

Error exponents of quantum state discrimination with composite correlated hypotheses

Kun Fang

School of Data Science

The Chinese University of Hong Kong, Shenzhen
Shenzhen, Guangdong, China
kunfang@cuhk.edu.cn

Masahito Hayashi

School of Data Science

The Chinese University of Hong Kong, Shenzhen
Shenzhen, Guangdong, China
International Quantum Academy
Futian District, Shenzhen, China
Graduate School of Mathematics
Nagoya University, Chikusa-ku, Nagoya, Japan
hmasahito@cuhk.edu.cn

Abstract—We study the error exponents in quantum hypothesis testing between two sets of quantum states, extending the analysis beyond the independent and identically distributed case to encompass composite correlated hypotheses. In particular, we introduce and compare two natural extensions of the quantum Hoeffding divergence and anti-divergence to sets of quantum states, establishing their equivalence or quantitative relations. In the error exponent regime, we generalize the quantum Hoeffding bound to stable sequences of convex, compact sets of quantum states, demonstrating that the optimal Type-I error exponent, under an exponential constraint on the Type-II error, is precisely characterized by the regularized quantum Hoeffding divergence between the sets. In the strong converse exponent regime, we provide a general lower bound on the exponent in terms of the regularized quantum Hoeffding anti-divergence and a matching upper bound when the null hypothesis is a singleton with additional assumptions. The generality of these results enables applications in various contexts, including (i) refining the generalized quantum Stein’s lemma by [Fang, Fawzi & Fawzi, 2024]; (ii) exhibiting counterexamples to the continuity of the regularized Petz Rényi divergence and Hoeffding divergence; (iii) obtaining error exponents for adversarial channel discrimination and resource detection problems.

Index Terms—Hypothesis testing, Hoeffding bound, anti-Hoeffding bound, Composite hypotheses, Correlated hypotheses

I. INTRODUCTION

Distinguishability is a central topic in information theory. A fundamental framework is *asymmetric hypothesis testing*: a sample x is drawn from either $p \equiv \{p(x)\}_{x \in \mathcal{X}}$ or $q \equiv$

$\{q(x)\}_{x \in \mathcal{X}}$, and one chooses between the two hypotheses. The goal is to minimize the Type-II error (deciding p when the truth is q) while keeping the Type-I error (deciding q when the truth is p) below a threshold. Chernoff–Stein’s Lemma [1] states that, for any fixed bound on the Type-I error, the optimal Type-II error decays exponentially with a rate by the relative entropy.

A natural question is whether this generalizes to the quantum setting. This has been extensively studied (see, e.g., [2]–[10]). One considers discrimination between two hypotheses: the system is in state ρ_n (null) or σ_n (alternative). The decision is made via a two-outcome POVM $\{M_n, I - M_n\}$. The Type-I and Type-II errors are $\alpha(\rho_n, M_n) := \text{Tr}[\rho_n(I - M_n)]$ and $\beta(\sigma_n, M_n) := \text{Tr}[\sigma_n M_n]$, respectively. In general, no measurement makes both errors vanish simultaneously. One therefore studies the asymptotics of α and β as $n \rightarrow \infty$, revealing a trade-off between them. This trade-off can be analyzed in three operational regimes: (I) the *Stein exponent* regime, focusing on the exponential decay of the Type-II error under a fixed Type-I constraint; (II) the *error exponent* regime, studying the decay of the Type-I error when the Type-II error is forced to decay with a given exponent; and (III) the *strong converse exponent* regime, characterizing the convergence of the Type-I error to one when the Type-II error decays at a given exponential rate.

While much of the existing literature has focused on i.i.d. sources, practices often involve quantum states that are not fully specified (i.e., *composite hypotheses* [10]–[15]) such as in adversarial or black-box settings [8], [16] and exhibit correlations that preclude a simple tensor product structure (i.e., *correlated hypotheses* [10], [17]–[19]). In this context, the task is to discriminate between two *sets of correlated quantum states*. That is, a tester receives samples prepared according to either the set $\mathcal{A}_n$ or $\mathcal{B}_n$, and determines, via $\{M_n, I - M_n\}$, from which set the samples originate.

