langle k| \otimes \kappa_k(\rho). \tag{1}$$

In the following, both of the above CPTP map $\mathcal{E}$ and a CP-map valued measure are called a quantum instrument.

B. Formulation of adaptive method

To study the adaptive discrimination of cq channels, the general strategy for discrimination of qq channels in Sec. I should be tailored to the cq channels. We argue that the most general strategy in Sec. I can without loss of generality be replaced by the kind of strategy with the instrument and only classical feed forward when the hypotheses are a pair of cq channels, as Fig. 1. This in particular will turn out to be crucial since we consider general cq channels with arbitrary (continuous) input alphabet.

The first input is chosen subject to the distribution $p_{X_1}(x_1)$. The receiver receives the output ρ_{x_1} or σ_{x_1} on B_1. Dependent on the input x_1, the receiver applies the first quantum instrument $\{\Gamma^{(1)}_{k_1|x_1}\}_{k_1\in\mathcal{K}_1} : B_1 \to K_1R_2$, where R_2 is the quantum memory system and K_1 is the classical outcome. The receiver sends the outcome K_1 to the sender. Then, the sender chooses the second input x_2 according to the conditional distribution $p_{X_2|X_1,K_1}(x_2|x_1, k_1)$. The receiver receives the second output ρ_{x_2} or σ_{x_2} on B_2. Dependent on the previous outcome k_1 and the previous inputs x_1, x_2, the receiver applies the second quantum instrument $\{\Gamma^{(2)}_{k_2|x_1,x_2,k_1}\}_{k_2\in\mathcal{K}_2} : B_2R_2 \to K_2R_3$, and sends the outcome K_2 to the sender. The third input is chosen as the distribution $p_{X_3|X_1,X_2,K_1,K_2}(x_2|x_1, x_2, k_1, k_2)$.

In the same way as the above, the mth step is given as follows. The sender chooses the mth input x_m according to the conditional distribution $p_{X_m|\vec{X}_{m-1},\vec{K}_{m-1}}(x_m|\vec{x}_{m-1}, \vec{k}_{m-1})$. The receiver receives the second output ρ_{x_m} or σ_{x_m} on B_m. The remaining processes need the following divided cases. For $m < n$, dependent on the previous outcomes $\vec{k}_{m-1} := (k_1, \dots, k_{m-1})$ and the previous inputs $\vec{x}_m := (x_1, \dots, x_m)$, the receiver applies the mth quantum instrument $\{\Gamma^{(m)}_{k_m|\vec{x}_m,\vec{k}_{m-1}}\}_{k_m\in\mathcal{K}_m} : R_mB_m \to K_mR_{m+1}$, and sends the outcome k_m to the sender. For $m = n$, dependent on the previous outcomes $\vec{K}_{n-1}$ and the previous inputs $\vec{X}_n$, the receiver measures the final state on R_nB_n with the binary POVM $(T_{n|\vec{k}_{n-1},\vec{x}_n}, I - T_{n|\vec{k}_{n-1},\vec{x}_n})$, where hypothesis $\mathcal{N}$ (respectively $\overline{\mathcal{N}}$) is accepted if and only if the first (respectively second) outcome clicks.

In the following, we denote the class of the above general strategies by $\underline{\mathbb{A}}^{c,0}$ because it can be considered that this strategy has no quantum memory in the input side and no quantum feedback. As a subclass, we focus on the class when no feedback is allowed and the input state deterministically is fixed to a single input x, which is denoted $\underline{\mathbb{P}}^0$. When the true channel is $\mathcal{N} : x \to \rho_x$, the state before the final measurement is

$$\rho^{(n)} := \sum_{\vec{x}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1}) \times \left[\Gamma_{k_{n-1}|\vec{x}_{n-1},k_{n-2}}(\dots\Gamma_{k_2|x_1,x_2,k_1}(\Gamma_{k_1|x_1}(\rho_{x_1})\otimes\rho_{x_2})\otimes\dots\otimes\rho_{x_{n-1}})\otimes\rho_{x_n}\otimes|\vec{x}_n,\vec{k}_{n-1}\rangle\langle\vec{x}_n,\vec{k}_{n-1}|\right], \tag{2}$$

where here we need to store the information for inputs $\vec{x}_n$. Similarly, when the true channel is $\overline{\mathcal{N}} : x \to \sigma_x$,

$$\sigma^{(n)} := \sum_{\vec{x}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1}) \times \left[\Gamma_{k_{n-1}|\vec{x}_{n-1},k_{n-2}}(\dots\Gamma_{k_2|x_1,x_2,k_1}(\Gamma_{k_1|x_1}(\sigma_{x_1})\otimes\sigma_{x_2})\otimes\dots\otimes\sigma_{x_{n-1}})\otimes\sigma_{x_n}\otimes|\vec{x}_n,\vec{k}_{n-1}\rangle\langle\vec{x}_n,\vec{k}_{n-1}|\right]. \tag{3}$$

A test of the hypotheses $\{\mathcal{N}, \overline{\mathcal{N}}\}$ on the true channel is a two-valued POVM $\{T_n, I - T_n\}$, where T_n is given as a Hermitian operator $\sum_{\vec{x}_n} T_{\vec{x}_n}\otimes|\vec{x}_n\rangle\langle\vec{x}_n|$ on $B^{\otimes n}\otimes X^{\otimes n}$ satisfying $0 \leqslant T_n \leqslant I$. Overall, our strategy to distinguish the channels $\{\mathcal{N}, \overline{\mathcal{N}}\}$ when n independent uses of each are available, is given by the triple $\mathcal{T}_n := (\{\Gamma^{(m)}_{k_m|\vec{x}_m,\vec{k}_{m-1}}\}_{m=1}^{n-1}, \{p_{X_m|\vec{X}_{m-1},\vec{K}_{m-1}}\}_{m=1}^{n}, T_n)$. The n-copy error probabilities of type I and type II are, respectively, as follows:

$$\alpha_n(\mathcal{N}\|\overline{\mathcal{N}}|\mathcal{T}_n) := \mathrm{Tr}\rho^{(n)}(I - T_n),$$
$$\beta_n(\mathcal{N}\|\overline{\mathcal{N}}|\mathcal{T}_n) := \mathrm{Tr}\sigma^{(n)}T_n.$$

The generalized Chernoff and Hoeffding quantities introduced in the Introduction read as follows in the present cq-channel case for a given class $\underline{\mathbb{S}} = \underline{\mathbb{P}}^0, \underline{\mathbb{A}}^{c,0}$:

$$C^{\underline{\mathbb{S}}}(a, b|\mathcal{N}\|\overline{\mathcal{N}}) := \sup_{\{\mathcal{T}_n\}}\left\{\liminf_{n\to\infty} -\frac{1}{n}\log_2[2^{an}\alpha_n(\mathcal{N}\|\overline{\mathcal{N}}|\mathcal{T}_n) + 2^{bn}\beta_n(\mathcal{N}\|\overline{\mathcal{N}}|\mathcal{T}_n)]\right\}, \tag{4}$$

$$B_e^{\underline{\mathbb{S}}}(r|\mathcal{N}\|\overline{\mathcal{N}}) := \sup_{\{\mathcal{T}_n\}}\left\{\liminf_{n\to\infty} -\frac{1}{n}\log_2[\alpha_n(\mathcal{N}\|\overline{\mathcal{N}}|\mathcal{T}_n)]\,\middle|\,\liminf_{n\to\infty} -\frac{1}{n}\log_2[\beta_n(\mathcal{N}\|\overline{\mathcal{N}}|\mathcal{T}_n)] \geqslant r\right\}, \tag{5}$$

where a, b, are arbitrary real numbers and r is an arbitrary non-negative number.

C. Main results

We set $\rho_x := \mathcal{N}(x)$ and $\sigma_x := \overline{\mathcal{N}}(x)$, and define

$$C(a, b|\mathcal{N}\|\overline{\mathcal{N}}) := \sup_x \sup_{0\leqslant\alpha\leqslant1} (1-\alpha)D_\alpha(\rho_x\|\sigma_x) - \alpha a - (1-\alpha)b$$
$$= \sup_{0\leqslant\alpha\leqslant1} (1-\alpha)D_\alpha(\mathcal{N}\|\overline{\mathcal{N}}) - \alpha a - (1-\alpha)b, \tag{6}$$

$$B(r|\mathcal{N}\|\overline{\mathcal{N}}) := \sup_x \sup_{0\leqslant\alpha\leqslant 1} \frac{\alpha-1}{\alpha}[r - D_\alpha(\rho_x\|\sigma_x)] = \sup_{0\leqslant\alpha\leqslant 1} \frac{\alpha-1}{\alpha}[r - D_\alpha(\mathcal{N}\|\overline{\mathcal{N}})], \tag{7}$$

where $D_\alpha(\mathcal{N}\|\overline{\mathcal{N}}) := \sup_x D_\alpha(\rho_x\|\sigma_x)$ and $D_\alpha(\rho_x\|\sigma_x) := \frac{1}{\alpha-1}\log_2 \mathrm{Tr}\rho_x^\alpha \sigma_x^{1-\alpha}$ is a quantum extension of the Rényi relative entropy. In this section, we abbreviate $C(a,b|\mathcal{N}\|\overline{\mathcal{N}})$ and $B(r|\mathcal{N}\|\overline{\mathcal{N}})$ to $C(a,b)$ and $B(r)$, respectively.

Since $D_\alpha(\rho_x\|\sigma_x)$ is monotonically increasing for α, $D_\alpha(\mathcal{N}\|\overline{\mathcal{N}})$ is monotonically increasing for α. Thus,

$$\begin{aligned}\lim_{\alpha\to 1} D_\alpha(\mathcal{N}\|\overline{\mathcal{N}}) &= \sup_{0\leqslant\alpha\leqslant 1} D_\alpha(\mathcal{N}\|\overline{\mathcal{N}}) = \sup_{0\leqslant\alpha\leqslant 1}\sup_x D_\alpha(\rho_x\|\sigma_x)\\ &= \sup_x \sup_{0\leqslant\alpha\leqslant 1} D_\alpha(\rho_x\|\sigma_x) = \sup_x D(\rho_x\|\sigma_x) = D(\mathcal{N}\|\overline{\mathcal{N}}).\end{aligned}$$

Before stating the main results of this section we shall study the $B(r)$ function further. Since the $B(r)$ function is monotonically decreasing in r, $B(D(\mathcal{N}\|\overline{\mathcal{N}}))=0$. To find $B(0)$, since $\frac{1-\alpha}{\alpha}D_\alpha(\mathcal{N}\|\overline{\mathcal{N}}) = D_{1-\alpha}(\overline{\mathcal{N}}\|\mathcal{N})$, we infer that $\frac{1-\alpha}{\alpha}D_\alpha(\mathcal{N}\|\overline{\mathcal{N}})$ is monotonically decreasing for α, and $D(\overline{\mathcal{N}}\|\mathcal{N}) = \lim_{\alpha\to 0}\frac{1-\alpha}{\alpha}D_\alpha(\mathcal{N}\|\overline{\mathcal{N}})$. Hence, $B(0) = D(\overline{\mathcal{N}}\|\mathcal{N})$, and $B(r) < D(\overline{\mathcal{N}}\|\mathcal{N})$ for $r>0$.

As shown in Appendix C, we have the following lemma.

Lemma 1. When real numbers a, b satisfy $-D(\mathcal{N}\|\overline{\mathcal{N}}) \leqslant a-b \leqslant D(\overline{\mathcal{N}}\|\mathcal{N})$, there exists $r_{a,b}\in[0, D(\mathcal{N}\|\overline{\mathcal{N}})]$ such that $B(r_{a,b}) - r_{a,b} = a-b$.

We are now in a position to present and prove our main result, the generalized Chernoff bound and Hoeffding bound as follows:

Theorem 1 (Generalized Chernoff bound and Hoeffding bound). For two cq channels $\mathcal{N}$ and $\overline{\mathcal{N}}$, we have

$$\begin{aligned}C^{\underline{\mathbb{A}}^{c,0}}(a,b|\mathcal{N}\|\overline{\mathcal{N}}) &= C^{\underline{\mathbb{P}}^0}(a,b|\mathcal{N}\|\overline{\mathcal{N}})\\ &= C(a,b) = r_{a,b} - b = B(r_{a,b}) - a\end{aligned}$$

for real numbers a, b satisfying $-D(\mathcal{N}\|\overline{\mathcal{N}}) \leqslant a-b \leqslant D(\overline{\mathcal{N}}\|\mathcal{N})$, and

$$B_e^{\underline{\mathbb{A}}^{c,0}}(r|\mathcal{N}\|\overline{\mathcal{N}}) = B_e^{\underline{\mathbb{P}}^0}(r|\mathcal{N}\|\overline{\mathcal{N}}) = B(r)$$

for any $0\leqslant r\leqslant D(\mathcal{N}\|\overline{\mathcal{N}})$. ■

This theorem is shown in Appendix D after various preparations. The key point of the proof of Theorem 1 is the reduction of our general strategy to the special strategy that restricts general instruments $\{\Gamma^{(m)}_{k_m|\vec{x}_m,\vec{k}_{m-1}}\}_{k_m\in\mathcal{K}_m}$ to the application of projective measurement with projection postulate. This reduction is stated as Proposition 2 in Appendix B. In this reduction, as stated in Lemma 8, we convert the cq channels into classical channels by means of the eigenvalue decomposition of the output states, using the two distributions introduced by [8,29].

III. FORMULATION OF GENERAL ADAPTIVE METHOD FOR QQ-CHANNEL DISCRIMINATION

Hereafter, the hypotheses are described by two qq channels, i.e., completely positive and trace-preserving (CPTP) maps, acting on a given quantum system, and more precisely $n\gg 1$ independent realizations of the unknown channel. It is not hard to see that both the type-I and type-II error probabilities can be made to go to 0 exponentially fast, just as in the case of hypotheses described by quantum states, and hence the fundamental question is the characterization of the possible pairs of error exponents.

We identify states ρ with their density operators and use superscripts to denote the systems on which the mathematical objects are defined. The set of density matrices (positive-semidefinite matrices with unit trace) on A is written as $\mathcal{S}^A$, a subset of the trace class operators, denoted $\mathcal{T}^A$. An operator is called projection operator if applying it twice has the same effect as applying it once, i.e., $\rho^2=\rho$. The subspace that the projection operator ρ projects onto is called its image and is denoted by $\mathrm{Im}\,\rho$. When talking about tensor products of spaces, we may habitually omit the tensor sign, so $A\otimes B = AB$, etc. The capital letters X, Y, etc., denote random variables whose realizations and the alphabets will be shown by the corresponding small and calligraphic letters, respectively: $X = x\in\mathcal{X}$. All Hilbert spaces and ranges of variables may be infinite; the dimension of a Hilbert space A is denoted $|A|$, as is the cardinality $|\mathcal{X}|$ of a set $\mathcal{X}$. For any positive integer m, we define $\vec{x}_m := (x_1,\ldots,x_m)$. For the state $\rho\in\mathcal{S}^{AB}$ in the composite system AB, the partial trace over system A (respectively B) is denoted by Tr_A (respectively Tr_B). We denote the identity operator by I. Moving on to quantum channels, these are linear, completely positive and trace-preserving maps $\mathcal{M}:\mathcal{S}^A\to\mathcal{S}^B$ for two quantum systems A and B; $\mathcal{M}$ extends uniquely to a linear map from trace class operators on A to those on B. We often denote quantum channels, by slight abuse of notation, as $\mathcal{M}: A\to B$. The input and output systems of quantum channels can include quantum and classical information; if both input and output systems are quantum, the channel is referred to as quantum-quantum channel (qq channel). Similarly, one can identify classical-quantum channels (cq channels) and quantum-classical channels (qc channels). The ideal, or identity, channel on A is denoted id_A. Note furthermore that a state ρ^A on a system A can be viewed as a quantum channel $\rho: 1\to A$, where 1 denotes the canonical one-dimensional Hilbert space, isomorphic to the complex numbers $\mathbb{C}$, which interprets a state operationally consistently as a state preparation procedure.

The most general operationally justified strategy to distinguish two channels $\mathcal{M}, \overline{\mathcal{M}}: A\to B$ is to prepare a state ρ^{RA}, apply the unknown channel to A (and the identity channel id_R to R), and then apply a binary measurement POVM $(T, I-T)$ on BR, so that

$$\alpha = \mathrm{Tr}[(\mathrm{id}_R\otimes\mathcal{M})\rho](I-T) \quad\text{and}\quad \beta = \mathrm{Tr}[(\mathrm{id}_R\otimes\overline{\mathcal{M}})\rho]T,$$

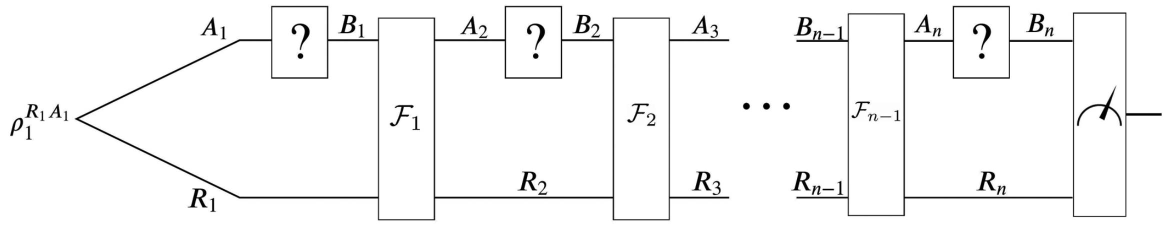

FIG. 2. The most general adaptive strategy for discrimination of qq channels, from the class $\mathbb{A}_n$. After the mth use of the unknown channel (denoted "?"), the output system B_m as well as the state on the memory, i.e., the reference system R_m, is processed by the CPTP map $\mathcal{F}_m$, resulting in $\rho_{m+1}^{R_{m+1}A_{m+1}}$; this continues as long as $m < n$. After the nth use of the channel, the state $\omega_n^{R_nB_n}$ is measured by a two-outcome POVM. Two variants of this strategy include restricting feed-forward information to be only classical, and additionally only allowing products state inputs; these variants are denoted by $\mathbb{A}_n^c$ and $\mathbb{A}_n^{c,0}$, respectively.

are the error probabilities of type I and type II, respectively. When we choose the system R to be sufficiently large, ρ^{RA} is a pure state. Since the rank of ρ^R is the same as the rank of ρ^A in this case, we can restrict the dimension of R to be $|A|$ without loss of generality. For more on the dimension of reference system, we refer to [23]. The strategy is entirely described by the pair $(\rho, (T, I-T))$ consisting of the initial state and the final measurement, and we denote it $\mathcal{T}$. Consequently, the above error probabilities are more precisely denoted $\alpha(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T})$ and $\beta(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T})$, respectively.

These strategies use the unknown channel exactly once; to use it $n > 1$ times, one could simply consider that $\mathcal{M}^{\otimes n}$ and $\overline{\mathcal{M}}^{\otimes n}$ are quantum channels themselves and apply the above recipe. While for states this indeed leads to the most general possible discrimination strategy, for general channels other, more elaborate, procedures are possible. The most general strategy we shall consider in this paper is the *adaptive* strategy, applying the n channel instances sequentially, using quantum memory and quantum feed forward, and a measurement at the end. This is called, variously, an adaptive strategy, a memory channel, or a comb in the literature. It is defined as follows [16,30–34].