As in standard hypothesis testing, two types of errors can occur. Since we aim to control the errors for any state within the given sets, regardless of which one is drawn,

K.F. is supported in part by the National Natural Science Foundation of China (Grant No. 12404569 and 92470113), the Shenzhen Science and Technology Program (Grant No. QNXMB20250701091826036 and JCYJ20240813113519025), the Shenzhen International Quantum Academy (Grant No. SIQA2025KFKT03), the Shenzhen Fundamental Research Program (Grant No. JCYJ20241202124023031), the General R&D Projects of 1+1+1 CUHK-CUHK(SZ)-GDST Joint Collaboration Fund (Grant No. GRDP2025-022), and the University Development Fund (Grant No. UDF01003565). M.H. was supported in part by the General R&D Projects of 1+1+1 CUHK-CUHK(SZ)-GDST Joint Collaboration Fund (Grant No. GRDP2025-022), the Guangdong Provincial Quantum Science Strategic Initiative (Grant No. GDZX2505003), the Shenzhen International Quantum Academy (Grant No. SIQA2025KFKT07), and the National Natural Science Foundation of China under Grant 62171212.

the (worst-case) Type-I error is defined by $\alpha(\mathcal{A}_n, M_n) := \sup_{\rho_n \in \mathcal{A}_n} \text{Tr}[\rho_n(I - M_n)]$ and the (worst-case) Type-II error is defined by $\beta(\mathcal{B}_n, M_n) := \sup_{\sigma_n \in \mathcal{B}_n} \text{Tr}[\sigma_n M_n]$. A few variants of quantum Stein's lemma has been shown in this worst-case setting under some structural assumptions on the sets $\mathcal{A}_n$ and $\mathcal{B}_n$ [9], [20], [21]. In particular, the result in [9] states that, for any fixed Type-I constraint, the optimal Type-II error exponent for testing $\mathcal{A}_n$ against $\mathcal{B}_n$ is given by the regularized relative entropy between the sets.

In this work, we refine the analysis of asymmetric hypothesis testing for composite correlated hypotheses, as developed in [9], [20], [21], by extending it to the error exponent and strong converse exponent regimes.

Due to the uncertainty and correlation inherent in composite correlated hypotheses, several significant challenges arise when obtaining precise characterizations. First, discrimination strategies must be state-agnostic, ensuring that error probabilities are universally controlled for every state within the respective sets, regardless of which specific state is encountered. Second, the optimization problem exhibits a minimax structure, forming a competing scenario that requires simultaneous maximization over all possible states in the sets and minimization over all possible quantum measurements. Third, the non-i.i.d. structure significantly complicates the asymptotic analysis, as standard techniques relying on tensor product structures no longer directly apply. Fourth, it becomes necessary to define suitable extensions of the quantum Hoeffding divergence and anti-divergence to sets of quantum states that both recover existing results for i.i.d. sources and precisely capture the essential features of the general composite correlated setting.

In the error exponent regime, we compare two natural ways of extending the Hoeffding divergence from individual states to sets of states. One viewpoint defines the relevant quantity by looking at the most difficult pair of states drawn from the two sets. The other first extends the underlying Petz Rényi divergence to sets and then builds the corresponding Hoeffding quantity from that extension. We show that these two definitions agree for every finite blocklength, and that their asymptotic versions remain closely related. Our main result, Theorem 1, then shows that the optimal error exponent is exactly characterized by the regularized Hoeffding divergence from the first viewpoint.

In the strong converse regime, we similarly study two extensions of the quantum Hoeffding anti-divergence to sets of states. One is based on the largest anti-divergence attained by a pair of states from the two sets, while the other is obtained by first extending the sandwiched Rényi divergence to sets and then forming the associated anti-divergence. We show that these two constructions coincide both at finite blocklength and in the asymptotic limit. Theorem 2 then shows that the strong converse exponent is always bounded below by the regularized Hoeffding anti-divergence, and that this lower bound is exact when the null hypothesis consists of a single state under additional assumptions.

As applications, we recover the quantum Stein's lemma for composite correlated hypotheses as established in [9], and further strengthen it by providing explicit convergence rates for the Type-I error. Note that the Stein exponent only indicates whether the Type-I error decays, but does not quantify how fast it decays. Besides this, we also provide a few more explicit applications, including: (i) finding counterexamples to the continuity of the regularized Petz Rényi divergence and Hoeffding divergence; (ii) deriving error exponents for adversarial quantum channel discrimination; and (iii) obtaining error exponents for resource detection problems in coherence theory and entanglement theory.

II. PRELIMINARIES

We adopt the following notational conventions. Finite-dimensional Hilbert spaces are denoted by $\mathcal{H}$, with $|\mathcal{H}|$ indicating their dimension. The set of all linear operators on $\mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$, while $\mathcal{H}(\mathcal{H})$ and $\mathcal{H}_+(\mathcal{H})$ denote the sets of Hermitian and positive semidefinite operators on $\mathcal{H}$, respectively. The set of density operators (i.e., positive semidefinite operators with unit trace) on $\mathcal{H}$ is denoted by $\mathcal{D}(\mathcal{H})$. Calligraphic letters such as $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are used to represent sets of linear operators. Unless otherwise specified, all logarithms are taken to base two and denoted by $\log(x)$.

A functional $\mathbb{D} : \mathcal{D} \times \mathcal{H}_+ \rightarrow \mathbb{R}$ is called a *quantum divergence* if it satisfies the data-processing inequality. For any $\rho \in \mathcal{D}$ and $\sigma \in \mathcal{H}_+$, the Umegaki relative entropy is defined by [22] as $D(\rho\|\sigma) := \text{Tr}[\rho(\log \rho - \log \sigma)]$ if $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ and $+\infty$ otherwise. For $\alpha \in (0, 1)$, the Petz Rényi divergence is defined [23] as $D_{P,\alpha}(\rho\|\sigma) := \frac{1}{\alpha-1} \log Q_\alpha(\rho\|\sigma)$ with $Q_\alpha(\rho\|\sigma) := \text{Tr}[\rho^\alpha \sigma^{1-\alpha}]$ if $\rho \not\perp \sigma$ and $+\infty$ otherwise. For $\alpha > 1$, the sandwiched Rényi divergence is defined [24], [25] as $D_{S,\alpha}(\rho\|\sigma) := \frac{1}{\alpha-1} \log \text{Tr} \left[\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right]^\alpha$ if $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ and $+\infty$ otherwise.

Definition 1. Let $\mathbb{D}$ be a quantum divergence between two quantum states. Let $\mathcal{H}$ be a finite-dimensional Hilbert space. Then for any sets $\mathcal{A}, \mathcal{B} \subseteq \mathcal{D}(\mathcal{H})$, the quantum divergence between these two sets is defined by $\mathbb{D}(\mathcal{A}\|\mathcal{B}) := \inf \{ \mathbb{D}(\rho\|\sigma) : \rho \in \mathcal{A}, \sigma \in \mathcal{B} \}$. Let $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ be two sequences of sets of quantum states, where each $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. The regularized divergence between these sequences is defined by $\mathbb{D}^\infty(\mathcal{A}\|\mathcal{B}) := \liminf_{n \rightarrow \infty} \frac{1}{n} \mathbb{D}(\mathcal{A}_n\|\mathcal{B}_n)$. If the limit exists, we define the regularized divergence as $\mathbb{D}^\infty(\mathcal{A}\|\mathcal{B}) := \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{D}(\mathcal{A}_n\|\mathcal{B}_n)$.

In many practical scenarios, the sequences of sets under consideration are not arbitrary but possess a structure that is compatible with tensor products. This property is known as *stability* (or *closeness*) under tensor product.

Definition 2 (Stable sequence). Let $\mathcal{A} \subseteq \mathcal{H}_+(\mathcal{H}_1)$, $\mathcal{B} \subseteq \mathcal{H}_+(\mathcal{H}_2)$, and $\mathcal{C} \subseteq \mathcal{H}_+(\mathcal{H}_1 \otimes \mathcal{H}_2)$. We say that $\{\mathcal{A}, \mathcal{B}, \mathcal{C}\}$ is *stable under tensor product* if, for any $X_1 \in \mathcal{A}$ and $X_2 \in \mathcal{B}$,

it holds that $X_1 \otimes X_2 \in \mathcal{C}$. In short, we write $\mathcal{A} \otimes \mathcal{B} \subseteq \mathcal{C}$. A sequence of sets $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ with $\mathcal{C}_n \subseteq \mathcal{H}_+(\mathcal{H}^{\otimes n})$ is called stable under tensor product if $\mathcal{C}_n \otimes \mathcal{C}_m \subseteq \mathcal{C}_{n+m} \forall n, m \in \mathbb{N}$.