Definition 1. A general adaptive strategy $\mathcal{T}_n$ is given by an $(n+1)$-tuple $(\rho_1^{R_1A_1}, \mathcal{F}_1, \dots, \mathcal{F}_{n-1}, (T, I-T))$, consisting of an auxiliary system R_1 and a state ρ_1 on R_1A_1, quantum channels $\mathcal{F}_m : R_mB_m \to R_{m+1}A_{m+1}$ and a binary POVM $(T, I-T)$ on R_nB_n. It encodes the following procedure (see Fig. 2): in the mth round ($1 \leqslant m \leqslant n$), apply the unknown channel $\Xi \in \{\mathcal{M}, \overline{\mathcal{M}}\}$ to $\rho_m = \rho_m^{R_mA_m}$, obtaining

$$\omega_m^{R_mB_m} = \omega_m^{R_mB_m}(\Xi) = (\mathrm{id}_{R_t} \otimes \Xi)\rho_m^{R_mA_m}.$$

Then, as long as $m < n$, use $\mathcal{F}_m$ to prepare the state for the next channel use:

$$\rho_{m+1}^{R_{m+1}A_{m+1}} = \mathcal{F}_m\big(\omega_m^{R_mB_m}\big).$$

When $m = n$, measure the state $\omega_n^{R_nB_n}$ with $(T, I-T)$, where the first outcome corresponds to declaring the unknown channel to be $\mathcal{M}$, the second $\overline{\mathcal{M}}$. Thus, the n-copy error probabilities of type I and type II are given by

$$\alpha_n(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T}_n) := \mathrm{Tr}\big[\omega_n^{R_nB_n}(\mathcal{M})\big](I-T),$$
$$\beta_n(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T}_n) := \mathrm{Tr}\big[\omega_n^{R_nB_n}(\overline{\mathcal{M}})\big]T,$$

respectively. ■

As in the case of a single use of the channel, one can without loss of generality simplify the strategy, by purifying the initial state ρ_1, hence $|R_1| \leqslant |A|$, and for each $m > 1$ going to the Stinespring isometric extension of the CPTP map $\mathrm{Tr}_{R_{m+1}} \circ \mathcal{F}_m : R_mB_m \to A_{m+1}$ that prepares the next channel input (and which by the uniqueness of the Stinespring extension is an extension of the given map $\mathcal{F}_m$). This requires a system R_{m+1} with dimension no more than $|R_{m+1}| \leqslant |R_m||A||B|$ (cf. [30]). This allows to efficiently parametrize all strategies in the case that A and B are finite dimensional. An equivalent description is in terms of so-called causal channels [30], which are ruled by a generalization of the Choi isomorphism. This turns many optimizations over adaptive strategies into semidefinite programs (SDP) [30,34–36], which is relevant for practical calculations. See [37,38] for recent comprehensive surveys of the concept of strategy and its history.

The set of all adaptive strategies of n sequential channel uses is denoted $\mathbb{A}_n$. It quite evidently includes the n parallel uses described at the beginning, when a single-use strategy is applied to the channel $(?)^{\otimes n}$, i.e., n-fold tensor product of the unknown channel; the set of these nonadaptive or parallel strategies is denoted $\mathbb{P}_n$. Among those again, we can distinguish the subclass of parallel strategies without quantum memory, meaning that $R = 1$ is trivial and that the input state ρ^{A^n} at the input system $A^n = A_1 \dots A_n$ is a product state $\rho^{A^n} = \rho_1^{A_1} \otimes \dots \otimes \rho_n^{A_n}$; this set is denoted $\mathbb{P}_n^0$. Other restricted sets of strategies we are considering in this paper are that of adaptive strategies with classical feed forward, denoted $\mathbb{A}_n^c$, and with classical feed forward and no quantum memory at the input, denoted $\mathbb{A}_n^{c,0}$, as well as no quantum memory at the input but quantum feed forward, denoted $\mathbb{A}_n^0$. They are defined formally in Sec. V.

The various classes considered obey the following inclusions that are evident from the definitions. Note that all of them are strict:

$$\begin{array}{ccccc} \mathbb{A}_n & \supset & \mathbb{A}_n^c & \supset & \mathbb{P}_n \\ \cup & & \cup & & \cup \\ \mathbb{A}_n^0 & \supset & \mathbb{A}_n^{c,0} & \supset & \mathbb{P}_n^0. \end{array} \qquad (8)$$

In Table I we show a summary of the different classes and their notation, and where they are discussed.

TABLE I. The different classes of adaptive strategies considered in this paper, how they are denoted, where they are defined. and which mathematical elements have to specified to identify a strategy from each class. In the last column we point to the sections of the paper containing results on the respective classes.

Name	Defined	Mathematical elements	Description	Discussed
$\mathbb{A}_n$	Def. 1, Fig. 2	State $\rho_1^{R_1A_1}$, channels $\mathcal{F}_m : R_mB_m \to R_{m+1}A_{m+1}$, POVM $(T, I-T)$	Most general adaptive strategy of n channel uses	Secs. IV, V A, VI B
$\mathbb{P}_n$	Def. 1, Fig. 3	State ρ^{RA^n}, POVM $(T, I-T)$	Most general nonadaptive (parallel) strategy allowing quantum memory at the input	Sec. IV
$\mathbb{P}_n^0$	Def. 1, Fig. 3	State $\rho_1^{A_1} \otimes \cdots \otimes \rho_n^{A_n}$, POVM $(T, I-T)$	Nonadaptive (parallel) strategy without quantum memory at the input	Secs. V A, V B, VI B
$\mathbb{A}_n^c$	Def. 2	State $\rho_1^{R_1A_1}$, instruments $\{\mathcal{F}_{\vec{k}_m} : B_mC_m \to C_{m+1}\}_{\vec{k}_m}$, cptp $\mathcal{P}_{\vec{k}_m} : R_m \to R_{m+1}A_{m+1}$, POVM $(T, I-T)$	Adaptive strategy of n channel uses with classical feed forward, but otherwise arbitrary quantum memory at the input	Sec. V C
$\mathbb{A}_n^{c,0}$	Def. 2, Fig. 4	States $\rho_{x_m}^{A_m}$, instruments $\{\mathcal{F}_{\vec{k}_m} : B_mC_m \to C_{m+1}\}_{\vec{k}_m}$, $q(x_m\vert\vec{x}_{m-1}, \vec{k}_{m-1})$, POVM $(T, I-T)$	Adaptive strategy of n channel uses with classical feed forward, and without quantum memory at the input	Secs. V B, V C,
$\mathbb{A}_n^0$	Def. 1, Rem. 3	State $\rho_1^{R_1A_1}$, channels $\mathcal{F}_m : B_mC_m \to A_{m+1}C_{m+1}$, POVM $(T, I-T)$	Adaptive strategy of n channel uses without quantum memory at the input, but otherwise arbitrary quantum feed forward	Sec. V C

For a given class $\mathbb{S}_n \subset \mathbb{A}_n$ of adaptive strategies for any number n of channel uses, the fundamental problem is now to characterize the possible pairs of error exponents for two channels $\mathcal{M}$ and $\overline{\mathcal{M}}$:

$$\mathfrak{E}(\mathcal{M}\|\overline{\mathcal{M}}|\mathbb{S}) := \left\{(r, s) : \exists \mathcal{T}_n \in \mathbb{S}_n \; 0 \leqslant r \leqslant \liminf_{n\to\infty} -\frac{1}{n}\log_2 \beta_n(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T}_n),\; 0 \leqslant s \leqslant \liminf_{n\to\infty} -\frac{1}{n}\log_2 \alpha_n(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T}_n)\right\}. \quad (9)$$

In particular, we are interested, for each $r \geqslant 0$, in the largest s such that $(r, s) \in \mathfrak{E}(\mathcal{M}\|\overline{\mathcal{M}}|\mathbb{S})$. To this end, we define the error rate tradeoff

$$B_e^{\mathbb{S}}(r|\mathcal{M}\|\overline{\mathcal{M}}) := \sup\left\{ s \left| \begin{array}{c} \exists \mathcal{T}_n \in \mathbb{S}_n \; r \leqslant \liminf_{n\to\infty} -\frac{1}{n}\log_2 \beta_n(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T}_n), \\ s \leqslant \liminf_{n\to\infty} -\frac{1}{n}\log_2 \alpha_n(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T}_n), \end{array}\right.\right\} \quad (10)$$

known as Hoeffding exponent, as well as the closely related function

$$C^{\mathbb{S}}(a, b|\mathcal{M}\|\overline{\mathcal{M}}) := \inf_{\mathcal{T}_n\in\mathbb{S}_n} \liminf_{n\to\infty} -\frac{1}{n}\log_2[2^{na}\alpha_n(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T}_n) + 2^{nb}\beta_n(\mathcal{M}\|\overline{\mathcal{M}}|\mathcal{T}_n)]. \quad (11)$$

Note that $\mathfrak{E}(\mathcal{M}\|\overline{\mathcal{M}}|\mathbb{S})$ is a closed set by definition, and for most "natural" restrictions $\mathbb{S}$, it is also convex. In the latter case, the graph of $B_e^{\mathbb{S}}(r|\mathcal{M}\|\overline{\mathcal{M}})$ traces the upper boundary of $\mathfrak{E}(\mathcal{M}\|\overline{\mathcal{M}}|\mathbb{S})$, and it can be reconstructed from $C^{\mathbb{S}}(a, b|\mathcal{M}\|\overline{\mathcal{M}})$ by a Legendre transform.

Historically, two extreme regimes are of special interest: the maximally asymmetric error exponent,

$$\max r \text{ s.t. } \exists s\; (r, s) \in \mathfrak{E}(\mathcal{M}\|\overline{\mathcal{M}}|\mathbb{S}) = \max r \text{ s.t. } (r, 0) \in \mathfrak{E}(\mathcal{M}\|\overline{\mathcal{M}}|\mathbb{S}),$$

together with the opposite one of maximization of s, which are known as Stein's exponents, and the symmetric error exponent

$$\begin{aligned} C^{\mathbb{S}}(\mathcal{M}, \overline{\mathcal{M}}) &= \max r \text{ s.t. } (r, r) \in \mathfrak{E}(\mathcal{M}\|\overline{\mathcal{M}}|\mathbb{S}) \\ &= C^{\mathbb{S}}(0, 0|\mathcal{M}\|\overline{\mathcal{M}}), \end{aligned}$$

which is generally known as Chernoff exponent or Chernoff bound.

In this paper, we assume that all Hilbert spaces of interest are separable, i.e., they are spanned by countable bases, and we are primarily occupied with the performance of adaptive strategies. Naturally, the first question in this search would be to investigate the existence of quantum channels for which some class $\mathbb{S}_n \subset \mathbb{A}_n$ outperforms the parallel strategy when $n \to \infty$; in other words, if there exists a separation between adaptive and nonadaptive strategies. We study this question in general, and in particular when the channels are entanglement breaking of the following form:

$$\mathcal{M}(\xi) = \sum_x (\mathrm{Tr} E_x \xi)\rho_x, \quad \overline{\mathcal{M}}(\xi) = \sum_x (\mathrm{Tr} E'_x \xi)\sigma_x, \tag{12}$$

where $\{E_x\}$ and $\{E'_x\}$ are PVMs and ρ_x, σ_x are states on the output system. We show that when these two PVMs are the same, $E_x = E'_x$, then the largest class $\mathbb{A}_n$ cannot outperform the parallel strategy as $n \to \infty$. When the two PVMs are different, we find two examples such that the largest class $\mathbb{A}_n$ outperforms the parallel strategies as $n \to \infty$. For a general pair of qq channels we focus on the class $\mathbb{A}_n^{c,0}$ of strategies without quantum memory at the sender's side and with adaptive strategies that only allow for classical discrete feed forward. We show that the class $\mathbb{A}_n^{c,0}$ cannot outperform the parallel strategies when $n \to \infty$. These findings are then applied to the discrimination power of a quantum channel, which quantifies how well two given states in $A^{\otimes n}$ can be discriminated after passing through a quantum channel, and whether adaptive strategies can be beneficial. To this end, we focus on a particular class of channels, namely, cq channels, and investigate if the most general strategy offers any benefit over the most weak strategy $\mathbb{P}_n^0$. This study takes an essential role in the above problems.

IV. THE FIRST ASYMPTOTIC SEPARATION BETWEEN ADAPTIVE AND NONADAPTIVE STRATEGIES

A. Useful proposition for asymptotic separation

In this section we exhibit an asymptotic separation between the Chernoff error exponents of discriminating between two channels by adaptive versus nonadaptive strategies. Concretely, we will show that two channels described in [14], and shown to be perfectly distinguishable by adaptive strategies of $n \geqslant 2$ copies, hence having infinite Chernoff exponent, nevertheless have a finite-error exponent under nonadaptive strategies.

The separation is based on a general lower bound on nonadaptive strategies for an arbitrary pair of channels. Consider two quantum channels, i.e., CPTP maps, $\mathcal{M}, \overline{\mathcal{M}} : A \to B$. To fix notation, we can write their Kraus decompositions as

$$\mathcal{M}(\rho) = \sum_i E_i \rho E_i^\dagger, \quad \overline{\mathcal{M}}(\rho) = \sum_j F_j \rho F_j^\dagger.$$

The most general strategy to distinguish them consists in the preparation of a, without loss of generality pure, state φ on $A \otimes R$, where $R \simeq A$, send it through the unknown channel, and make a binary measurement $(T, I - T)$ on $B \otimes R$:

$$p = \mathrm{Tr}[(\mathrm{id}_R \otimes \mathcal{M})\varphi]T, \quad q = \mathrm{Tr}[(\mathrm{id}_R \otimes \overline{\mathcal{M}})\varphi]T,$$

and likewise $1 - p$ and $1 - q$ by replacing T in the above formulas with $I - T$. Note that for uniform prior probabilities on the two hypotheses, the error probability in inferring the true channel from the measurement output is $\frac{1}{2}(1 - |p - q|)$.

The maximum of $|p - q|$ over state preparations and measurements gives rise to the (normalized) diamond norm distance of the channels [35,39–41]:

$$\max_{\varphi,T} |p - q| = \frac{1}{2}\|\mathcal{M} - \overline{\mathcal{M}}\|_\diamond,$$

which in turn quantifies the minimum discrimination error under the most general quantum strategy:

$$P_e = \frac{1}{2}\left(1 - \frac{1}{2}\|\mathcal{M} - \overline{\mathcal{M}}\|_\diamond\right).$$

We are interested in the asymptotics of this error probability when the discrimination strategy has access to $n \gg 1$ many instances of the unknown channel in parallel, or in other words, in a nonadaptive way. This means effectively that the two hypotheses are the simple channels $\mathcal{M}^{\otimes n}$ and $\overline{\mathcal{M}}^{\otimes n}$, so that the error probability is

$$P_{e,\mathbb{P}}^{(n)} = \frac{1}{2}\left(1 - \frac{1}{2}\left\|\mathcal{M}^{\otimes n} - \overline{\mathcal{M}}^{\otimes n}\right\|_\diamond\right).$$

The (nonadaptive) Chernoff exponent is then given as

$$C^{\mathbb{P}}(\mathcal{M}, \overline{\mathcal{M}}) = \lim_{n\to\infty} -\frac{1}{n}\log_2 P_{e,\mathbb{P}}^{(n)},$$

the existence of the limit being guaranteed by general principles. Note that the limit can be $+\infty$, which happens in all cases where there is an n such that $P_{e,\mathbb{P}}^{(n)} = 0$. It is currently unknown whether this is the only case; cf. the case of the more flexible adaptive strategies, for which there is a simple criterion to determine whether there exists an n such that the adaptive error probability $P_{e,\mathbb{A}}^{(n)} = 0$ [21], and then evidently $C^{\mathbb{A}}(\mathcal{M}, \overline{\mathcal{M}}) = +\infty$; conversely, we know that in all other cases, the adaptive Chernoff exponent is $C^{\mathbb{A}}(\mathcal{M}, \overline{\mathcal{M}}) < +\infty$ [42]. There exist also other lower bounds on the symmetric discrimination error by adaptive strategies, for instance [43, Theorem 3] geared towards finite n.

Duan *et al.* [22] have attempted a characterization of the channel pairs such that there exists an n with $P_{e,\mathbb{P}}^{(n)} = 0$, and have given a simple sufficient condition for the contrary. Namely, the existing result [22, Corollary 1] states that if $\mathrm{span}\{E_i^\dagger F_j\}$ contains a positive-definite element, then for all n we have $P_{e,\mathbb{P}}^{(n)} > 0$. The following proposition, which makes the result of [22] quantitative, is the main result of this section.

Proposition 1. When complex numbers $\gamma_{ij} \in \mathbb{C}$ satisfy the condition that $\sum_{ij} |\gamma_{ij}|^2 = 1$ and $P := \sum_{ij} \gamma_{ij} E_i^\dagger F_j > 0$, i.e., P is positive definite, then the inequality

$$P_{e,\mathbb{P}}^{(n)} \geqslant \frac{1}{4}\lambda_{\min}(P)^{4n}$$

holds for all n, where $\lambda_{\min}(A)$ denotes the smallest eigenvalue of the Hermitian operator A. Consequently,

$$C^{\mathbb{P}}(\mathcal{M}, \overline{\mathcal{M}}) \leqslant 4\log_2 \|P^{-1}\|_\infty.$$

Proof. We begin with a test state φ as in the above description of the most general nonadaptive strategy for the channels $\mathcal{M}$ and $\overline{\mathcal{M}}$, so that the two output states are $\rho = (\mathrm{id}_R \otimes \mathcal{M})\varphi$, $\sigma = (\mathrm{id}_R \otimes \overline{\mathcal{M}})\varphi$. By well-known inequalities [44], it holds

$$\frac{1}{2}\|\rho - \sigma\|_1 \leqslant \sqrt{1 - F(\rho, \sigma)^2} \leqslant 1 - \frac{1}{2}F(\rho, \sigma)^2,$$

where $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ is the fidelity. Thus, it will be enough to lower bound the fidelity between the output states of the two channels. With $\tau = \mathrm{Tr}_R|\varphi\rangle\langle\varphi|$, we have

$$\begin{aligned} F(\rho,\sigma) &= \|\sqrt{\rho}\sqrt{\sigma}\|_1 \\ &\geqslant \mathrm{Tr}\sqrt{\rho}\sqrt{\sigma} \\ &\geqslant \mathrm{Tr}\rho\sigma \\ &= \sum_{ij} |\mathrm{Tr}E_i^\dagger F_j\tau|^2 \\ &\geqslant \left|\sum_{ij}\gamma_{ij}\mathrm{Tr}E_i^\dagger F_j\tau\right|^2 \\ &= |\mathrm{Tr}\tau P|^2. \end{aligned}$$

Here, the second line is by standard inequalities for the trace norm, the third is because of $\rho \leqslant \sqrt{\rho}$, the fourth is a formula from [22, Sec. II], in the fifth we used Cauchy-Schwarz inequality, and in the last line the definition of P. Since τ, like φ, ranges over all states, we get

$$F(\rho,\sigma)^2 \geqslant \lambda_{\min}(P)^4,$$

and so

$$P_e \geqslant \frac{1}{4}\lambda_{\min}(P)^4.$$

We can apply the same reasoning to $\mathcal{M}^{\otimes n}$ and $\overline{\mathcal{M}}^{\otimes n}$, for which the vector $(\gamma_{ij})^{\otimes n}$ is eligible and leads to the positive-definite operator $P^{\otimes n}$. Thus,

$$P_{e,\mathbb{P}}^{(n)} \geqslant \frac{1}{4}\lambda_{\min}(P^{\otimes n})^4 = \frac{1}{4}\lambda_{\min}(P)^{4n}.$$

Taking the limit and noting $\lambda_{\min}(P)^{-1} = \|P^{-1}\|_\infty$ concludes the proof. ∎

B. Two examples

Example 1. Next we show that two channels defined by Harrow *et al.* [14] yield an example of a pair with $C^{\mathbb{P}}(\mathcal{M},\overline{\mathcal{M}}) < +\infty$, yet $C^{\mathbb{A}}(\mathcal{M},\overline{\mathcal{M}}) = +\infty$ because indeed $P_{e,\mathbb{A}}^{(2)} = 0$. In [14], the following two entanglement-breaking channels from $A\otimes C = \mathbb{C}^2\otimes\mathbb{C}^2$ (two qubits) to $B = \mathbb{C}^2$ (one qubit) are considered:

$$\begin{aligned} \mathcal{M}(\rho^A\otimes\gamma^C) &= |0\rangle\langle 0|\,\langle 0|\gamma|0\rangle + |0\rangle\langle 0|\,\langle 1|\gamma|1\rangle\langle 0|\rho|0\rangle \\ &\quad + \frac{1}{2}I\langle 1|\gamma|1\rangle\langle 1|\rho|1\rangle, \\ \overline{\mathcal{M}}(\rho^A\otimes\gamma^C) &= |+\rangle\langle +|\,\langle 0|\gamma|0\rangle + |1\rangle\langle 1|\,\langle 1|\gamma|1\rangle\langle +|\rho|+\rangle \\ &\quad + \frac{1}{2}I\langle 1|\gamma|1\rangle\langle -|\rho|-\rangle, \end{aligned}$$

extended by linearity to all states. Here, $|0\rangle, |1\rangle$ are the computational basis (Z eigenbasis) of the qubits, while $|+\rangle, |-\rangle$ are the Hadamard basis (X eigenbasis).

In words, both channels measure the qubit C in the computational basis. If the outcome is "0," they each prepare a pure state on B (ignoring the input in A): $|0\rangle\langle 0|$ for $\mathcal{M}$, $|+\rangle\langle +|$ for $\overline{\mathcal{M}}$. If the outcome is "1," they each make a measurement on A and prepare an output state on B depending on its outcome: standard basis measurement for $\mathcal{M}$ with $|0\rangle\langle 0|$ on outcome 0 and the maximally mixed state $\frac{1}{2}I$ on outcome 1 Hadamard basis measurement for $\overline{\mathcal{M}}$ with $|1\rangle\langle 1|$ on outcome "+" and the maximally mixed state $\frac{1}{2}I$ on outcome "-". In [14], a simple adaptive strategy for $n = 2$ uses of the channel is given that discriminates $\mathcal{M}$ and $\overline{\mathcal{M}}$ perfectly: The first instance of the channel is fed with $|0\rangle\langle 0|\otimes|0\rangle\langle 0|$, resulting in an output state ρ_1; the second instance of the channel is fed with $|1\rangle\langle 1|\otimes\rho_1$; the output state ρ_2 of the second instance is $|0\rangle\langle 0|$ if the unknown channel is $\mathcal{M}$, and $|1\rangle\langle 1|$ if the unknown channel is $\overline{\mathcal{M}}$, so a computational basis measurement reveals it. Note that no auxiliary system R is needed, but the feed forward nevertheless requires a qubit of quantum memory for the strategy to be implemented. In any case, this proves that $P_{e,\mathbb{A}}^{(2)} = 0$. In [14], it is furthermore proved that for all $n \geqslant 1$, $P_{e,\mathbb{P}}^{(n)} > 0$.

We now show that Proposition 1 is applicable to yield an exponential lower bound on the nonadaptive error probability. The Kraus operators of the two channels can be chosen as follows:

$$\begin{aligned} \mathcal{M}: E_i \in \{&|0\rangle^B\langle 00|^{AC}, & \overline{\mathcal{M}}: F_j \in \{&|+\rangle^B\langle 00|^{AC}, \\ &|0\rangle^B\langle 10|^{AC}, & &|+\rangle^B\langle 10|^{AC}, \\ &|0\rangle^B\langle 01|^{AC}, & &|1\rangle^B\langle +1|^{AC}, \\ &|0\rangle^B\langle 11|^{AC}/\sqrt{2}, & &|0\rangle^B\langle -1|^{AC}/\sqrt{2}, \\ &|1\rangle^B\langle 11|^{AC}/\sqrt{2}\}, & &|1\rangle^B\langle -1|^{AC}/\sqrt{2}\}. \end{aligned}$$

Thus, the products $E_i^\dagger F_j$ include the matrices

$$\begin{aligned} E_1^\dagger F_1 &= \sqrt{\frac{1}{2}}\,|00\rangle\langle 00|, \\ E_2^\dagger F_2 &= \sqrt{\frac{1}{2}}\,|10\rangle\langle 10|, \\ E_5^\dagger F_3 &= \sqrt{\frac{1}{2}}|11\rangle\langle +1|, \\ E_5^\dagger F_5 &= \frac{1}{2}\,|11\rangle\langle -1|, \\ E_3^\dagger F_4 &= \sqrt{\frac{1}{2}}\,|01\rangle\langle -1|, \end{aligned}$$

from which we can form, by linear combination, the operators

$$\begin{aligned} E_1^\dagger F_1 &= \sqrt{\frac{1}{2}}\,|0\rangle\langle 0|\otimes|0\rangle\langle 0|, \\ E_2^\dagger F_2 &= \sqrt{\frac{1}{2}}\,|1\rangle\langle 1|\otimes|0\rangle\langle 0|, \\ \sqrt{\frac{1}{2}}E_5^\dagger F_3 - E_5^\dagger F_5 &= \sqrt{\frac{1}{2}}\,|1\rangle\langle 1|\otimes|1\rangle\langle 1|, \\ \sqrt{\frac{1}{2}}E_3^\dagger F_4 - E_5^\dagger F_5 &= \sqrt{\frac{1}{2}}\,|-\rangle\langle -|\otimes|1\rangle\langle 1|, \end{aligned}$$

whose sum is indeed positive definite, so we get an exponential lower bound on $P_{e,\mathbb{P}}^{(n)}$ and hence a finite value of $C^{\mathbb{P}}(\mathcal{M},\overline{\mathcal{M}})$. To get a concrete upper bound on $C^{\mathbb{P}}(\mathcal{M},\overline{\mathcal{M}})$ from the above method, we choose $\gamma_{11} = \gamma_{22} = \alpha$ and $\gamma_{53} = \gamma_{34} = \gamma_{55} = \beta$, with $\alpha, \beta > 0$ and $2\alpha^2 + 5\beta^2 = 1$ and $\gamma_{i,j} =$

0 for other cases in Proposition 1. Then, P is written as

$$\begin{aligned} P &= \alpha E_1^\dagger F_1 + \alpha E_2^\dagger F_2 + \beta\sqrt{\frac{1}{2}}E_5^\dagger F_3 + \beta\sqrt{\frac{1}{2}}E_3^\dagger F_4 - 2\beta E_5^\dagger F_5 \\ &= \alpha\sqrt{\frac{1}{2}}I \otimes |0\rangle\langle 0| + \beta\sqrt{\frac{1}{2}}(|1\rangle\langle 1| + |-\rangle\langle -|) \otimes |1\rangle\langle 1|, \end{aligned}$$

which implies the condition $P > 0$. Now, P is an orthogonal sum of two rank-2 operators, i.e., as a 4×4 matrix it has block-diagonal structure with two 2×2 blocks. Their minimum eigenvalues are easily calculated: they are $\alpha\sqrt{\frac{1}{2}}$ and $\beta\sqrt{2}\sin^2\frac{\pi}{8}$. Since $\lambda_{\min}(P)$ will be the smaller of the two, we optimize it by making the two values equal, i.e., we want $\alpha = 2\beta\, \sin^2\frac{\pi}{8}$. Inserting this in the normalization condition and solving for β yields $\beta^2 = (8\, \sin^4\frac{\pi}{8} + 5)^{-1}$, thus,

$$\lambda_{\min}(P) = \sqrt{\frac{2}{8\, \sin^4\frac{\pi}{8} + 5}}\sin^2\frac{\pi}{8} = \frac{2-\sqrt{2}}{4\sqrt{4-\sqrt{2}}} \approx 0.091,$$

where we have used the identity $\sin^2\frac{\pi}{8} = \frac{1}{2}(1 - \sqrt{\frac{1}{2}})$. Hence, Proposition 1 guarantees that

$$C^{\mathbb{P}}(\mathcal{M}, \overline{\mathcal{M}}) \leqslant 4\, \log_2\frac{4\sqrt{4-\sqrt{2}}}{2-\sqrt{2}} \approx 13.83.$$

Note that a lower bound is the Chernoff bound of the two pure output states $|0\rangle\langle 0| = \mathcal{M}(|00\rangle\langle 00|)$ and $|+\rangle\langle +| = \overline{\mathcal{M}}(|00\rangle\langle 00|)$, which is $\log_2 = 1$, so $C^{\mathbb{P}}(\mathcal{M}, \overline{\mathcal{M}}) \geqslant 1$. It seems reasonable to conjecture that this is optimal, but we do not have at present a proof of it. ■

Example 2. For later use, we briefly discuss another example due to Krawiec *et al.* [15], which consists of two qc channels implementing two rank-1 POVMs on a qutrit A, and the output Y is a nine-dimensional Hilbert space. They are given by vectors $|x_i\rangle \in A$ and $|y_i\rangle \in A$ $(i = 1, \ldots, 9)$ such that $\sum_{i=1}^9 |x_i\rangle\langle x_i| = \sum_{j=1}^9 |y_j\rangle\langle y_j| = I$:

$$\mathcal{P}(\rho) = \sum_{i=1}^{9}\langle x_i|\rho|x_i\rangle\, |i\rangle\langle i|, \quad \overline{\mathcal{P}}(\rho) = \sum_{j=1}^{9}\langle y_j|\rho|y_j\rangle\, |j\rangle\langle j|. \tag{13}$$

The Kraus operators are $E_i = |i\rangle\langle x_i|$ and $F_j = |j\rangle\langle y_j|$, which makes it easy to calculate $\text{span}\{E_i^\dagger F_j\} = \text{span}\{|x_i\rangle\langle y_i|\}$.

In [15] it is shown how to choose the two POVMs in such a way that this subspace does not contain the identity I and indeed satisfies the "disjointness" condition of Duan *et al.* [21] for perfect finite-copy distinguishability of the two channels using adaptive strategies. Thus, $C^{\mathbb{A}}(\mathcal{P}, \overline{\mathcal{P}}) = +\infty$. On the other hand, it is proven in [15] that the subspace contains a positive-definite matrix $P > 0$. Hence, Proposition 1 guarantees that $C^{\mathbb{P}}(\mathcal{P}, \overline{\mathcal{P}}) < +\infty$. ■

So indeed there are channels, entanglement-breaking channels at that, for which the adaptive and the nonadaptive Chernoff exponents are different; in fact, the separation is maximal, in that the former is $+\infty$ while the latter is finite: they lend themselves easily to experiments, as the channels of Example 1 are composed of simple qubit measurement and state preparations. It should be noted that this separation is a robust phenomenon, and not for example related to the perfect finite-copy distinguishability. Namely, by simply mixing our example channels with the same small fraction $\epsilon > 0$ of the completely depolarizing channel τ, we get two new channels $\mathcal{M}' = (1-\epsilon)\mathcal{M} + \epsilon\tau$ and $\overline{\mathcal{M}}' = (1-\epsilon)\overline{\mathcal{M}} + \epsilon\tau$ with only smaller nonadaptive Chernoff bound $C^{\mathbb{P}}(\mathcal{M}', \overline{\mathcal{M}}') \leqslant C^{\mathbb{P}}(\mathcal{M}, \overline{\mathcal{M}}) < +\infty$. As shown below, by choosing a suitable $\epsilon > 0$, the fully general adaptive strategy satisfies

$$C^{\mathbb{P}}(\mathcal{M}, \overline{\mathcal{M}}) < C^{\mathbb{A}}(\mathcal{M}', \overline{\mathcal{M}}') < \infty. \tag{14}$$

This case gives an example for the asymptotic separation between adaptive and nonadaptive strategies even with a finite exponent for adaptive strategy.

Now, we show the existence of $\epsilon > 0$ to satisfy (14). Because $C^{\mathbb{A}}(\mathcal{M}', \overline{\mathcal{M}}')$ goes to infinity as ϵ goes to zero, there exists $\epsilon > 0$ to satisfy the first inequality in (14). On the other hand, the relation $C^{\mathbb{A}}(\mathcal{M}', \overline{\mathcal{M}}') < +\infty$ with an arbitrary $\epsilon > 0$ can be shown in the following way. Because the Kraus operators $\{E_i'\}$ and $\{F_j'\}$ of the channels satisfy $I \in \text{span}\{E_i'^\dagger F_j'\}$, Duan *et al.* [21] guarantee that $\mathcal{M}'$ and $\overline{\mathcal{M}}'$ are not perfectly distinguishable under any $\mathbb{A}_n$ for any finite n. Applying this fact to the result by Yu and Zhou [42], we find the existence of a finite upper bound on the Chernoff exponent $C^{\mathbb{A}}(\mathcal{M}', \overline{\mathcal{M}}')$.

Furthermore, since the error-rate tradeoff function $B_e^{\mathbb{P}}(r|\mathcal{M}\|\overline{\mathcal{M}})$ is continuous near $r = C^{\mathbb{P}}(\mathcal{M}, \overline{\mathcal{M}})$, whereas the adaptive variant $B_e^{\mathbb{A}}(r|\mathcal{M}\|\overline{\mathcal{M}})$ is infinite everywhere, we automatically get separations in the Hoeffding setting, as well. Note that there is no contradiction with the results of [17,24], which showed equality of the adaptive and the nonadaptive Stein's exponents, which are indeed both $+\infty$: for the nonadaptive one this follows from the fact that the channels on the same input prepare different pure states $|0\rangle\langle 0|$ for $\mathcal{M}$ and $|+\rangle\langle +|$ for $\overline{\mathcal{M}}$.

V. RESPONSIBLE RESOURCES FOR QUANTUM ADVANTAGE

We showed in Sec. IV that quantum feed forward can improve the error exponent in the symmetric and Hoeffding settings for the discrimination of two qq channels. This result followed by investigating a pair of entanglement-breaking channels introduced in [14], and a pair of qc channels from [15].

In contrast, this section investigates which features of general feed-forward strategies are responsible for this advantage and, conversely, which restricted feed-forward strategies cannot improve the error exponents for discrimination of two qq channels. To address this question, we first import the results on cq channels from Sec. II to a special class of qq channels. Note that if $\mathcal{X}$ is discrete, i.e., either finite or countably infinite, with the atomic (power set) Borel algebra, so that arbitrary mappings $\mathcal{N} : x \to \rho_x$ and $\overline{\mathcal{N}} : x \to \sigma_x$ define cq channels, we can think of them as special, entanglement-breaking, qq channels $\mathcal{M}, \overline{\mathcal{M}} : \mathcal{T}^{\mathcal{X}} \to \mathcal{T}^{\mathcal{B}}$:

$$\mathcal{M}(\xi) = \sum_{x\in\mathcal{X}} \rho_x \text{Tr}\xi E_x, \quad \overline{\mathcal{M}}(\xi) = \sum_{x\in\mathcal{X}} \sigma_x \text{Tr}\xi E_x, \tag{15}$$

where $\{E_x\}_{x\in\mathcal{X}}$ is a PVM of rank-1 projectors $E_x = |x\rangle\langle x|$, and $\mathcal{X}$ labels an orthonormal basis $\{|x\rangle\}_{x\in\mathcal{X}}$ of a separable Hilbert space, denoted $\mathcal{X}$, too [cf. Eq. (12)].

In particular, using the results of Sec. II, we will show the following fact for discrimination of special entanglement-breaking channels given by Eq. (15). The most general class of adaptive strategies $\mathbb{A}_n$ offers no gain over the weakest class of strategies $\mathbb{P}_n^0$, i.e., nonadaptive strategies without entangled input, even though this class uses entangled input and quantum feed forward. Since in the analysis of cq channels it turns out that the most general strategy does not use quantum memory at the input and feed forward that is classical, we are motivated to consider this restricted class of adaptive strategies for general qq channels, denoted $\mathbb{A}_n^{c,0}$, in Sec. V B. We will show that this subclass of adaptive strategies offers no gain over nonadaptive strategies without quantum memory at the input. Finally, in Sec. V C we consider whether it is really necessary to impose both the restriction of no input quantum memory and classical feed forward to rule out an advantage for nonadaptive strategies. Indeed, we shall show that the examples considered in Sec. IV demonstrate asymptotic advantages both for adaptive strategies with no input quantum memory but quantum feed forward ("$\mathbb{A}_n^0$") and for adaptive strategies with quantum memory at the input and classical feed forward ("$\mathbb{A}_n^c$").

A. Discrimination of cq channels as CPTP maps under $\mathbb{A}_n$ strategies

The most general class $\mathbb{A}_n$ of strategies to distinguish two qq channels $\mathcal{M}$ and $\overline{\mathcal{M}}$ is the set of strategies given in Definition 1. For this class, recall that we denote the generalized Chernoff and Hoeffding quantities as $C^{\mathbb{A}}(a, b|\mathcal{M}\|\overline{\mathcal{M}})$ and $B_e^{\mathbb{A}}(r|\mathcal{M}\|\overline{\mathcal{M}})$, respectively. In this section, we discuss the effect of input entanglement for our cq-channel discrimination strategy, when the input alphabet is discrete. Recall the form (15) of the two channels as qq-quantum channels.

In this case, the most general strategy stated in Definition 1 for the discrimination of two qq channels $\mathcal{M}$ and $\overline{\mathcal{M}}$ can be converted to the strategy stated in Sec. II B for the discrimination of two cq channels $\mathcal{N} : x \mapsto \rho_x$ and $\overline{\mathcal{N}} : x \mapsto \sigma_x$ as follows. In the general strategy for qq channel, the operation in the mth step is given as a quantum channel $\mathcal{F}_m : R_mB_m \to R_{m+1}A_{m+1}$. To describe the general strategy for cq channel, we define the quantum instrument $\mathcal{E}_m : R_mB_m \to X_mR_{m+1}$ in the sense of Eq; (1) as

$$\mathcal{E}_m(\xi) := \sum_{x_m\in\mathcal{X}} |x_m\rangle\langle x_m| \otimes [\mathrm{Tr}_{A_{m+1}} E_{x_m}\mathcal{F}_m(\xi)]. \tag{16}$$

Then, the general strategy for cq channel is given as applying the above quantum instrument and choosing the obtained outcome x_m as the input of the cq channel to be discriminated. The final states in the general strategy for qq channel are the same as the final state in the general strategy for cq channel. That is, the performance of the general strategy for these two qq channels is the same as the performance of the general strategy for the above-defined cq channels. This fact means that the adaptive method does not improve the performance of the discrimination of the channels (15).

Furthermore, when the quantum channel $\mathcal{F}_m$ in the strategy is replaced by the channel $\mathcal{F}'_m$ defined as $\mathcal{F}'_m(\xi) := \sum_{x_m} E_{x_m}\mathcal{F}_m(\xi)E_{x_m}$, we do not change the statistics of the protocol for either channel. Since the output of $\mathcal{F}'_m$ has no entanglement between X_m and R_{m+1}, the presence of input entanglement does not improve the performance in this case.

To state the next result, define for two quantum channels $\mathcal{M}$ and $\overline{\mathcal{M}}$ mapping A to B,

$$D(\mathcal{M}\|\overline{\mathcal{M}}) := \sup_{\rho\in\mathcal{S}^A} D(\mathcal{M}(\rho)\|\overline{\mathcal{M}}(\rho)) \text{ and} \tag{17}$$

$$D_\alpha(\mathcal{M}\|\overline{\mathcal{M}}) := \sup_{\rho\in\mathcal{S}^A} D_\alpha(\mathcal{M}(\rho)\|\overline{\mathcal{M}}(\rho)). \tag{18}$$

Theorem 2. Assume that two qq-quantum channels $\mathcal{M}$ and $\overline{\mathcal{M}}$ are given by Eq. (15). For $0 \leqslant r \leqslant D(\mathcal{M}\|\overline{\mathcal{M}})$ and real a and b with $-D(\mathcal{M}\|\overline{\mathcal{M}}) \leqslant a - b \leqslant D(\overline{\mathcal{M}}\|\mathcal{M})$, the following holds:

$$C^{\mathbb{A}}(a, b|\mathcal{M}\|\overline{\mathcal{M}}) = C^{\mathbb{P}^0}(a, b|\mathcal{M}\|\overline{\mathcal{M}}) = C(a, b|\mathcal{N}\|\overline{\mathcal{N}}),$$

$$B_e^{\mathbb{A}}(r|\mathcal{M}\|\overline{\mathcal{M}}) = B_e^{\mathbb{P}^0}(r|\mathcal{M}\|\overline{\mathcal{M}}) = B_e(r|\mathcal{N}\|\overline{\mathcal{N}}).$$

■

Note that it was essential that not only the channels are entanglement breaking, but that the measurement $\{E_x\}$ is a PVM, and in fact the same PVM for both channels. The discussion fails already when the channels each have their own PVM, which are noncommuting. Indeed, such channels were essential to the counterexample in Sec. IV, Example 1, showing a genuine advantage of general adaptive strategies. In this case, the construction of the channel $\mathcal{F}'_m$ depends on the choice of the hypothesis. Therefore, the condition (15) is essential for this discussion.