III. Hoeffding (ANTI-)DIVERGENCE FOR SETS

In this section, we develop extensions of the quantum Hoeffding divergence and anti-divergence to sets of quantum states. Two natural approaches arise for this purpose.

A. Quantum Hoeffding divergence

Let $\mathcal{H}$ be a finite-dimensional Hilbert space, $r > 0$ be a real number, and $n \in \mathbb{N}$. Let $\rho_n, \sigma_n \in \mathcal{D}(\mathcal{H}^{\otimes n})$ be two quantum states. The quantum Hoeffding divergence is defined as $H_{n,r}(\rho_n \parallel \sigma_n) := \sup_{\alpha \in (0,1)} \frac{\alpha-1}{\alpha} (nr - D_{P,\alpha}(\rho_n \parallel \sigma_n))$. Let $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$ be two sets of quantum states. Two variants of the quantum Hoeffding divergence between these sets can be defined. The first extension treats the Hoeffding divergence as a quantum divergence and extends it to sets via Definition 1: $H_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n) := \inf \{H_{n,r}(\rho_n \parallel \sigma_n) : \rho_n \in \mathcal{A}_n, \sigma_n \in \mathcal{B}_n\}$. The second approach leverages the explicit formula for the Hoeffding divergence in terms of the Petz Rényi divergences: $\mathfrak{H}_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n) := \sup_{\alpha \in (0,1)} \frac{\alpha-1}{\alpha} (nr - D_{P,\alpha}(\mathcal{A}_n \parallel \mathcal{B}_n))$, where $D_{P,\alpha}(\mathcal{A}_n \parallel \mathcal{B}_n)$ is defined as in Definition 1.

Moreover, let $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ be two sequences of sets of quantum states, where each $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. The regularized quantum Hoeffding divergences between these sequences are defined as $\underline{H}_r^\infty(\mathcal{A} \parallel \mathcal{B}) := \liminf_{n \rightarrow \infty} \frac{1}{n} H_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n)$. If the limits exist, we define the regularized divergence as $H_r^\infty(\mathcal{A} \parallel \mathcal{B}) := \lim_{n \rightarrow \infty} \frac{1}{n} H_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n)$ and $\mathfrak{H}_r^\infty(\mathcal{A} \parallel \mathcal{B}) := \sup_{\alpha \in (0,1)} \frac{\alpha-1}{\alpha} (r - D_{P,\alpha}^\infty(\mathcal{A} \parallel \mathcal{B}))$, where $D_{P,\alpha}^\infty(\mathcal{A} \parallel \mathcal{B})$ is defined as in Definition 1.

Lemma 1. Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and $r > 0$ be a real number, $n \in \mathbb{N}$. Let $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$ be two convex compact sets of quantum states. Then $H_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n) = \mathfrak{H}_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n)$. Let $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ be two stable sequences of convex compact sets of quantum states, where each $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. For any $n \in \mathbb{N}$, $\frac{1}{n} \mathfrak{H}_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n) \geq H_r^\infty(\mathcal{A} \parallel \mathcal{B}) \geq \mathfrak{H}_r^\infty(\mathcal{A} \parallel \mathcal{B})$.

Establishing an equality $H_r^\infty(\mathcal{A} \parallel \mathcal{B}) = \mathfrak{H}_r^\infty(\mathcal{A} \parallel \mathcal{B})$ for the regularizations appears to be challenging, as existing minimax theorems typically require at least one of the spaces to be compact—a condition that is not directly satisfied here. Moreover, as shown in [26] that the Petz Rényi divergence and the Hoeffding divergence between two sets can be non-additive in general, which further complicates the situation.