Furthermore, if the channels are entanglement breaking, but with a general POVM in Eq. (15), i.e., the E_x are not orthogonal projectors, the above discussion does not hold, either. Indeed, the second counterexample in Sec. IV, Example 2, consists of qc channels implementing overcomplete rank-1 measurements, once more showing a genuine advantage of general adaptive strategies. In this case, the output state is separable, but it cannot be necessarily simulated by a separable input state.

Remark 1. The discussion of this section shows that without loss of generality, we can assume that the measurement outcome equals the next input when $\mathcal{X}$ is discrete. That is, it is sufficient to consider the case when $k_m = x_m$. This fact can be shown as follows. Given two cq channels $x \mapsto \rho_x$ and $x \mapsto \sigma_x$, we define two entanglement-breaking channels $\mathcal{M}$ and $\overline{\mathcal{M}}$ by Eq. (15). For the case with two qq channels, the most general strategy is given in Definition 1. For two cq channels $\mathcal{M} : x \mapsto \rho_x$ and $\overline{\mathcal{M}} : x \mapsto \sigma_x$, the most general strategy can be simulated by an instrument with $k_m = x_m$.

However, when $\mathcal{X}$ is not discrete, neither can we view the cq channels as special qq channels [as the Definition in Eq. (15) only makes sense for discrete $\mathcal{X}$], nor do we allow arbitrary, only discrete feed forward; hence, to cover the case with continuous $\mathcal{X}$, we need to address it using general outcomes k_m as in Sec. II. ■

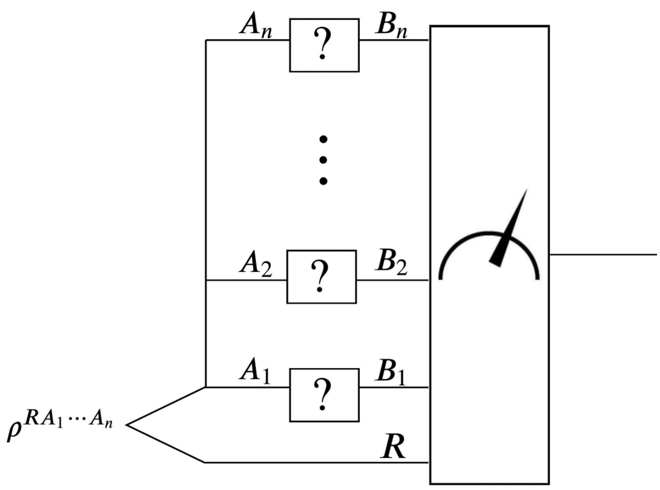

FIG. 3. The most general parallel strategy for discrimination of qq channels, from the class $\mathbb{P}_n$. An $(n+1)$-partite state ρ on $RA_1\dots A_n$ is prepared and each system A_i is fed into a separate channel input; the final measurement is performed with a two-outcome POVM on $RB_1\dots B_n$. If we do not allow input states to be entangled among different A systems or with the reference system R, the strategy falls into the class $\mathbb{P}_n^0$.

B. Restricting to classical feed forward and no quantum memory at the input: $\mathbb{A}_n^{c,0}$

In this setting, the protocol is similar to the adaptive protocol described in Sec, II, but extended to general quantum channels (see Fig. 4): after each transmission, the input state ρ_{x_m} is chosen adaptively from the classical feed forward. Denoting this adaptive choice of input states as $\vec{x}_m = (x_1,\dots,x_m)$, the mth input is chosen conditioned on the feed-forward information $\vec{k}_{m-1}$ and $\vec{x}_{m-1}$ from the conditional distribution $p_{X_m|\vec{X}_{m-1},\vec{K}_{m-1}}(x_m|\vec{x}_{m-1},\vec{k}_{m-1})$.

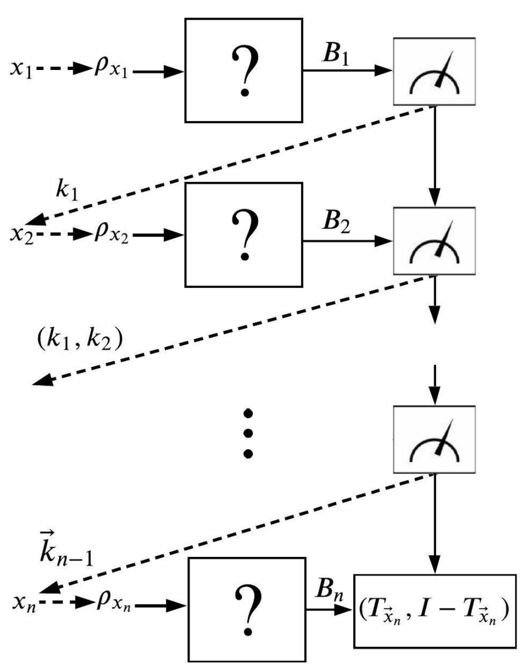

FIG. 4. Adaptive quantum channel discrimination with classical feed forward and without quantum memory at the channel input, from the class $\mathbb{A}_n^{c,0}$. Solid and dashed arrows denote the flow of quantum and classical information, respectively. At step m, Alice sends the state ρ_{x_m} which she has prepared using Bob's $m-1$ classical feed-forward information, and sends it via either $\mathcal{M}$ or $\overline{\mathcal{M}}$ to Bob.

Theorem 3. Let $\mathcal{M}$ and $\overline{\mathcal{M}}$ be qq channels. Then, for real numbers a, b satisfying $-D(\mathcal{M}\|\overline{\mathcal{M}}) \leqslant a-b \leqslant D(\overline{\mathcal{M}}\|\mathcal{M})$ and any $0 \leqslant r \leqslant D(\mathcal{M}\|\overline{\mathcal{M}})$, it holds

$$\begin{aligned} C^{\mathbb{A}^{c,0}}(a,b|\mathcal{M}\|\overline{\mathcal{M}}) &= C^{\mathbb{P}^0}(a,b|\mathcal{M}\|\overline{\mathcal{M}}) \\ &= \sup_{0\leqslant\alpha\leqslant 1} (1-\alpha)D_\alpha(\mathcal{M}\|\overline{\mathcal{M}}) \\ &\quad -\alpha a-(1-\alpha)b, \\ B_e^{\mathbb{A}^{c,0}}(r|\mathcal{M}\|\overline{\mathcal{M}}) &= B_e^{\mathbb{P}^0}(r|\mathcal{M}\|\overline{\mathcal{M}}) \\ &= \sup_{0\leqslant\alpha\leqslant 1} \frac{\alpha-1}{\alpha}\big[r-D_\alpha(\mathcal{M}\|\overline{\mathcal{M}})\big], \end{aligned}$$

where $D(\mathcal{M}\|\overline{\mathcal{M}})$ and $D_\alpha(\mathcal{M}\|\overline{\mathcal{M}})$ are defined in Eqs. (17) and (18).

Proof. Since only classical feed forward is allowed, one can cast this discrimination problem in the framework of the cq-channel discrimination problem treated in Sec. II. Namely, we apply Theorem 1 to the case when the cq channels have input alphabet $\mathcal{X} = \mathcal{S}^A$, i.e., it equals the set of all states on the input systems. In other words, we choose the classical (continuous) input alphabet as $\mathcal{X}$, where each letter $x \in \mathcal{X}$ is a classical description of a state ξ on the input system A. In this application, ρ_x and σ_x are given as $\mathcal{M}(\xi)$ and $\overline{\mathcal{M}}(\xi)$, respectively, for $x \equiv \xi$. Hence, $\sup_x D_\alpha(\rho_x\|\sigma_x)$ equals $D_\alpha(\mathcal{M}\|\overline{\mathcal{M}}) = \sup_\xi D_\alpha(\mathcal{M}(\xi)\|\overline{\mathcal{M}}(\xi))$. Hence, the desired relation is obtained. ■

Remark 2. The above theorem concludes that in the absence of entangled inputs, no adaptive strategy built upon classical feed forward can outperform the best nonadaptive strategy, which is in fact a tensor power input. In other words, the optimal error rate can be achieved by a simple independent and identically distributed input sequence where all n input states are chosen to be the same: $\rho^{\otimes n}$. ■

C. No advantage of adaptive strategies beyond $\mathbb{A}_n^{c,0}$?

One has to wonder whether it is really necessary to impose classical feed forward *and* to rule out quantum memory at the channel input to arrive at the conclusion of Theorem 3, that nonadaptive strategies with tensor product inputs $\mathbb{P}_n^0$ are already optimal. What can we say when only one of the restrictions holds? We start with defining the class $\mathbb{A}_n^c$ of adaptive strategies using classical feed forward.

Definition 2. The class $\mathbb{A}_n^c$ of adaptive strategies using classical feed forward is defined as a subset of $\mathbb{A}_n$ given in Definition 1, where now the maps $\mathcal{F}_m$ are subject to an additional structure. To describe it, one has to distinguish two operationally different quantum memories, the systems R_m of the sender, and systems C_m of the receiver. The initial state is $\rho_1^{R_1A_1}$, with trivial system $C_1 = 1$. Then, $\mathcal{F}_m$ maps $R_mB_mC_m$ to

$R_{m+1}A_{m+1}C_{m+1}$, in the following way:

$$\mathcal{F}_m = \sum_{\vec{k}_m} \mathcal{F}_{\vec{k}_m} \otimes \mathcal{P}_{\vec{k}_m}, \tag{19}$$

where $\{\mathcal{F}_{\vec{k}_m}\}_{\vec{k}_m}$ is an instrument of CP maps mapping B_mC_m to C_{m+1} (this is the measurement of the channel outputs up to the mth channel use generating the classical feed forward, together with the evolution of the receiver's memory), and where all the $\mathcal{P}_{\vec{k}_m}$ are quantum channels mapping R_m to $R_{m+1}A_{m+1}$, which serve to prepare the next channel input.

The class $\mathbb{A}_n^{c,0}$ is now easily identified as the subclass of strategies in $\mathbb{A}_n^c$ where $R_m = 1$ is trivial throughout the protocol. ■

Remark 3. Regarding adaptive strategies with quantum feed forward, but no quantum memory at the input, which class might be denoted $\mathbb{A}_n^0$: Note that the adaptive strategy considered in Sec. IV, Example 1, that is applied to a pair of entanglement-breaking channels and shown to be better than any nonadaptive strategies, while actually using quantum feed forward, required, however, no entangled inputs nor indeed quantum memory at the channel input. This shows that quantum feed forward alone can be responsible for an advantage over nonadaptive strategies. ■

Remark 4. Regarding adaptive strategies with classical feed forward, however, allowing quantum memory at the input, i.e., $\mathbb{A}_n^c$: It turns out that the channels considered in Sec. IV, Example 2, show that this class offers an advantage over nonadaptive strategies. This is because they are qc channels, i.e., their output is already classical, and so any general quantum feed-forward protocol can be reduced to an equivalent one with classical feed forward. It can be seen, however, that the perfect adaptive discrimination protocol described in [15] relies indeed on input entanglement. ■

VI. DISCRIMINATION POWER OF A QUANTUM CHANNEL

In this section we study how well a pair of quantum states can be distinguished after passing through a quantum channel. This quantifies the power of a quantum channel when it is seen as a measurement device. In some sense this scenario is dual to the state discrimination problem in which a pair of states are given and the optimization is taken over all measurements, while in the current scenario a quantum channel is given and the optimization takes place over all pairs of states passing through the channel. Reference [27] studies the special case of qc channels, that is, investigation of the power of a quantum detector given by a specific POVM in discriminating two quantum states. It was shown in the paper that when the qc channel is available asymptotically many times, neither entangled state inputs nor classical feedback and adaptive choice of inputs can improve the performance of the channel. We extend the model of the latter paper to general quantum channels, considering whether adaptive strategies provide an advantage for the discrimination power; see Fig. 5, where we consider classical feedback without quantum memory at the sender's side.

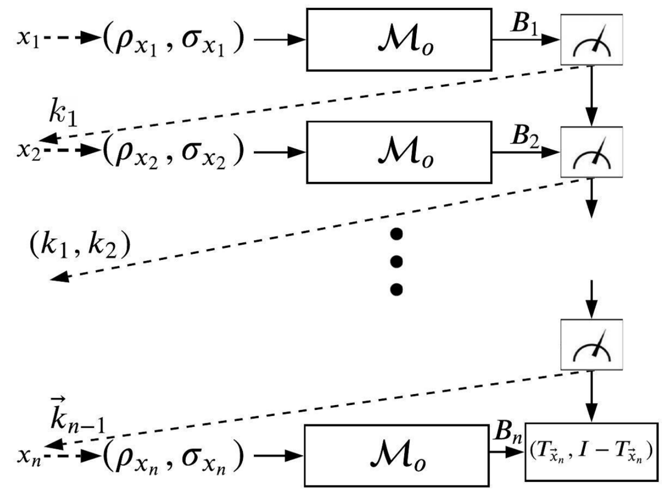

FIG. 5. Discrimination with a quantum channel $\mathcal{M}_o$. At step m, Alice prepares a state, either ρ_{x_m} or σ_{x_m}, which she has prepared using Bob's $m-1$ feedbacks (dashed arrows), and sends it via the channel $\mathcal{M}_o$ to Bob. Bob's measurements resemble the PVM's of Sec. II; they are used to extract classical information fed back to Alice and to prepare post-measurement states that he keeps for the next round of communication.

A. Simple extension of [27] with classical feedback: $\bar{\mathbb{A}}^{c,0}$

It is useful to cast this hypothesis testing setting as a communication problem as follows: Assume a quantum channel $\mathcal{M}_o = \mathcal{M}_o^{A_o\to B}$ connects Alice and Bob, where Alice possesses two systems $A_{o,0}, A_{o,1}$ and Bob has B. They did not know which system of $A_{o,0}, A_{o,1}$ works as the input system of the quantum channel $\mathcal{M}_o = \mathcal{M}_o^{A_o\to B}$. Hence, the hypothesis H_0 (H_1) refers to the case when the system $A_{o,0}$ ($A_{o,1}$) is the input system of the quantum channel $\mathcal{M}_o$ and the remaining system is simply traced out, i.e., is discarded. To identify which hypothesis is true, Alice and Bob make a collaboration. Alice chooses two input states ρ and σ on $A_{o,0}$ and $A_{o,1}$ for this aim. Bob receives the output state. They repeat this procedure n times. Bob obtains the n-fold tensor product system of B whose state is $\mathcal{M}_o(\rho)^{\otimes n}$ or $\mathcal{M}_o(\sigma)^{\otimes n}$. Applying two-outcome POVM $\{T_n, I-T_n\}$ on the n-fold tensor product system, Bob infers the variable Z by estimating which state is the true state. In this scenario, to optimize the discrimination power, Alice chooses the best two input states ρ and σ on $A_{o,0}$ and $A_{o,1}$ for this aim. We denote this class of Bob's strategies by $\bar{\mathbb{P}}^0$.

Now, similar to [27], we consider an adaptive strategy. To identify which hypothesis is true, Alice and Bob make a collaborating strategy, which allows Alice to use the channel n times and also allows Bob, who has access to quantum memory, to perform any measurement of his desire on its received systems and send back classical information to Alice; then Alice chooses a suitable pair of states ρ and σ on two systems $A_{o,0}$ and $A_{o,1}$ adaptively based on the feedback that she receives after each transmission. We denote this class of adaptive strategies by $\bar{\mathbb{A}}^{c,0}$.

The adaptive strategy in the class $\bar{\mathbb{A}}_n^{c,0}$ follows the cq-channel discrimination strategy: denoting the input generically as $x_1, \ldots, x_n$, the sequence of Bob's measurements is given as $\{\Pi^{(m)}_{\vec{k}_m|\vec{x}_m}\}_{m=1}^{n-1}$ and the classical feedback depends on the previous information $\vec{x}_m, \vec{k}_{m-1}$, and Alice's adaptive choice of the input states $(\rho_{x_1}, \sigma_{x_1}), \dots, (\rho_{x_n}, \sigma_{x_n})$ labeled by $(x_1, \dots, x_n)$ is given as the sequence of conditional randomized choice $\{p_{X_m|\vec{X}_{m-1},\vec{K}_{m-1}}\}_{m=1}^n$ of the pair of the input states (ρ, σ). In this formulation, after obtaining the measurement outcome K_m, using a two-outcome POVM $\{T_n, I - T_n\}$ on the n-fold tensor product system, Bob decides which hypothesis of H_0 and H_1 is true according to the conditional distributions $\{p_{X_m|\vec{X}_{m-1},\vec{K}_{m-1}}\}_{m=1}^n$.

In this class, we denote the generalized Chernoff and Hoeffding quantities as $C^{\bar{\mathbb{A}}^{c,0}}(a, b|\mathcal{M}_o)$ and $B_e^{\bar{\mathbb{A}}^{c,0}}(r|\mathcal{M}_o)$, respectively. When no feedback is allowed and the input state deterministically is fixed to a single form (ρ, σ), we denote the generalized Chernoff and Hoeffding quantities as $C^{\bar{\mathbb{P}}^0}(a, b|\mathcal{M}_o)$ and $B_e^{\bar{\mathbb{P}}^0}(r|\mathcal{M}_o)$, respectively.

We set

$$\begin{aligned} D(\mathcal{M}_o) : &= \max_{\rho,\sigma} D(\mathcal{M}_o(\rho)\|\mathcal{M}_o(\sigma)) \\ &= \max_{\rho,\sigma} D(\mathcal{M}_o(\sigma)\|\mathcal{M}_o(\rho)). \end{aligned} \tag{20}$$

Theorem 4. Let $0 \leqslant r \leqslant D(\mathcal{M}_o)$ and real numbers a and b satisfy $-D(\mathcal{M}_o) \leqslant a - b \leqslant D(\mathcal{M}_o)$, then we have

$$\begin{aligned} &C^{\bar{\mathbb{A}}^{c,0}}(a, b|\mathcal{M}_o) = C^{\bar{\mathbb{P}}^0}(a, b|\mathcal{M}_o) \\ &= \sup_{\rho,\sigma} \sup_{0\leqslant\alpha\leqslant 1} (1-\alpha)D_\alpha(\mathcal{M}(\rho)\|\mathcal{M}_o(\sigma)) - \alpha a - (1-\alpha)b, \\ &B_e^{\bar{\mathbb{A}}^{c,0}}(r|\mathcal{M}_o) = B_e^{\bar{\mathbb{P}}^0}(r|\mathcal{M}_o) \\ &= \sup_{\rho,\sigma} \sup_{0\leqslant\alpha\leqslant 1} \frac{\alpha-1}{\alpha}[r - D_\alpha(\mathcal{M}_o(\rho)\|\mathcal{M}_o(\sigma))]. \end{aligned}$$

Proof. Here we only need to consider the set $\mathcal{S}^{A_o} \times \mathcal{S}^{A_o'}$ of pairs of input states as the set $\mathcal{X}$. In other words, we choose the classical (continuous) input alphabet as $\mathcal{X} = \mathcal{S}^{A_o} \times \mathcal{S}^{A_o'}$, where each letter $x \equiv (\rho, \sigma) \in \mathcal{X}$ is a classical description of the pair of states (ρ, σ). Then, the result follows from the adaptive protocol in Sec. II. (Compare also the proof of Theorem 3.) ■

Remark 5. As another scenario, [27] also considers the case when the input states are given as ρ_n, σ_n where ρ_n and σ_n are states on the n-fold systems $A_{o,0}^{\otimes n}$ and $A_{o,1}^{\otimes n}$, respectively. It shows that this strategy can be reduced to the adaptive strategy presented in this subsection when the channel $\mathcal{M}_o$ is a qc channel, i.e., it has the form

$$\mathcal{M}_o(\rho) = \sum_{x\in\mathcal{X}} (\mathrm{Tr}\rho M_x)|x\rangle\langle x|, \tag{21}$$

where $\{|x\rangle\}_{x\in\mathcal{X}}$ forms an orthogonal system. However, it is not so easy to show the above reduction when the channel $\mathcal{M}_o$ is a general qq channel. When the channel $\mathcal{M}_o$ is a cq channel in the sense of (15), the next subsection shows that the above type of general strategy cannot improve the performance.

B. Quantum feedback: $\mathbb{A}_n$

Next, we discuss the most general class, in which Bob makes quantum feedback to Alice. To discuss this case, we generalize the above formulated problem by allowing more general inputs because the formulation in the above section allows only a pair of states $(\rho, \sigma) \in \mathcal{S}^{A_{o,0}} \times \mathcal{S}^{A_{o,1}}$. In the generalized setting, the hypothesis H_i is that the true channel is $\rho \mapsto \mathcal{M}_o(\mathrm{Tr}_{i\oplus 1}\rho)$. Then, Alice and Bob collaborate in order to identify which hypothesis is true. That is, it is formulated as the discrimination between two qq channels $\mathcal{M}$ and $\overline{\mathcal{M}}$, mapping $A = A_{o,0}A_{o,1}$ to B defined as

$$\mathcal{M}(\rho) := \mathcal{M}_o(\mathrm{Tr}_1\rho) = \mathrm{Tr}_1(\mathcal{M}_o \otimes \mathcal{M}_o)(\rho), \tag{22}$$

$$\overline{\mathcal{M}}(\rho) := \mathcal{M}_o(\mathrm{Tr}_0\rho) = \mathrm{Tr}_0(\mathcal{M}_o \otimes \mathcal{M}_o)(\rho), \tag{23}$$

for $\rho \in \mathcal{S}^{A_{o,0}A_{o,1}}$. For this discrimination, Alice has the input quantum composite system $A_{o,0}A_{o,1}$ and her own quantum memory. She makes the input state on this system by using the quantum feedback and her own quantum memory. In each step, Bob makes measurement, and sends back a part of the resultant quantum system to Alice while the remaining part is kept in his local quantum memory. Therefore, this general strategy contains the strategy presented in Remark 5.

Then, the problem can be regarded as a special case of discriminating the two qq channels given in Sec. V. That is, Bob's operation is given as the strategy of discriminating the two qq channels. In the most general class, we denote the generalized Chernoff and Hoeffding quantities as $C^{\mathbb{A}}(a, b|\mathcal{M}_o)$ and $B_e^{\mathbb{A}}(r|\mathcal{M}_o)$, respectively. When no feedback nor no quantum memory of Alice side is allowed, we denote the generalized Chernoff and Hoeffding quantities as $C^{\mathbb{P}^0}(a, b|\mathcal{M}_o)$ and $B_e^{\mathbb{P}^0}(r|\mathcal{M}_o)$, respectively. As a corollary of Theorems 2 and 4, we have the following corollary.

Corollary 1. Assume that the qq channel $\mathcal{M}_o$ has the form

$$\mathcal{M}_o(\rho) = \sum_x \rho_x \mathrm{Tr} E_x \rho, \tag{24}$$

where $\{E_x\}_{x\in\mathcal{X}}$ is a PVM and the rank of E_x is one. For $0 \leqslant r \leqslant D(\mathcal{M}_o)$ [see Eq. (20)] and real a and b with $-D(\mathcal{M}_o) \leqslant a - b \leqslant D(\mathcal{M}_o)$, the following holds:

$$C^{\mathbb{A}}(a, b|\mathcal{M}_o) = C^{\mathbb{P}^0}(a, b|\mathcal{M}_o) = C^{\bar{\mathbb{P}}^0}(a, b|\mathcal{M}_o), \tag{25}$$

$$B_e^{\mathbb{A}}(r|\mathcal{M}_o) = B_e^{\mathbb{P}^0}(r|\mathcal{M}_o) = B_e^{\bar{\mathbb{P}}^0}(r|\mathcal{M}_o). \tag{26}$$

■

This corollary shows that the above extension of our strategy does not improve the generalized Chernoff and Hoeffding quantities under the condition (24).

Proof. Theorem 2 implies the first equations in (25) and (26) under the condition (24). When the condition (24) holds, any input state on $A = A_{o,0}A_{o,1}$ can be simulated on a separable input state on $A = A_{o,0}A_{o,1}$. Such a separable input state can be considered as a probabilistic input with the form $(\rho, \sigma) \in \mathcal{S}^{A_{o,0}} \times \mathcal{S}^{A_{o,1}}$. The strategy $\bar{\mathbb{A}}^{c,0}$ in the problem setting of Sec. VI A contains such probabilistic input. Hence, Theorem 4 implies the second equations in the first equations in (25) and (26). ■

Remark 6. The above result states that the optimal error rates for discrimination with a quantum channel can be achieved by independent and identically distributed state pairs $(\rho^{\otimes n}, \sigma^{\otimes n})$, among all strategies without quantum memory at the sender's side. On the other hand, when entangled state inputs are allowed, we could only show the optimality of nonadaptive tensor-product strategy $\mathbb{P}_n^0$ for entanglement-breaking channel of the form (24). The same conclusion holds for the Chernoff bound and Stein's lemma. ■

C. Examples

In this section we derive the generalized Chernoff and Hoeffding bounds for three qubit channels, namely, we study the discrimination power of depolarizing, Pauli, and amplitude damping channels. In each case, the key is identifying the structure of the output states of each channel by employing the lessons learned in [45]. Here we briefly summarize the basics. A quantum state ρ in two-level systems can be parametrized as $\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma})$, where $\vec{r} = (r_x, r_y, r_z) \in \mathbb{R}^3$ is the Bloch vector which satisfies $r_x^2 + r_y^2 + r_z^2 \leqslant 1$ and $\vec{\sigma}$ denotes the vector of Pauli matrices $\{\sigma_x, \sigma_y, \sigma_z\}$ such that $\vec{r}\cdot\vec{\sigma} := r_x\sigma_x + r_y\sigma_y + r_z\sigma_z$. Any CPTP map $\mathcal{M}_o$ on qubits can be represented as follows:

$$\mathcal{M}_o\left(\frac{1}{2}(I + \vec{r}\cdot\vec{\sigma})\right) = \frac{1}{2}[I + (\vec{t} + T\vec{r})\cdot\vec{\sigma}],$$

where $\vec{t}$ is a vector and T is a real 3×3 matrix. For each channel, we first need to identify these parameters. The following lemma comes in handy in simplifying the optimization problem.

Lemma 2 (Cf. [46, Theorem 3.10.11]). A continuous convex function f on a compact convex set attains its global maximum at an extreme point of its domain. ■

Lemma 3. For any quantum channel $\mathcal{M}_o$ we have

$$\begin{aligned}&\sup_{\rho,\sigma} D_\alpha(\mathcal{M}_o(\rho)\|\mathcal{M}_o(\sigma))\\ &= \sup_{|\psi\rangle,|\phi\rangle} D_\alpha(\mathcal{M}_o(|\psi\rangle\langle\psi|)\|\mathcal{M}_o(|\phi\rangle\langle\phi|)),\end{aligned}$$

that is, pure states are sufficient for the maximization of the Rényi divergence with channel $\mathcal{M}_o$.

Proof. This is a consequence of Lemma 2. Note that the space of quantum states is a convex set; on the other hand, the Rényi divergence is a convex function, and we actually need convexity separately in each argument. Therefore, the optimal states are extreme points of the set, i.e., pure states. ■

Remark 7. Since we will focus on two-level systems, we should recall that a special property of the convex set of qubits which is not shared by n-level systems with $n \geqslant 3$ is that every boundary point of the set is an extreme point. Since the states on the surface of the Bloch sphere are mapped onto the states on the surface of the ellipsoid, the global maximum will be achieved by a pair of states on the surface of the output ellipsoid. ■

Remark 8. In the following we will use symmetric properties of the states in the Bloch sphere to calculate the Rényi divergence. Note that the Rényi divergence of two qubit states is not just a function of their Bloch sphere distance. For instance, for two states ρ_1 and σ_1 with Bloch vectors $\vec{r}_1 = (0, 0, \frac{1}{4})$ and $\vec{s}_1 = (0, 0, -\frac{1}{4})$, respectively, we can see that $\|\rho_1 - \sigma_1\|_1 = \|\vec{r}_1 - \vec{s}_1\|_2 = \frac{1}{2}$ and the divergence equals 0.17 ($\alpha \to 1$). On the other hand, for states ρ_2 and σ_2 with Bloch vectors $\vec{r}_2 = (0, 0, 1)$ and $\vec{s}_2 = (1, 0, 0)$, respectively, we can see that $\|\rho_2 - \sigma_2\|_1 = \|\vec{r}_2 - \vec{s}_2\|_2 = \sqrt{2}$ and the divergence equals 0 ($\alpha \to 1$). However, we will see that for states with certain symmetric properties, the Rényi divergence increases with the distance between two arguments. ■

Example 3 (Depolarizing channel). For $0 \leqslant q \leqslant 1$, the depolarizing channel is defined as follows:

$$\mathcal{D}_q : \rho \mapsto (1-q)\rho + q\frac{I}{2},$$

that is, the depolarizing channel transmits the state with probability $(1-q)$ or replaces it with the maximally mixed state with probability q. In both generalized Chernoff and Hoeffding exponents, we should be dealing with two optimizations, one over (ρ, σ) and the other over $0 \leqslant \alpha \leqslant 1$. We can take the supremum over the state pair inside each expression and deal with α next. Hence, we start with the supremum of the Rényi divergence employing Lemma 3.

For the depolarizing channel, it can be easily seen that

$$\vec{t} = \begin{pmatrix}0\\0\\0\end{pmatrix} \quad\text{and}\quad T = \begin{pmatrix}1-q & 0 & 0\\ 0 & 1-q & 0\\ 0 & 0 & 1-q\end{pmatrix}.$$

Therefore, the set of output states consists of a sphere of radius $1-q$ centered at the origin, i.e., $r_x^2 + r_y^2 + r_z^2 = (1-q)^2$. Note that we only consider the states on the surface of the output sphere. Because of the symmetry of the problem and the fact that divergence is larger on orthogonal states, we can choose any two states at the opposite sides of a diameter. Here for simplicity we choose the states corresponding to $\vec{r}_1 = (0, 0, 1-q)$ and $\vec{r}_2 = (0, 0, -1+q)$ leading to the following states, respectively:

$$\rho' = \left(1 - \frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}|1\rangle\langle 1|, \tag{27}$$

$$\sigma' = \frac{q}{2}|0\rangle\langle 0| + \left(1 - \frac{q}{2}\right)|1\rangle\langle 1|. \tag{28}$$

Then it can be easily seen that

$$\sup_{\rho,\sigma} D_\alpha(\mathcal{M}_o(\rho)\|\mathcal{M}_o(\sigma)) = \frac{1}{\alpha-1}\log_2 Q(q,\alpha), \tag{29}$$

where $Q(q,\alpha) = (1-\frac{q}{2})^\alpha(\frac{q}{2})^{1-\alpha} + (1-\frac{q}{2})^{1-\alpha}(\frac{q}{2})^\alpha$. By plugging back into the respective equations, we have for $0 \leqslant r \leqslant -(1-q)\log_2\frac{q}{2-q}$ and $(1-q)\log_2\frac{q}{2-q} \leqslant a - b \leqslant -(1-q)\log_2\frac{q}{2-q}$,

$$C^{\mathbb{A}^{c,0}}(a, b|\mathcal{M}_o) = \sup_{0\leqslant\alpha\leqslant 1} -\log_2 Q(q,\alpha) - \alpha a - (1-\alpha)b,$$

$$B_e^{\mathbb{A}^{c,0}}(r|\mathcal{M}_o) = \sup_{0\leqslant\alpha\leqslant 1} \frac{\alpha-1}{\alpha}\left(r - \frac{1}{\alpha-1}\log_2 Q(q,\alpha)\right).$$

The function $Q(q,\alpha)$ introduced above is important and will also appear in later examples; we have

$$\begin{aligned}\frac{\partial Q(q,\alpha)}{\partial\alpha} &= \left(\ln\frac{q}{2-q}\right)\left[\left(\frac{q}{2}\right)^\alpha\left(1-\frac{q}{2}\right)^{1-\alpha}\right.\\ &\quad \left.-\left(\frac{q}{2}\right)^{1-\alpha}\left(1-\frac{q}{2}\right)^\alpha\right],\\ \frac{\partial^2 Q(q,\alpha)}{\partial\alpha^2} &= \left(\ln\frac{q}{2-q}\right)^2 Q(q,\alpha),\end{aligned}$$

where $\frac{\partial}{\partial\alpha}$ and $\frac{\partial^2}{\partial\alpha^2}$ denote the first- and second-order partial derivatives with respect to the variable α. It can also be easily checked that $\log_2\frac{q}{2-q} \leqslant 0$, $0 \leqslant Q(q,\alpha) \leqslant 1$.

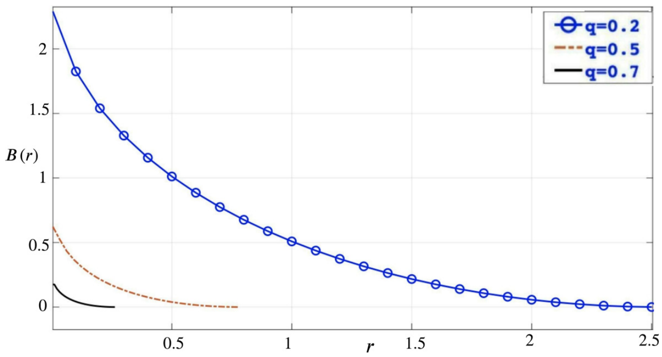

FIG. 6. Hoeffding bound for depolarizing channel when entangled inputs are not allowed. [The vertical axis shows $B_e^{\mathbb{A}_n^{c,0}}(r|\mathcal{M}_o)$, represented as $B(r)$.] The legitimate values of r for each exponent are imposed by strong Stein's lemma and differ with q as $r = (q-1)\log_2 \frac{q}{2-q}$.

Let $\overline{C}(\alpha)$ denote the expression inside the supremum in $C^{\mathbb{A}^{c,0}}(a, b|\mathcal{M}_o)$. For the generalized Chernoff bound, from the observations above and some algebra, it can be seen that

$$\frac{\partial \overline{C}(\alpha)}{\partial \alpha} = 0 \Rightarrow \alpha = \frac{1}{2} - \frac{\log_2 \frac{\log_2 \frac{q}{2-q} + (a-b)}{\log_2 \frac{q}{2-q} - (a-b)}}{2 \log_2 \frac{q}{2-q}}. \tag{30}$$

On the other hand, it can be checked that $\frac{\partial^2 \overline{C}(\alpha)}{\partial \alpha^2} \geqslant 0$, making sure that the generalized Chernoff bound is a convex function and also that the above zero is unique. Note that the generalized Chernoff bound is not a monotonic function since $\frac{\partial \overline{C}(\alpha)}{\partial \alpha}$ obviously changes sign, hence, the zero is not necessarily at the ends of the interval.

For the Hoeffding exponent $B_e^{\mathbb{A}^{c,0}}(r|\mathcal{M}_o)$, finding a compact formula for the global maximum is not possible. However, numerical simulation guarantees that $B_e^{\mathbb{A}^{c,0}}(r|\mathcal{M}_o)$ is a convex function that the first derivative has a unique zero. We solved the optimization numerically for depolarizing channel with three different parameters (see Fig. 6). ■

Example 4 (Pauli channel). Let $\vec{p} = (p_I, p_x, p_y, p_z)$ be a probability vector. The Pauli channel is defined as follows:

$$\mathcal{P}_{\vec{p}} : \rho \mapsto p_I \rho + \sum_{i=x,y,z} p_i \sigma_i \rho \sigma_i^{\dagger},$$

that is, it returns the state with probability p_I or applies the Pauli operators $\sigma_x, \sigma_y, \sigma_z$ with probabilities p_x, p_y, p_z, respectively.

For this channel, it can be seen by some algebra that (see, e.g., [9, Sec. 5.3] and [47])

$$\vec{t} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} p_I + p_x - p_y - p_z & 0 & 0 \\ 0 & p_I - p_x + p_y - p_z & 0 \\ 0 & 0 & p_I - p_x - p_y + p_z \end{pmatrix}. \tag{31}$$

Therefore, the states on the surface of the Bloch sphere are mapped into the surface of the following ellipsoid:

$$\left(\frac{r_x}{p_I + p_X - p_Y - p_z}\right)^2 + \left(\frac{r_y}{p_I - p_X + p_Y - p_z}\right)^2 + \left(\frac{r_z}{p_I - p_X - p_Y + p_z}\right)^2 = 1. \tag{32}$$

Note that the Pauli channel shrinks the unit sphere with different magnitudes along each axis, and the two states on the surface of the ellipsoid that have the largest distance depend on the lengths of the coordinates on each axis. We need to choose the states along the axis that is shrunk the least. We define the following:

$$p_{\max} = \max\{|p_I + p_X - p_Y - p_Z|, |p_I - p_X + p_Y - p_Z|, |p_I - p_X - p_Y + p_Z|\}, \tag{33}$$

then from the symmetry of the problem and the fact that the eigenvalues of the state $\vec{r} = (r_x, r_y, r_z)$ are $\{\frac{1-|\vec{r}|}{2}, \frac{1+|\vec{r}|}{2}\}$, the following can be seen after some algebra:

$$\sup_{\rho,\sigma} D_\alpha(\mathcal{M}_o(\rho)\|\mathcal{M}_o(\sigma)) = \frac{1}{\alpha - 1} \log_2 Q(1 - p_{\max}, \alpha). \tag{34}$$

From this, for $0 \leqslant r \leqslant -p_{\max} \log_2 \frac{1-p_{\max}}{1+p_{\max}}$ and $p_{\max} \log_2 \frac{1-p_{\max}}{1+p_{\max}} \leqslant a - b \leqslant -p_{\max} \log_2 \frac{1-p_{\max}}{1+p_{\max}}$, we have

$$C^{\mathbb{A}^{c,0}}(a, b|\mathcal{M}) = \sup_{0 \leqslant \alpha \leqslant 1} -\log_2 Q(1 - p_{\max}, \alpha) - \alpha a - (1-\alpha) b,$$

$$B_e^{\mathbb{A}^{c,0}}(r|\mathcal{M}) = \sup_{0 \leqslant \alpha \leqslant 1} \frac{\alpha - 1}{\alpha}\left(r - \frac{1}{\alpha - 1} \log_2 Q(1 - p_{\max}, \alpha)\right).$$

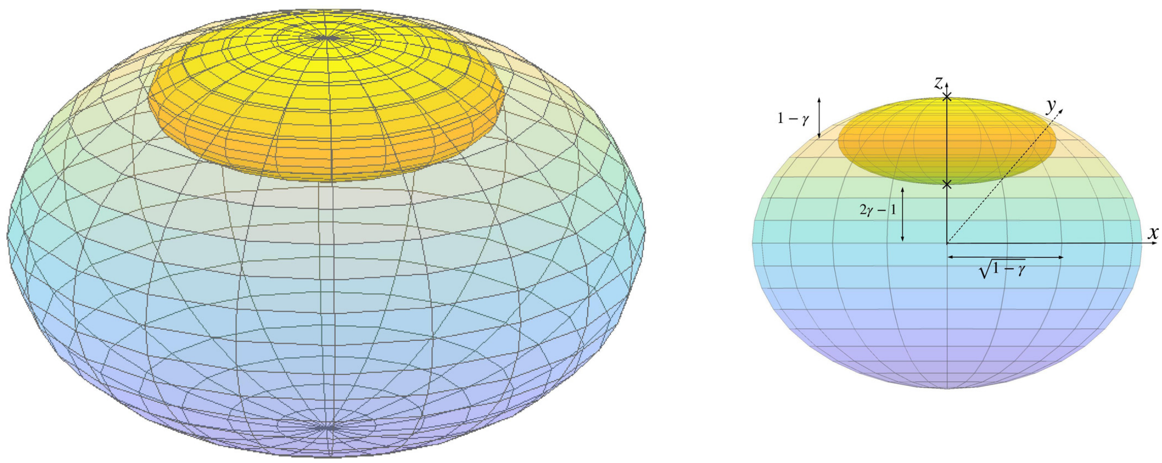

FIG. 7. The Bloch sphere and its image under the amplitude damping channel with parameter γ. There are two large and one small principal axes. As indicated in the right-hand figure, the points (0,0,1) and $(0,0,2\gamma-1)$ are the intersection points of the surface of the displaced ellipsoid with the z axis; the former point also is its intersection point with the Bloch sphere.