B. Quantum Hoeffding anti-divergence

The quantum Hoeffding anti-divergence is defined as $H_{n,r}^*(\rho_n \parallel \sigma_n) := \sup_{\alpha > 1} \frac{\alpha-1}{\alpha} (nr - D_{S,\alpha}(\rho_n \parallel \sigma_n))$. Let $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$ be two sets of quantum states. Two variants of the quantum Hoeffding anti-divergence between these sets are defined as

$H_{n,r}^*(\mathcal{A}_n \parallel \mathcal{B}_n) := \sup \{H_{n,r}^*(\rho_n \parallel \sigma_n) : \rho_n \in \mathcal{A}_n, \sigma_n \in \mathcal{B}_n\}$ and $\mathfrak{H}_{n,r}^*(\mathcal{A}_n \parallel \mathcal{B}_n) := \sup_{\alpha > 1} \frac{\alpha-1}{\alpha} (nr - D_{S,\alpha}(\mathcal{A}_n \parallel \mathcal{B}_n))$, where $D_{S,\alpha}(\mathcal{A}_n \parallel \mathcal{B}_n)$ is defined as in Definition 1. Moreover, let $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ be two sequences of sets of quantum states, where each $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. The regularized quantum Hoeffding anti-divergences between these sequences are defined as $\underline{H}_r^{*,\infty}(\mathcal{A} \parallel \mathcal{B}) := \liminf_{n \rightarrow \infty} \frac{1}{n} H_{n,r}^*(\mathcal{A}_n \parallel \mathcal{B}_n)$. If the limits exist, we define the regularized divergence as $H_r^{*,\infty}(\mathcal{A} \parallel \mathcal{B}) := \lim_{n \rightarrow \infty} \frac{1}{n} H_{n,r}^*(\mathcal{A}_n \parallel \mathcal{B}_n)$ and $\mathfrak{H}_r^{*,\infty}(\mathcal{A} \parallel \mathcal{B}) := \sup_{\alpha > 1} \frac{\alpha-1}{\alpha} (r - D_{S,\alpha}^\infty(\mathcal{A} \parallel \mathcal{B}))$, where $D_{S,\alpha}^\infty(\mathcal{A} \parallel \mathcal{B})$ is defined as in Definition 1.

Lemma 2. Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and $r > 0$ be a real number, $n \in \mathbb{N}$. Let $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$ be two sets of quantum states. Then $H_{n,r}^*(\mathcal{A}_n \parallel \mathcal{B}_n) = \mathfrak{H}_{n,r}^*(\mathcal{A}_n \parallel \mathcal{B}_n)$. Let $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ be two stable sequences of sets of quantum states, where each $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. Then $H_r^{*,\infty}(\mathcal{A} \parallel \mathcal{B}) = \mathfrak{H}_r^{*,\infty}(\mathcal{A} \parallel \mathcal{B})$.

Note that $H_{n,r}^*(\mathcal{A}_n \parallel \mathcal{B}_n)$ is defined as a supremum over the feasible states, which makes its additivity property for stable sequences unclear—even though we know the Hoeffding anti-divergence for states is subadditive. Nevertheless, the above result shows that the regularization $H_r^{*,\infty}$ indeed exists for stable sequences and coincides with $\mathfrak{H}_r^{*,\infty}$ in general.

C. Optimal Type-I error probability

The error exponent and strong converse exponent regimes study the optimal behavior of the Type-I error provided that the Type-II error exponentially decays. More explicitly, the optimal Type-I error for hypothesis testing between two sets of quantum states, $\mathcal{A}_n$ and $\mathcal{B}_n$, is defined as $\alpha_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n) := \min_{0 \leq M_n \leq I} \{\alpha(\mathcal{A}_n, M_n) : \beta(\mathcal{B}_n, M_n) \leq 2^{-nr}\}$, where the measurement M_n is chosen to minimize the worst-case Type-I error $\alpha(\mathcal{A}_n, M_n)$, subject to the constraint that the Type-II error $\beta(\mathcal{B}_n, M_n)$ decays exponentially at a rate r . In other words, the measurement must perform universally well for all states in $\mathcal{A}_n$ and $\mathcal{B}_n$. As a special case, $\alpha_{n,r}(\rho_n \parallel \sigma_n)$ is defined similarly for individual states ρ_n and σ_n .