Similar to our findings in Example 3, we can show that the generalized Hoeffding bound is maximized at

$$\alpha=\frac{1}{2}-\frac{\log_2\frac{\log_2\frac{1-p_{\max}}{1+p_{\max}}+(a-b)}{\log_2\frac{1-p_{\max}}{1+p_{\max}}-(a-b)}}{2\log_2\frac{1-p_{\max}}{1+p_{\max}}},$$

and this point is unique. The same conclusion using numerical optimization indicates that the Hoeffding bound of the Pauli channel resembles that of the depolarizing channel. Note that a depolarizing channel with parameter q is equivalent to a Pauli channel with parameters $\{p_I=1-\frac{3q}{4}, p_x=\frac{q}{4}, p_y=\frac{q}{4}, p_z=\frac{q}{4}\}$ [9, Example 5.3]. ■

Example 5 (Amplitude damping channel). The amplitude damping channel with parameter $0\leqslant\gamma\leqslant 1$ is defined as follows:

$$\mathcal{A}_\gamma:\rho\mapsto A_0\rho A_0^\dagger+A_1\rho A_1^\dagger, \tag{35}$$

where the Kraus operators are given as $A_0=\sqrt{\gamma}|0\rangle\langle 1|$ and $A_1=|0\rangle\langle 0|+\sqrt{1-\gamma}|1\rangle\langle 1|$.

For this channel, simple algebra shows that

$$\vec{t}=\begin{pmatrix}0\\0\\\gamma\end{pmatrix}\quad\text{and}\quad T=\begin{pmatrix}\sqrt{1-\gamma}&0&0\\0&\sqrt{1-\gamma}&0\\0&0&1-\gamma\end{pmatrix}. \tag{36}$$

Note that unlike depolarizing and Pauli channels, $\vec{t}$ has a nonzero element for the amplitude damping channel, meaning that the amplitude damping channel is not unital. The nonzero $\vec{t}$ indicates shifting the center of the ellipsoid. The ellipsoid of output states of the amplitude damping channel is depicted in Fig. 7 . Some algebra reveals the equation of the image to be as follows:

$$\left(\frac{r_x}{\sqrt{1-\gamma}}\right)^2+\left(\frac{r_y}{\sqrt{1-\gamma}}\right)^2+\left(\frac{r_z-\gamma}{1-\gamma}\right)^2=1. \tag{37}$$

To calculate the divergence, from the argument we made in Remark 8, we choose the optimal states on x-z plane as $\vec{r}_1=(\sqrt{1-\gamma},0,\gamma)$ and $\vec{r}_2=(-\sqrt{1-\gamma},0,\gamma)$. It can be numerically checked that these points lead to maximum divergence. These two points correspond to the following states, respectively:

$$\rho_1=\frac{1}{2}\begin{pmatrix}1+\gamma&\sqrt{1-\gamma}\\\sqrt{1-\gamma}&1-\gamma\end{pmatrix}\quad\text{and}$$
$$\rho_2=\frac{1}{2}\begin{pmatrix}1+\gamma&-\sqrt{1-\gamma}\\-\sqrt{1-\gamma}&1-\gamma\end{pmatrix}.$$

Since $|\vec{r}_1|=|\vec{r}_2|=\sqrt{\gamma^2-\gamma+1}$, both states have the following eigenvalues:

$$\lambda_1,\lambda_2=\frac{1\pm\sqrt{\gamma^2-\gamma+1}}{2},$$

and since ρ_1 and ρ_2 obviously do not commute, we find the eigenvectors for ρ_1 and ρ_2, respectively, as follows:

$$|\nu_1\rangle=\frac{1}{\sqrt{1+\left(\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\right)^2}}\begin{pmatrix}1\\\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\end{pmatrix},$$
$$|\nu_2\rangle=\frac{1}{\sqrt{1+\left(\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\right)^2}}\begin{pmatrix}1\\\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\end{pmatrix},$$

and

$$|\mu_1\rangle=\frac{1}{\sqrt{1+\left(\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\right)^2}}\begin{pmatrix}1\\-\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\end{pmatrix},$$
$$|\mu_2\rangle=\frac{1}{\sqrt{1+\left(\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\right)^2}}\begin{pmatrix}1\\-\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\end{pmatrix}.$$

The following can be seen after some algebra:

$$\sup_{\rho,\sigma}D_\alpha(\mathcal{M}_o(\rho)\|\mathcal{M}_o(\sigma))=\frac{1}{\alpha-1}\log_2 W(\gamma,\alpha),$$

where

$$W(\gamma,\alpha)=\lambda_1\left(\frac{1-\left(\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\right)^2}{1+\left(\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\right)^2}\right)^2+\lambda_2\left(\frac{1-\left(\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\right)^2}{1+\left(\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\right)^2}\right)^2+\frac{\left(Q(1-\sqrt{\gamma^2-\gamma+1},\alpha)\right)\left(1-\frac{(2\lambda_1-1-\gamma)(2\lambda_2-1-\gamma)}{(\sqrt{1-\gamma})^2}\right)^2}{\left[1+\left(\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\right)^2\right]\left[1+\left(\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\right)^2\right]}.$$

We also have

$$D(\mathcal{M})=\lambda_1\log_2\lambda_1+\lambda_2\log_2\lambda_2-\lambda_1\log_2\lambda_1\left(\frac{1-\left(\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\right)^2}{1+\left(\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\right)^2}\right)^2-\lambda_2\log_2\lambda_2\left(\frac{1-\left(\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\right)^2}{1+\left(\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\right)^2}\right)^2$$
$$-\frac{(\lambda_1\log_2\lambda_2+\lambda_2\log_2\lambda_1)\left(1-\frac{(2\lambda_1-1-\gamma)(2\lambda_2-1-\gamma)}{1-\gamma}\right)^2}{\left[1+\left(\frac{2\lambda_1-1-\gamma}{\sqrt{1-\gamma}}\right)^2\right]\left[1+\left(\frac{2\lambda_2-1-\gamma}{\sqrt{1-\gamma}}\right)^2\right]}.$$

The cumbersome expressions reflect the complexity of analytically solving the optimizations; however, it can be seen numerically that the first derivative of the generalized Chernoff bound has a unique zero and its second derivative is positive ensuring the convexity. We calculate and plot the Hoeffding exponent for three different parameters of the amplitude damping channel in Fig. 8. ■

VII. CONCLUSION

In an attempt to further extend the classical results of [16] to quantum channels, we have shown that for the discrimination of a pair of cq channels, adaptive strategies cannot offer any advantage over nonadaptive strategies concerning the asymmetric Hoeffding and the symmetric Chernoff problems in the asymptotic limit of error exponents, even when the input system is continuous. Our approach is to turn the cq channels into classical channels using eigenvalue decomposition of the output states by using the two distributions introduced by [8,29], and subsequently deal with the classical channels. This latter finding led us to prove the optimality of nonadaptive strategies for discriminating qq channels via a subclass of protocols which only use classical feed-forward and product inputs.

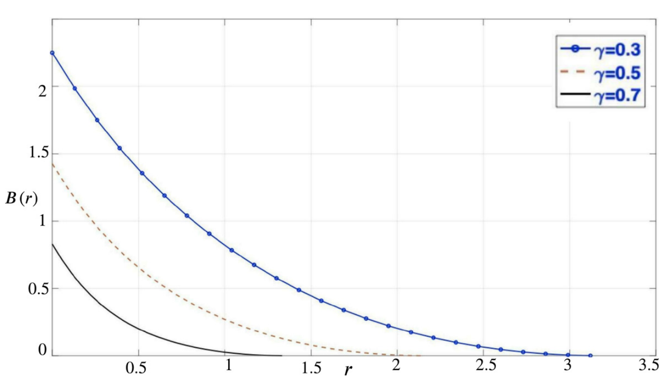

FIG. 8. Hoeffding exponent for amplitude damping channel when entangled inputs are not allowed. [The vertical axis shows $B_e^{A_n^{c,0}}(r|\mathcal{M}_o)$, represented as $B(r)$.] The legitimate values of r for each exponent are imposed by the strong Stein's lemma and differ as a function of γ, i.e., $D(\mathcal{M})$.

In contrast, the most general strategy for discriminating qq channels allows quantum feed-forward and entangled inputs. In this class, we have obtained two results for a pair of two entanglement-breaking channels. When these two entanglement-breaking channels are constructed via the same PVM, the most general strategy cannot improve the parallel scheme concerning the asymmetric Hoeffding and the symmetric Chernoff problems. In contrast, in an example of a pair of entanglement-breaking channels that are constructed via different PVMs, and in another example of a pair of qc channels implementing general POVMs, we have shown asymptotic separations between the Chernoff and Hoeffding exponents of adaptive and nonadaptive strategies. These examples show the importance of the above condition for two entanglement-breaking channels. For general pairs of qq channels, we leave open the question of the condition for the optimality of nonadaptive protocols; note that it is open already for entanglement-breaking channels.

We have also studied the hypothesis testing of binary information via a noisy quantum channel and have shown that when no entangled inputs nor quantum feedback are allowed, nonadaptive strategies are optimal. In addition, when the channel is an entanglement-breaking channel composed of a PVM followed by a state preparation, we have shown the optimality of nonadaptive strategies without the need for entangled inputs among all adaptive strategies.

Both our work and quantum machine-learning (ML) model in [1] aim at learning about quantum channels. Reference [1] considers a finite number of uses of a quantum channel and establishes quantum advantage in the sense that classical learning process is exponential while quantum learning process is polynomial in the number of queries to the quantum channel. These results are conceptually in line with results in [14,21,22] where the number of channel uses leading to perfect identification is relevant. In fact, one particularly interesting research topic would be to find particular quantum channels such that the quantum ML model strictly outperforms classical ML models in the setting of [1]. We feel that such channels might be found by looking into our Examples 1 and 2. On the other hand, in the context of quantum ML models, our results establish when and what kind of quantum technology is required to benefit from quantum ML. In particular, our results in Sec. VI are related to the setting of

[1] in that in both problems there is one single channel inside a black box, and the question is how well one can predict (or learn about or distinguish between) the outputs of the channel. While we study the asymptotic advantage, we expect that our results can be applied to the scenarios where the scaling of the prediction accuracy with respect to the sample complexity becomes important. An example of such scaling relevant to our work is presented in [1]. More precisely, the so-called scaling property of our results stems from two points: First, we have shown that, for certain channels, adaptive strategies cannot beat nonadaptive ones. We have done so by proving that the Rényi relative entropy in the adaptive setting can be reduced to the Rényi relative entropy in the nonadaptive setting. This analysis has been applied to the discrimination of qq entanglement-breaking channels where the measurement bases are the same, and without considering asymptotic limits. The relation between the Rényi relative entropy and the discrimination task holds no matter which type of scaling is considered. Therefore, this reduction is expected to play an important role even in the scaling of [1]. Second, we have derived a lower bound for discrimination error for general nonadaptive strategies. Since this bound can be applied to any pair of qq channels, it led us to the first examples of asymptotic separation between adaptive and nonadaptive strategies. On the other hand, as this lower bound comes from the minimum eigenvalue of a certain operator, it applies in the nonasymptotic regime, in particular in the scaling of [1] as well.

An obvious extension of our work would be to restrict the number of samples (channel uses) to be a random variable rather than a fixed number (see Li *et al.* [48]). Besides, Ref. [1] studies prediction of classical bits even when quantum ML is employed. Since our obtained bounds work in the scaling of [1], an extension of our results should go beyond the classical data prediction of [1].

ACKNOWLEDGMENTS

The authors thank Z. Puchała for drawing our attention to Example 2, from Ref. [15], and Z. Puchała and S. Pirandola for pointing out various pertinent previous works. F.S. is grateful to M. Berta for stimulating discussions during QIP 2020. He also acknowledges the hospitality and support of the Peng Cheng Laboratory (PCL) where the initial part of this work was done. A.W. thanks E. White and D. Colt for spirited conversations on issues around discrimination and inequalities. F.S. acknowledges support by the DFG cluster of excellence 2111 (Munich Center for Quantum Science and Technology). F.S. and A.W. acknowledge partial financial support by the Baidu-UAB collaborative project Learning of Quantum Hidden Markov Models, the Spanish MINECO (Projects No. FIS2016-86681-P and No. PID2019-107609GB-I00/AEI/10.13039/501100011033) with the support of FEDER funds, and the Generalitat de Catalunya (Project No. 2017-SGR-1127). F.S. is also supported by the Catalan Government 001-P-001644 QuantumCAT within the ERDF Program of Catalunya. M.H. is supported in part by Guangdong Provincial Key Laboratory (Grant No. 2019B121203002), a JSPS Grant-in-Aids for Scientific Research (A) No. 17H01280 and for Scientific Research (B) No. 16KT0017, and Kayamori Foundation of Information Science Advancement.

APPENDIX A: QUANTUM MEASUREMENTS

The aim of the Appendixes is showing Theorem 1, which discusses the generalized Chernoff bound and Hoeffding bound for cq-channel discrimination. The Appendixes are organized as follows: We first introduce quantum instruments and provide useful lemmas needed for the rest of this Appendix. Our adaptive method is proven in Appendix B, and subsequently Appendix C proves several auxiliary lemmas leading to the main result of this section, which is presented in Appendix D.

Since we need to handle CP-map valued measure, we prepare the following lemma.

Lemma 4 (Cf. [9, Theorem 7.2]). Let $\boldsymbol{\kappa} = \{\kappa_\omega : A \to B\}_\omega$ be an instrument (i.e., a CP-map valued measure) with an input system A and an output system B. Then there exist a POVM $\boldsymbol{M} = \{M_\omega\}$ on a Hilbert space A and CPTP maps κ'_ω from A to B for each outcome ω, such that for any density operator ρ,

$$\kappa_\omega(\rho) = \kappa'_\omega\big(\sqrt{M_\omega}\rho\sqrt{M_\omega}\big).$$

■

A general POVM can be lifted to a projection-valued measure (PVM), as follows.

Lemma 5 (Naimark's theorem [49]). Given a positive operated-valued measure (POVM) $\boldsymbol{M} = \{M_\omega\}_{\omega\in\Omega}$ on A with a discrete measure space Ω, there exists a larger Hilbert space C including A and a projection-valued measure (PVM) $\boldsymbol{E} = \{E_\omega\}_{\omega\in\Omega}$ on C such that

$$\mathrm{Tr}\rho M_\omega = \mathrm{Tr}\rho E_\omega \quad \forall\ \rho \in S^A,\ \omega \in \Omega.$$

■

Combining these two lemmas, we have the following corollary.

Corollary 2. Let $\boldsymbol{\kappa} = \{\kappa_\omega : A \to B\}_\omega$ be an instrument (i.e., a CP-map valued measure) with an input system A and an output system B. Then there exists a PVM $\boldsymbol{E} = \{E_\omega\}$ on a larger Hilbert space C including A and CPTP maps κ''_ω from C to B for each outcome ω, such that for any density operator ρ,

$$\kappa_\omega(\rho) = \kappa''_\omega(E_\omega\rho E_\omega). \tag{A1}$$

Proof. First, using Lemma 4, we choose a POVM $\boldsymbol{M} = \{M_\omega\}$ on a Hilbert space A and CPTP maps $\boldsymbol{\kappa}'_\omega$ from A to B for each outcome ω. Next, using Lemma 5, we choose a larger Hilbert space C including A and a projection-valued measure (PVM) $\boldsymbol{E} = \{E_\omega\}_{\omega\in\Omega}$ on C. We denote the projection from C to A by P. Then, we have

$$(E_\omega P)^\dagger E_\omega P = PE_\omega P = M_\omega = \sqrt{M_\omega}\sqrt{M_\omega} \tag{A2}$$

for any $\omega \in \Omega$. Thus, there exists a partial isometry V_ω from C to A such that $\sqrt{M_\omega} = V_\omega E_\omega P$. Hence, we have

$$\begin{aligned}\kappa_\omega(\rho) &= \kappa'_\omega(\sqrt{M_\omega}\rho\sqrt{M_\omega}) = \kappa'_\omega(V_\omega E_\omega P\rho PE_\omega V_\omega^\dagger)\\ &= \kappa'_\omega(V_\omega E_\omega\rho E_\omega V_\omega^\dagger).\end{aligned}$$

Defining CPTP maps κ''_ω by $\kappa''_\omega(\rho) = \kappa'_\omega(V_\omega\rho V_\omega^\dagger)$. This completes the proof. ■

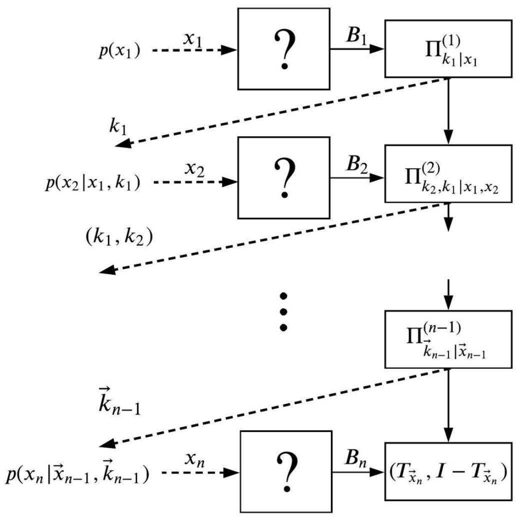

FIG. 9. Adaptive strategy for cq-channel discrimination. Solid and dashed lines denote flow of classical and quantum information, respectively. The classical outputs of PVMs are employed to decide the inputs adaptively, and leave a post-measurement state that can be accessed together with the next channel output.

APPENDIX B: PROTOCOL WITH PVM FOR CQ CHANNELS

Now, we rewrite a general adaptive method in a form of a protocol with PVM. The general procedure for discriminating cq channels can be rewritten as follows using PVMs. To start, Fig. 9 illustrates the general protocol with PVMs, which we shall describe now. In the following, according to Naimark's dilation theorem, in each mth step, we choose a sufficiently large space B_m including the original space B_m such that the measurement is a PVM.

The first input is chosen subject to the distribution $p_{X_1}(x_1)$. Then, the output state is measured by a projection-valued measure (PVM) $\{\Pi^{(1)}_{k_1|x_1}\}_{k_1}$ on B_1. The second input is then chosen according to the distribution $p_{X_2|X_1,K_1}(x_2|x_1,k_1)$. Then, a PVM $\{\Pi^{(2)}_{k_2,k_1|x_1,x_2}\}_{k_1,k_2}$ is made on B_1B_2, which satisfies $\sum_{k_2}\Pi^{(2)}_{k_2,k_1|x_1,x_2}=\Pi^{(1)}_{k_1|x_1}\otimes I$. The third input is chosen as the distribution $p_{X_3|X_1,X_2,K_1,K_2}(x_3|x_1,x_2,k_1,k_2)$, etc. Continuing, the mth step is given as follows. The sender chooses the mth input x_m according to the conditional distribution $p_{X_m|\vec{X}_{m-1},\vec{K}_{m-1}}(x_m|\vec{x}_{m-1},\vec{k}_{m-1})$. The receiver receives the mth output ρ_{x_m} or σ_{x_m} on B_m.

The description of the remaining processing requires that we distinguish two cases.

(i) For $m<n$, depending on the previous outcomes $\vec{k}_{m-1}=(k_1,\dots,k_{m-1})$ and the previous inputs $\vec{x}_m=(x_1,\dots,x_m)$, as the mth projective measurement, the receiver applies a PVM $\{\Pi^{(m)}_{\vec{k}_m|\vec{x}_m}\}_{\vec{k}_m}$ on $B_1B_2\dots B_m$, which satisfies the condition $\sum_{k_m}\Pi^{(m)}_{\vec{k}_m|\vec{x}_m}=\Pi^{(m-1)}_{\vec{k}_{m-1}|\vec{x}_{m-1}}\otimes I$. He sends the outcome k_m to the sender.

(ii) For $m=n$, dependent on the inputs $\vec{x}_n$, the receiver measures the final state on $B_1B_2\dots B_n$ with the binary POVM $(T_{\vec{x}_n},I-T_{\vec{x}_n})$ on $B_1B_2\dots B_n$, where hypothesis $\mathcal{N}$ (respectively $\overline{\mathcal{N}}$) is accepted if and only if the first (respectively second) outcome clicks.

Proposition 2. Any general procedure given in Sec. II B can be rewritten in the above form.

Proof. Recall Corollary 2 given in Sec. II A. Due to Corollary 2, when the Hilbert space B can be chosen sufficiently large, any state reduction written by a CP-map valued measure $\{\Gamma_{k_1|x_1}\}_{k_1}$ can also be written as the combination of a PVM $\{\Pi^{(1)}_{k_1|x_1}\}_{k_1}$ and a state change by a CPTP map Λ_{k_1,x_1} depending on the measurement outcome k_1 such that $\Gamma_{k_1|x_1}(\rho)=\Lambda_{k_1,x_1}(\Pi^{(1)}_{k_1|x_1}\rho\Pi^{(1)}_{k_1|x_1})$ for k_1,x_1. Hence, we have $\Gamma_{k_1|x_1}(\rho)=\Lambda_{k_1,x_1}(\Pi_{k_1|x_1}\rho\Pi_{k_1|x_1})$ for k_1,x_1.

Then, we treat the CPTP map Λ_{k_1,x_1} as a part of the next measurement. Let $\{\Gamma_{k_2|x_1,x_2,k_1}\}_{k_2}$ be the quantum instrument to describe the second measurement. We define the quantum instrument $\{\overline{\Gamma}_{k_2|x_1,x_2,k_1}\}_{k_2}$ as $\overline{\Gamma}_{k_2|x_1,x_2,k_1}(\rho):=\Gamma_{k_2|x_1,x_2,k_1}(\Lambda_{k_1,x_1}(\rho))$. Applying Corollary 2 to the quantum instrument $\{\overline{\Gamma}_{k_2|x_1,x_2,k_1}\}_{k_2}$, we choose the PVM $\{\Pi^{(2)}_{k_2|x_1,x_2,k_1}\}_{k_2}$ on $\operatorname{Im}\Pi^{(1)}_{k_1|x_1}\otimes B_2$ and the state change by a CPTP map $\Lambda_{k_1,k_2,x_1,x_2}$ depending on the measurement outcome k_2 to satisfy (A1). Since $\sum_{k_1,k_2}\Pi^{(2)}_{k_2|x_1,x_2,k_1}$ is the identity on B_1B_2, setting $\Pi^{(2)}_{k_1,k_2|x_1,x_2}:=\Pi^{(2)}_{k_2|x_1,x_2,k_1}$, we define the PVM $\{\Pi^{(2)}_{k_1,k_2|x_1,x_2}\}_{k_1,k_2}$ on B_1B_2.

In the same way, for the mth step, using a quantum instrument $\{\Gamma_{k_m|\vec{x}_m,\vec{k}_{m-1}}\}_{k_m}$, CPTP maps $\Lambda_{\vec{k}_{m-1},\vec{x}_{m-1}}$, and Corollary 2, we define the PVM $\{\Pi^{(m)}_{k_m|\vec{x}_m,\vec{k}_{m-1}}\}_{k_m}$ on $\operatorname{Im}\Pi^{(m-1)}_{\vec{k}_{m-1}|\vec{x}_{m-1}}\otimes B_m$ and the state change by CPTP maps $\Lambda_{\vec{k}_m,\vec{x}_m}$. Then, setting $\Pi^{(m)}_{\vec{k}_m|\vec{x}_m}:=\Pi^{(m)}_{k_m|\vec{x}_m,\vec{k}_{m-1}}$, we define the PVM $\{\Pi^{(m)}_{\vec{k}_m|\vec{x}_m}\}_{\vec{k}_m}$ on $B_1B_2\dots B_m$.

In the nth step, i.e., the final step, using the binary POVM $(T_{n|\vec{k}_{n-1},\vec{x}_n},I-T_{n|\vec{k}_{t-1},\vec{x}_n})$ and CPTP maps $\Lambda_{\vec{k}_{n-1},\vec{x}_{n-1}}$, we define the binary POVM $(T_{\vec{x}_n},I-T_{\vec{x}_n})$ on $B_1B_2\dots B_n$ as follows:

$$T_{\vec{x}_n}:=\sum_{\vec{k}_n}\Lambda^\dagger_{\vec{k}_{n-1},\vec{x}_{n-1}}(T_{n|\vec{k}_{n-1},\vec{x}_n}), \tag{B1}$$

where $\Lambda^\dagger_{\vec{k}_{n-1},\vec{x}_{n-1}}$ is defined as $\operatorname{Tr}\Lambda_{\vec{k}_{n-1},\vec{x}_{n-1}}(\rho)X=\operatorname{Tr}\rho\Lambda^\dagger_{\vec{k}_{n-1},\vec{x}_{n-1}}(X)$. In this way, the general protocol given in Sec. II B has been converted to a protocol given in this subsection. ■

It is implicit that the projective measurement $\{\Pi^{(m)}_{\vec{k}_m|\vec{x}_m}\}_{\vec{k}_m}$ includes first projecting the output from the quantum memory onto a subspace spanned by $\{\Pi^{(m-1)}_{\vec{k}_{m-1}|\vec{x}_{m-1}}\}_{\vec{k}_{m-1}}$, and then finding $\vec{k}_m$ in the entire subspace of $\operatorname{Im}\Pi^{(m-1)}_{\vec{k}_{m-1}|\vec{x}_{m-1}}\otimes B_m$. Hence, $\{\Pi^{(m)}_{k_m|\vec{k}_{m-1},\vec{x}_{m-1}}\}_{\vec{k}_m}$ can be regarded as a PVM on $B_1B_2\dots B_m$ and from the construction

$$\sum_{k_m}\Pi^{(m)}_{\vec{k}_m|\vec{x}_m}=\big(\Pi^{(1)}_{k_1|x_1}\otimes I^{\otimes(m-1)}\big)\dots\big(\Pi^{(m-1)}_{\vec{k}_{m-1}|\vec{x}_{m-1}}\otimes I\big),$$

which shows that the PVMs commute.

Notice also that

$$\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}\leqslant\Pi^{(n-2)}_{\vec{k}_{n-2}|\vec{x}_{n-2}}\otimes I\leqslant\dots\leqslant\Pi^{(1)}_{k_1|\vec{x}_1}\otimes I^{\otimes(n-2)}.$$

Therefore, the states $\rho^{(n)}$ and $\sigma^{(n)}$ before the final measurement, which are defined in (2) and (3), are rewritten as

$$\rho^{(n)} = \sum_{\vec{x}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1}) \times \left(\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}\left(\rho_{x_1}\otimes\cdots\otimes\rho_{x_n}\right)\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}} \otimes |\vec{x}_n\rangle\langle\vec{x}_n|\right), \tag{B2}$$

$$\sigma^{(n)} = \sum_{\vec{x}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1}) \times \left(\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}\left(\sigma_{x_1}\otimes\cdots\otimes\sigma_{x_n}\right)\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}} \otimes |\vec{x}_n\rangle\langle\vec{x}_n|\right). \tag{B3}$$

APPENDIX C: AUXILIARY RESULTS AND PROOF OF LEMMA 1

For our proof of Theorem 1, we prepare several properties for the quantities $C(a,b)$ and $B(r)$ defined in (6) and (7). The following lemma states the continuity of the $B(r)$ function, of which we give two different proofs. The first proof uses the known facts for the case of two states, and the cq-channel case is reduced to the former by general statements from convex analysis. The second proof is rather more *ad hoc* and relies on peculiarities of the functions at hand.

Lemma 6. The function (Hoeffding exponent) $B(r)$ is continuous in r, i.e., for any non-negative real number r_0,

$$\lim_{r\to r_0} B(r) = B(r_0). \tag{C1}$$

The combination of Lemma 6 and the above observation guarantees that the map $r \mapsto B(r) - r$ is a continuous and strictly decreasing function from $[0, D(\mathcal{N}\|\overline{\mathcal{N}})]$ to $[-D(\mathcal{N}\|\overline{\mathcal{N}}), D(\overline{\mathcal{N}}\|\mathcal{N})]$. Hence, we obtain Lemma 1, i.e., when real numbers a, b satisfy $-D(\mathcal{N}\|\overline{\mathcal{N}}) \leqslant a - b \leqslant D(\overline{\mathcal{N}}\|\mathcal{N})$, there exists $r_{a,b} \in [0, D(\mathcal{N}\|\overline{\mathcal{N}})]$ such that $B(r_{a,b}) - r_{a,b} = a - b$.

Proof. The crucial difficulty in this lemma is that unlike previous works, here we allow that $|\mathcal{X}|$ is infinite. Note that in the case of a finite alphabet, we just need to note the role of the channel (as opposed to states): it is a supremum over channel inputs $x \in \mathcal{X}$, so a preliminary task is to prove that for a fixed x, i.e., a pair of states ρ_x and σ_x, the Hoeffding function is continuous. This is already known [10, Lemma 1] and follows straightforwardly from the convexity and monotonicity of the Hoeffding function. After that, the channel's Hoeffding function is the maximum over finitely many continuous functions and so continuous. However, when the alphabet size is infinite, the supremum of infinitely many continuous functions is not necessarily continuous. Nevertheless, it inherits the convexity of the functions for each x (cf. [46, Corollary 3.2.8]). Since the function is defined on the non-negative reals $\mathbb{R}_{\geqslant 0}$, it is continuous for all $r_0 > 0$, by the well-known and elementary fact that a convex function on an interval is continuous on its interior. It only remains to prove the continuity at $r_0 = 0$; to this end, consider swapping null and alternative hypotheses and denote the corresponding Hoeffding exponent by $\overline{B}(r)$. We then find that $\overline{B}(r)$ is the inverse function of $B(r)$. Since $\overline{B}(r)$ is continuous even when it is equal to zero, i.e., at $r = D(\overline{\mathcal{N}}\|\mathcal{N})$, we conclude $B(r)$ is continuous at $r = 0$ and $B(0) = D(\overline{\mathcal{N}}\|\mathcal{N})$. ■

Lemma 7. When real numbers a, b satisfy $-D(\mathcal{N}\|\overline{\mathcal{N}}) \leqslant a - b \leqslant D(\overline{\mathcal{N}}\|\mathcal{N})$, then we have

$$C(a,b) = r_{a,b} - b = B(r_{a,b}) - a. \tag{C2}$$

Proof. Definition of $C(a,b)$ [Eq. (6)] implies that $C(a-c, b-c) = C(a,b) + c$. Hence, it is sufficient to show that for $r \in [0, D(\mathcal{N}\|\overline{\mathcal{N}})]$,

$$C(B(r), r) = 0, \tag{C3}$$

$$\begin{aligned} C(B(r), r) &= \sup_{0\leqslant\alpha\leqslant 1} (1-\alpha)D_\alpha(\mathcal{N}\|\overline{\mathcal{N}}) - \alpha B(r) - (1-\alpha)r \\ &= \sup_{0\leqslant\alpha\leqslant 1} \alpha\left(\frac{\alpha-1}{\alpha}\left(r - D_\alpha(\mathcal{N}\|\overline{\mathcal{N}})\right) - B(r)\right) = 0, \end{aligned}$$

where the last equality follows since $\frac{\alpha-1}{\alpha}[r - D_\alpha(\mathcal{N}\|\overline{\mathcal{N}})] \leqslant B(r)$ for $0 \leqslant \alpha \leqslant 1$. ■

Our approach consists of associating suitable classical channels to the given cq channels, and noting the lessons learned about adaptive strategy for discrimination of classical channels in [16]. Our proof methodology, however, is the classical case. The following Lemmas 8 and 9 address these matters; the former is verified easily and its proof is omitted, and the latter is more involved and is the key to our developments.

Lemma 8. Consider the cq channels $\mathcal{N} : x \to \rho_x$ and $\overline{\mathcal{N}} : x \to \sigma_x$ with input alphabet $\mathcal{X}$ and output density operators on Hilbert space B. Let the eigenvalue decompositions of the output operators be as follows:

$$\rho_x = \sum_i \lambda_i^x |u_i^x\rangle\langle u_i^x|, \tag{C4}$$

$$\sigma_x = \sum_j \mu_j^x |v_j^x\rangle\langle v_j^x|. \tag{C5}$$

According to [8,29], we define two distributions

$$\Gamma_x(i,j) := \lambda_i^x |\langle v_j^x | u_i^x\rangle|^2, \tag{C6}$$

$$\overline{\Gamma}_x(i,j) := \mu_i^x |\langle v_j^x | u_i^x\rangle|^2. \tag{C7}$$

First, note that for all pair of indices (i,j), we have $\Gamma_x(i,j) \geqslant 0$, $\overline{\Gamma}_x(i,j) \geqslant 0$, and $\sum_{(i,j)} \Gamma_x(i,j) = \sum_{(i,j)} \overline{\Gamma}_x(i,j) = 1$, that is, $\Gamma_x(i,j) = p((i,j)|x)$ and $\overline{\Gamma}_x(i,j) = \bar{p}((i,j)|x)$ form conditional probability distributions on the range $\{(i,j)\}$ of the pairs (i,j). One can think of Γ and $\overline{\Gamma}$ as classical channels form the input system $\mathcal{X}$ to the output system $\{(i,j)\}_{i,j}$. Second, we have

$$D_\alpha(\rho_x\|\sigma_x) = D_\alpha(\Gamma_x\|\overline{\Gamma}_x),$$

which implies [see Eq. (7)]

$$B(r) = \sup_x \sup_{0\leqslant\alpha\leqslant 1} \frac{\alpha-1}{\alpha}[r - D_\alpha(\Gamma_x\|\overline{\Gamma}_x)]. \tag{C8}$$

■

Note that any extensions of the operators $\{\rho_x, \sigma_x\}$ (not just independent and identically distributed) correspond to the classical extensions by distributions $\Gamma_x(i,j)$ and $\overline{\Gamma}_x(i,j)$. Define

$$\Gamma^n_{\vec{x}_n}(\vec{i}_n,\vec{j}_n) := \Gamma_{x_1}(i_1,j_1)\dots\Gamma_{x_n}(i_n,j_n),$$
$$\overline{\Gamma}^n_{\vec{x}_n}(\vec{i}_n,\vec{j}_n) := \overline{\Gamma}_{x_1}(i_1,j_1)\dots\overline{\Gamma}_{x_n}(i_n,j_n).$$

Then, we have the following lemma.

Lemma 9. The states $\rho^{(n)}$ and $\sigma^{(n)}$ defined in (2) and (3) satisfy

$$E^Q_{a,b,n} := \min_T 2^{an}\mathrm{Tr}(I-T)\rho^{(n)} + 2^{bn}\mathrm{Tr}T\sigma^{(n)} \geqslant \frac{1}{2}E^C_{a,b,n},$$

where

$$E^C_{a,b,n} := \min_{q_{X_1},\dots,q_{X_nK_{n-1}|\vec{K}_{n-2}\vec{X}_{n-1}\vec{I}_{n-1}\vec{J}_{n-1}}} \sum_{\vec{x}_n,\vec{j}_n,\vec{i}_n,\vec{k}_{n-1}} q_{X_1}(x_1)\dots \times q_{X_nK_{n-1}|\vec{K}_{n-2}\vec{X}_{n-1}\vec{I}_{n-1}\vec{J}_{n-1}}(x_n,k_{n-1}|\vec{k}_{n-2},\vec{x}_{n-1},\vec{i}_{n-1},\vec{j}_{n-1}) \times \min\{2^{an}\Gamma^n_{\vec{x}_n}(\vec{i}_n,\vec{j}_n), 2^{bn}\overline{\Gamma}^n_{\vec{x}_n}(\vec{i}_n,\vec{j}_n)\}.$$

Proof. Let

$$|u^{\vec{x}_n}_{\vec{i}_n}\rangle := |u^{x_1}_{i_1},\dots,u^{x_n}_{i_n}\rangle,\quad \lambda^{\vec{x}_n}_{\vec{i}_n} := \lambda^{x_1}_{i_1},\cdots\lambda^{x_n}_{i_n},$$
$$|v^{\vec{x}_n}_{\vec{j}_n}\rangle := |v^{x_1}_{j_1},\dots,v^{x_n}_{j_n}\rangle,\quad \mu^{\vec{x}_n}_{\vec{j}_n} := \mu^{x_1}_{j_1},\cdots\mu^{x_n}_{j_n}.$$

Consider $\min_T 2^{an}\mathrm{Tr}(I-T)\rho^{(n)} + 2^{bn}\mathrm{Tr}T\sigma^{(n)}$; it is sufficient to consider T to a projective measurement because the minimum can be attained when T is a projection onto the subspace that is given as the linear span of eigenspaces corresponding to negative eigenvalues of $-2^{an}\rho^{(n)} + 2^{bn}\sigma^{(n)}$. For a given $\vec{x}_n$, the final decision is given as the projection $T_{\vec{x}_n}$ on the image of the projection $\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}$ on $B^{\otimes n}$ depending on $\vec{x}_n$. Since $\rho^{(n)}$ and $\sigma^{(n)}$ both commute with the projection $\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}$, without loss of generality, we can assume that the projection $T_{\vec{x}_n}$ is also commutative with $\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}$. Then, the final decision operator T_n is given as the projection $T_n := \sum_{\vec{x}_n} T_{\vec{x}_n}\otimes|\vec{x}_n\rangle\langle\vec{x}_n|$.

Now, we recall the forms (B2) and (B3) for the states $\rho^{(n)}$ and $\sigma^{(n)}$. Then, we expand the first term as follows:

$$\begin{aligned}
\mathrm{Tr}(I-T_n)\rho^{(n)} &= \sum_{\vec{x}_n,\vec{k}_{n-1}} \mathrm{Tr}(I-T_{\vec{x}_n})p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1})\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}(\rho_{x_1}\otimes\cdots\otimes\rho_{x_n})\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}\\
&= \sum_{\vec{x}_n,\vec{k}_{n-1}} \mathrm{Tr}(I-T_{\vec{x}_n})^2 p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1})\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}(\rho_{x_1}\otimes\cdots\otimes\rho_{x_n})\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}\\
&= \sum_{\vec{x}_n,\vec{k}_{n-1}} \mathrm{Tr}(I-T_{\vec{x}_n})\sum_{\vec{j}_n}\left|v^{\vec{x}_n}_{\vec{j}_n}\right\rangle\!\left\langle v^{\vec{x}_n}_{\vec{j}_n}\right|(I-T_{\vec{x}_n})p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1})\\
&\quad\times \Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}(\rho_{x_1}\otimes\cdots\otimes\rho_{x_n})\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}\\
&= \sum_{\vec{x}_n,\vec{j}_n,\vec{i}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1})\lambda^{\vec{x}_n}_{\vec{i}_n}\left|\langle u^{\vec{x}_n}_{\vec{i}_n}|(I-T_{\vec{x}_n})\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}|v^{\vec{x}_n}_{\vec{j}_n}\rangle\right|^2,
\end{aligned}$$

where the first line follows from the definition of T, the second line is due to the fact that the final measurement can be chosen as a projective measurement, the third line follows because $\sum_{\vec{j}_n}|v^{\vec{x}_n}_{\vec{j}_n}\rangle\langle v^{\vec{x}_n}_{\vec{j}_n}| = I^{\otimes n}$, and the last line is simple manipulation.

Similarly, we have

$$\mathrm{Tr}T\sigma^{(n)} = \sum_{\vec{x}_n,\vec{j}_n,\vec{i}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1})\mu^{\vec{x}_n}_{\vec{j}_n}\left|\langle u^{\vec{x}_n}_{\vec{i}_n}|T_{\vec{x}_n}\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}|v^{\vec{x}_n}_{\vec{j}_n}\rangle\right|^2.$$

For $m\in[1:n]$, define

$$\begin{aligned}
&q_{X_mK_{m-1}|\vec{K}_{m-2}\vec{X}_{m-1}\vec{I}_{m-1}\vec{J}_{m-1}}(x_m,k_{m-1}|\vec{x}_{m-1},\vec{k}_{m-2},\vec{i}_{m-1},\vec{j}_{m-1})\\
&:= p_{X_m|\vec{X}_{m-1},\vec{K}_{m-1}}(x_m|\vec{x}_{m-1},\vec{k}_{m-1})\frac{\left|\langle u^{\vec{x}_{m-1}}_{\vec{i}_{m-1}}|\Pi^{(m-1)}_{\vec{k}_{m-1}|\vec{x}_{m-1}}|v^{\vec{x}_{m-1}}_{\vec{j}_{m-1}}\rangle\right|^2}{\left|\langle u^{\vec{x}_{m-2}}_{\vec{i}_{m-2}}|\Pi^{(m-2)}_{\vec{k}_{m-2}|\vec{x}_{m-2}}|v^{\vec{x}_{m-2}}_{\vec{j}_{m-2}}\rangle\right|^2\left|\langle u^{x_{m-1}}_{i_{m-1}}|v^{x_{m-1}}_{j_{m-1}}\rangle\right|^2}.
\end{aligned}$$

Hence,

$$\begin{aligned}
\min_T 2^{an}\mathrm{Tr}(I-T)\rho^{(n)} + 2^{bn}\mathrm{Tr}T\sigma^{(n)} &= \sum_{\vec{x}_n,\vec{j}_n,\vec{i}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1})\\
&\quad\times\left(2^{an}\lambda^{\vec{x}_n}_{\vec{j}_n}\left|\langle u^{\vec{x}_n}_{\vec{i}_n}|(I-T_{\vec{x}_n})\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}|v^{\vec{x}_n}_{\vec{j}_n}\rangle\right|^2 + 2^{bn}\mu^{\vec{x}_n}_{\vec{i}_n}\left|\langle u^{\vec{x}_n}_{\vec{i}_n}|T_{\vec{x}_n}\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}|v^{\vec{x}_n}_{\vec{j}_n}\rangle\right|^2\right)\\
&\geqslant \sum_{\vec{x}_n,\vec{j}_n,\vec{i}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1})\min\left\{2^{an}\lambda^{\vec{x}_n}_{\vec{i}_n}, 2^{bn}\mu^{\vec{x}_n}_{\vec{j}_n}\right\}\\
&\quad\times\left(\left|\langle u^{\vec{x}_n}_{\vec{i}_n}|T_{\vec{x}_n}\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}|v^{\vec{x}_n}_{\vec{j}_n}\rangle\right|^2 + \left|\langle u^{\vec{x}_n}_{\vec{i}_n}|(I-T_{\vec{x}_n})\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_{n-1}}|v^{\vec{x}_n}_{\vec{j}_n}\rangle\right|^2\right)
\end{aligned}$$

$$\overset{\text{(a)}}{\geqslant} \sum_{\vec{x}_n,\vec{j}_n,\vec{i}_n,\vec{k}_{n-1}} p_{X_1}(x_1)\dots p_{X_n|\vec{X}_{n-1},\vec{K}_{n-1}}(x_n|\vec{x}_{n-1},\vec{k}_{n-1}) \min\left\{2^{an}\lambda^{\vec{x}_n}_{\vec{i}_n}, 2^{bn}\mu^{\vec{x}_n}_{\vec{j}_n}\right\}$$

$$\times\ \frac{1}{2}\left|\langle u^{\vec{x}_n}_{\vec{i}_n}|\Pi^{(n-1)}_{\vec{k}_{n-1}|\vec{x}_n}|v^{\vec{x}_n}_{\vec{j}_n}\rangle\right|^2$$

$$= \frac{1}{2}\sum_{\vec{x}_n,\vec{j}_n,\vec{i}_n,\vec{k}_{n-1}} q_{X_1}(x_1)\dots q_{X_nK_{n-1}|\vec{K}_{n-2}\vec{X}_{n-1}\vec{I}_{n-1}\vec{J}_{n-1}}(x_nk_{n-1}|\vec{k}_{n-2}\vec{x}_{n-1}\vec{i}_{n-1}\vec{j}_{n-1})$$

$$\times\ \min\{2^{an}\Gamma_{\vec{x}_n}(\vec{i}_n,\vec{j}_n), 2^{bn}\overline{\Gamma}_{\vec{x}_n}(\vec{i}_n,\vec{j}_n)\},$$

where (a) follows from the relation $|\alpha|^2+|\beta|^2 \geqslant \frac{1}{2}|\alpha+\beta|^2$. ■

APPENDIX D: PROOF OF THEOREM 1

We are now in a position to show Theorem 1, which is shown by the combination of Lemma 10 and Corollary 3, which are proven in this Appendix.

Lemma 10 (Generalized Chernoff bound). For two cq channels $\mathcal{N}$ and $\overline{\mathcal{N}}$, and for real numbers a, b satisfying $-D(\mathcal{N}\|\overline{\mathcal{N}}) \leqslant a-b \leqslant D(\overline{\mathcal{N}}\|\mathcal{N})$,

$$C^{\mathbb{A}^{c,0}}(a,b|\mathcal{N}\|\overline{\mathcal{N}}) = C^{\mathbb{P}^0}(a,b|\mathcal{N}\|\overline{\mathcal{N}}) = C(a,b) = r_{a,b}-b = B(r_{a,b})-a.$$

Proof. For the direct part, i.e., that strategies in $\mathbb{P}^0$ achieve this exponent, the following nonadaptive strategy achieves $C(a,b)$. Consider the transmission of a letter x on every channel use. Define the test T_n as the projection to the eigenspace of the positive eigenvalues of $2^{na}\rho_x^{\otimes n}-2^{nb}\sigma_x^{\otimes n}$. Audenaert *et al.* [7] showed that

$$\begin{aligned}2^{na}\mathrm{Tr}[\rho_x^{\otimes n}(I-T_n)]+2^{nb}\mathrm{Tr}[\sigma_x^{\otimes n}T_n] &\leqslant \inf_{0\leqslant\alpha\leqslant1}\mathrm{Tr}(2^{na}\rho_x^{\otimes n})^{\alpha}(2^{nb}\sigma_x^{\otimes n})^{1-\alpha}\\ &= 2^{-n\sup_{0\leqslant\alpha\leqslant1}[(1-\alpha)D_\alpha(\rho_x\|\sigma_x)-\alpha a-(1-\alpha)b]}.\end{aligned} \tag{D1}$$

Considering the optimization for x, we obtain the direct part.

For the converse part, since

$$C^{\mathbb{A}^{c,0}}(a,b|\mathcal{N}\|\overline{\mathcal{N}}) = C^{\mathbb{A}^{c,0}}(B(r_{a,b}),r_{a,b}|\mathcal{N}\|\overline{\mathcal{N}})+B(r_{a,b})-a = C^{\mathbb{A}^{c,0}}(B(r_{a,b}),r_{a,b}|\mathcal{N}\|\overline{\mathcal{N}})+r_{a,b}-b,$$

it is sufficient to show $C^{\mathbb{A}^{c,0}}(B(r),r|\mathcal{N}\|\overline{\mathcal{N}}) \geqslant 0$ for $r\in[0,D(\mathcal{N}\|\overline{\mathcal{N}})]$. Observe that

$$E^C_{a,b,n} = 2^{an}\alpha_n(\Gamma\|\overline{\Gamma}|\mathcal{T}_{a,b,n})+2^{bn}\beta_n(\Gamma\|\overline{\Gamma}|\mathcal{T}_{a,b,n}),$$

where we let $\mathcal{T}_{a,b,n}$ be the optimal test to achieve $E^C_{a,b,n}$. We choose $a=B(r)$ and $b=r$ in Lemma 9. The combination of (C8) and [16, Eq. (16)] guarantees that

$$B_e^{\mathbb{A}^{c,0}}(r|\Gamma\|\overline{\Gamma}) = B(r). \tag{D2}$$

Notice that the analysis in [16] does not assume any condition on the set $\mathcal{X}$. When

$$\liminf_{n\to\infty}\frac{1}{n}\log_2 2^{rn}\beta_n(\Gamma\|\overline{\Gamma}|\mathcal{T}_{B(r),r,n}) < 0,$$

then Eq. (D2) implies

$$\liminf_{n\to\infty}\frac{1}{n}\log_2 2^{B(r)n}\alpha_n(\Gamma\|\overline{\Gamma}|\mathcal{T}_{B(r),r,n}) \geqslant 0.$$

Hence, we have

$$\liminf_{n\to\infty}\frac{1}{n}\log_2 E^C_{B(r),r,n} = \max\left\{\liminf_{n\to\infty}\frac{1}{n}\log_2 2^{rn}\beta_n(\Gamma\|\overline{\Gamma}|\mathcal{T}_{B(r),r,n}),\ \liminf_{n\to\infty}\frac{1}{n}\log_2 2^{B(r)n}\alpha_n(\Gamma\|\overline{\Gamma}|\mathcal{T}_{B(r),r,n})\right\} \geqslant 0. \tag{D3}$$

Therefore, the combination of Lemma 9 and (D3) implies that

$$C^{\mathbb{A}^{c,0}}(B(r),r|\mathcal{N}\|\overline{\mathcal{N}}) = \liminf_{n\to\infty}\frac{1}{n}\log_2 E^Q_{B(r),r,n} \geqslant 0. \tag{D4}$$

This completes the proof. ■

As corollary, we obtain the Hoeffding exponent.

Corollary 3 (Hoeffding bound). For two cq channels $\mathcal{N}$ and $\overline{\mathcal{N}}$, and for any $0\leqslant r\leqslant D(\mathcal{N}\|\overline{\mathcal{N}})$,

$$B_e^{\mathbb{A}^{c,0}}(r|\mathcal{N}\|\overline{\mathcal{N}}) = B_e^{\mathbb{P}^0}(r|\mathcal{N}\|\overline{\mathcal{N}}) = B(r).$$

Proof. For the direct part, note that a nonadaptive strategy following the Hoeffding bound for state discrimination developed in [11] suffices to show the achievability. More precisely, sending the letter x optimizing the expression on the right-hand side to every channel use and invoking the result by [11] for state discrimination shows the direct part of the theorem.

For the converse part, note first that from Theorem 1, for any $r \in [0, D(\mathcal{N}\|\overline{\mathcal{N}})]$,

$$C^{\mathbb{A}^{c,0}}(B(r), r|\mathcal{N}\|\overline{\mathcal{N}}) = 0.$$

When a sequence of tests T_n satisfies $\liminf_{n\to\infty} \frac{1}{n}\log_2 \beta_n[\mathcal{N}\|\overline{\mathcal{N}}|T_n] \leqslant -r_0 < -r_0 + \epsilon$, Eq. (D4) with $r = r_0 - \epsilon$ implies that $\liminf_{n\to\infty} \frac{1}{n}\log_2 \alpha_n[\mathcal{N}\|\overline{\mathcal{N}}|T_n] \geqslant -B(r_0 - \epsilon)$. Hence, we have

$$B_e^{\mathbb{A}^{c,0}}(r_0|\mathcal{N}\|\overline{\mathcal{N}}) \leqslant B(r_0 - \epsilon). \tag{D5}$$

Due to Lemma 6, taking the limit $\epsilon \to 0$ leads to the following inequality:

$$B_e^{\mathbb{A}^{c,0}}(r_0|\mathcal{N}\|\overline{\mathcal{N}}) \leqslant B(r_0). \tag{D6}$$

This completes the proof. ■

[1] H.-Y. Huang, R. Kueng, and J. Preskill, Information-Theoretic Bounds on Quantum Advantage in Machine Learning, Phys. Rev. Lett. **126**, 190505 (2021).

[2] H. Chernoff, A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, Ann. Math. Stat. **23**, 493 (1952).

[3] W. Hoeffding, Asymptotically optimal tests for multinomial distributions, Ann. Math. Stat. **36**, 369 (1965).

[4] T. S. Han and K. Kobayashi, The strong converse theorem for hypothesis testing, IEEE Trans. Inf. Theory **35**, 178 (1989).

[5] F. Hiai and D. Petz, The proper formula for relative entropy and its asymptotics in quantum probability, Commun. Math. Phys. **143**, 99 (1991).

[6] T. Ogawa and H. Nagaoka, Strong converse and Stein's lemma in quantum hypothesis testing, IEEE Trans. Inf. Theory **46**, 2428 (2000).

[7] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, L. Masanes, A. Acin, and F. Verstraete, Discriminating States: The Quantum Chernoff Bound, Phys. Rev. Lett. **98**, 160501 (2007).

[8] M. Nussbaum and A. Szkoła, The Chernoff lower bound for symmetric quantum hypothesis testing, Ann. Stat. **37**, 1040 (2009).

[9] M. Hayashi, *Quantum Information Theory: Mathematical Foundation*, 2nd ed. (Springer, Berlin, 2016).

[10] T. Ogawa and M. Hayashi, On error exponents in quantum hypothesis testing, IEEE Trans. Inf. Theory **50**, 1368 (2004).

[11] M. Hayashi, Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding, Phys. Rev. A **76**, 062301 (2007).

[12] H. Nagaoka, The converse part of the theorem for quantum Hoeffding bound, arXiv:quant-ph/0611289.

[13] A. Chefles, A. Kitagawa, M. Takeoka, M. Sasaki, and J. Twamley, Unambiguous discrimination among oracle operators, J. Phys. A: Math. Theor. **40**, 10183 (2007).

[14] A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, Adaptive versus nonadaptive strategies for quantum channel discrimination, Phys. Rev. A **81**, 032339 (2010).

[15] A. Krawiec, Ł. Pawela, and Z. Puchała, Discrimination of POVMs with rank-one effects, Quantum Inf. Process. **19**, 428 (2020).

[16] M. Hayashi, Discrimination of two channels by adaptive methods and its application to quantum system, IEEE Trans. Inf. Theory **55**, 3807 (2009).

[17] M. Berta, C. Hirche, E. Kaur, and M. M. Wilde, Amortized channel divergence for asymptotic quantum channel discrimination, Lett. Math. Phys. **110**, 2277 (2020).

[18] Z. Puchała, Ł. Pawela, A. Krawiec, R. Kukulski, and M. Oszmaniec, Multiple-shot and unambiguous discrimination of von Neumann measurements, Quantum **5**, 425 (2021).

[19] P. Lewandowska, A. Krawiec, R. Kukulski, Ł. Pawela, and Z. Puchała, On the optimal certification of von Neumann measurements, Sci. Rep. **11**, 3623 (2021).

[20] S. Pirandola and C. Lupo, Ultimate Precision of Adaptive Noise Estimation, Phys. Rev. Lett. **118**, 100502 (2017).

[21] R. Duan, Y. Feng, and M. Ying, Perfect Distinguishability of Quantum Operations, Phys. Rev. Lett. **103**, 210501 (2009).

[22] R. Duan, C. Guo, C.-K. Li, and Y. Li, Parallel distinguishability of quantum operations, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, Piscataway, NJ, 2016), pp. 2259–2263.

[23] D. Puzzuoli and J. Watrous, Ancilla dimension in quantum channel discrimination, Ann. Henri Poincaré **18**, 1153 (2017).

[24] X. Wang and M. M. Wilde, Resource theory of asymmetric distinguishability for quantum channels, Phys. Rev. Research **1**, 033169 (2019).

[25] K. Fang, O. Fawzi, R. Renner, and D. Sutter, Chain Rule for the Quantum Relative Entropy, Phys. Rev. Lett. **124**, 100501 (2020).

[26] T. Cooney, M. Mosonyi, and M. M. Wilde, Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication, Commun. Math. Phys. **344**, 797 (2016).

[27] C. Hirche, M. Hayashi, E. Bagan, and J. Calsamiglia, Discrimination Power of a Quantum Detector, Phys. Rev. Lett. **118**, 160502 (2017).

[28] For simplicity, here and in the rest of the paper, we assume the set $\mathcal{K}$ to be discrete. In fact, if the Hilbert spaces A, B, etc., on which the CP maps act are finite dimensional, then every instrument is a convex combination, i.e., a probabilistic mixture, of instruments with only finitely many nonzero elements; this carries over to instruments defined on a general measurable space $\mathcal{K}$. Thus, in the finite-dimensional case the assumption of discrete $\mathcal{K}$ is not really a restriction.

[29] M. Hayashi, Optimal sequence of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing, J. Phys. A: Math. Gen. **35**, 10759 (2002).

[30] D. Kretschmann and R. F. Werner, Quantum channels with memory, Phys. Rev. A **72**, 062323 (2005).

[31] G. Gutoski and J. Watrous, Toward a general theory of quantum games, in *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC)* (Association for Computing Machinery, New York, 2007), pp. 565–574.

[32] G. Chiribella, G. Mauro D'Ariano, and P. Perinotti, Memory Effects in Quantum Channel Discrimination, Phys. Rev. Lett. **101**, 180501 (2008).

[33] G. Chiribella, G. Mauro D'Ariano, and P. Perinotti, Transforming quantum operations: Quantum supermaps, Europhys. Lett. **83**, 30004 (2008).

[34] G. Chiribella, G. Mauro D'Ariano, and P. Perinotti, Theoretical framework for quantum networks, Phys. Rev. A **80**, 022339 (2009).

[35] J. Watrous, Semidefinite programs for completely bounded norms, Theory Comput. **5**, 217 (2009).

[36] G. Gutoski, On a measure of distance for quantum strategies, J. Math. Phys. **53**, 032202 (2012).

[37] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, Advances in photonic quantum sensing, Nat. Photonics **12**, 724 (2018).

[38] V. Katariya and M. M. Wilde, Evaluating the advantage of adaptive strategies for quantum channel distinguishability, Phys. Rev. A **104**, 052406 (2021).

[39] A. Kitaev, Quantum computations: algorithms and error correction, Russ. Math. Surveys **52**, 1191 (1997).

[40] D. Aharonov, A. Kitaev, and N. Nisan, Quantum circuits with mixed states, in *Proceedings of the 13th Annual ACM Symposium on Theory of Computation (STOC)* (Association for Computing Machinery, New York, 1997), pp. 20–30.

[41] V. I. Paulsen, *Completely Bounded Maps and Operator Algebras*, Cambridge Studies in Advanced Mathematics (Cambridge University Press, Cambridge, 2002).

[42] N. Yu and L. Zhou, When is the Chernoff exponent for quantum operations finite? IEEE Trans. Inf. Theory **67**, 4517 (2021).

[43] S. Pirandola, R. Laurenza, C. Lupo, and J. L. Pereira, Fundamental limits to quantum channel discrimination, npj Quantum Inf. **5**, 50 (2019).

[44] C. A. Fuchs and J. van de Graaf, Cryptographic distinguishability measures for quantum-mechanical states, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[45] C. King and M.-B. Ruskai, Minimal entropy of states emerging from noisy quantum channels, IEEE Trans. Inf. Theory **47**, 192 (2001).

[46] C. P. Niculescu and L.-E. Persson, *Convex Functions and Their Applications*, 2nd ed. (Springer, Berlin, 2018).

[47] A. Fujiwara and P. Algoet, One-to-one parametrization of quantum channels, Phys. Rev. A **59**, 3290 (1999).

[48] Y. Li, V. Y. F. Tan, and M. Tomamichel, Optimal adaptive strategies for sequential quantum hypothesis testing, arXiv:2104.14706.

[49] M. A. Naimark (Neumark), On a representation of additive operator set functions, Dokl. Akad. Nauk SSSR: C. R. l'Acad. Sci. l'URSS (N. S.) **41**, 359 (1943).