The following result shows that the optimal Type-I error is precisely determined by the most challenging pair of states from these sets. This implies that there exists a universal measurement that is independent of the specific states, whose performance matches that of the optimal measurement for the worst-case pair of states.

Lemma 3. Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and $r > 0$ be a real number, $n \in \mathbb{N}$. Let $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$ be two convex sets of quantum states. Then $\alpha_{n,r}(\mathcal{A}_n \parallel \mathcal{B}_n) = \sup \{\alpha_{n,r}(\rho_n \parallel \sigma_n) : \rho_n \in \mathcal{A}_n, \sigma_n \in \mathcal{B}_n\}$.

IV. ERROR EXPONENT

In this section, we establish the quantum Hoeffding bound for composite correlated hypotheses. Notably, the result holds

under minimal and standard assumptions, which are satisfied by many frameworks of interest [9], [20], [21].

Assumption 1. Denote a sequence of sets of quantum states $\mathcal{C} = \{\mathcal{C}_n\}_{n \in \mathbb{N}}$ where each $\mathcal{C}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. (C1) Convexity: For any $n \in \mathbb{N}$, the set $\mathcal{C}_n$ is convex; (C2) Compactness: For any $n \in \mathbb{N}$, the set $\mathcal{C}_n$ is compact; (C3) Stability under tensor product: For any $m, n \in \mathbb{N}$, it holds that $\mathcal{C}_m \otimes \mathcal{C}_n \subseteq \mathcal{C}_{m+n}$; (C4) Finiteness: $D_{P,\alpha}(\mathcal{A}_1 \| \mathcal{B}_1) < \infty$ for $\alpha \in (0, 1)$.

Theorem 1. Let $\mathcal{H}$ be a finite-dimensional Hilbert space. Let $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ be two sequences of sets of quantum states, where each $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. Let $0 < r < D^\infty(\mathcal{A} \| \mathcal{B})$ be a real number.

- If $\mathcal{A}$ and $\mathcal{B}$ satisfy assumptions (C1) and (C2):

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log \alpha_{n,r}(\mathcal{A}_n \| \mathcal{B}_n) \geq \underline{H}_r^\infty(\mathcal{A} \| \mathcal{B}).$$

- If $\mathcal{A}$ and $\mathcal{B}$ satisfy assumptions (C3) and (C4):

$$\limsup_{n \rightarrow \infty} -\frac{1}{n} \log \alpha_{n,r}(\mathcal{A}_n \| \mathcal{B}_n) \leq H_r^\infty(\mathcal{A} \| \mathcal{B}).$$

Consequently, if $\mathcal{A}$ and $\mathcal{B}$ satisfy (C1), (C2), (C3) and (C4), then the following limit exists and

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \alpha_{n,r}(\mathcal{A}_n \| \mathcal{B}_n) = H_r^\infty(\mathcal{A} \| \mathcal{B}).$$

This strengthens the previous result by Mosonyi et al. [13, Eq. (II.65)] by establishing the tightness of the regularized Hoeffding bound.

V. STRONG CONVERSE EXPONENT

We also extend the strong converse exponent to the broader context of composite correlated hypotheses and show that the strong converse exponent is lower bounded by a regularized quantum Hoeffding anti-divergence between the sets in general. We also provide a matching upper bound when the null hypothesis is a singleton i.i.d. state.

For the upper bound, we need to introduce the permutation invariance. Let U_{A^n} denote the natural unitary representation of the permutation group S_n that permutes the subsystems of $A^n := A_1 A_2 \cdots A_n$. An linear operator $X_{A^n} \in \mathcal{L}(A^n)$ is called permutation invariant if it satisfies $X_{A^n} = U_{A^n}(\pi) X_{A^n} U_{A^n}(\pi)^\dagger$ for all $\pi \in S_n$. A set of quantum state $\mathcal{A}_n$ is called permutation invariant if $\rho_n \in \mathcal{A}_n$ implies that $U_{A^n}(\pi) \rho_n U_{A^n}(\pi)^\dagger \in \mathcal{A}_n$ for all $\pi \in S_n$. Let A be a system with $|A| = d$. For all $n \in \mathbb{N}$ there exists a permutation invariant state $\omega_{A^n}^n \in \mathcal{D}(A^n)$, which we call *universal state*, such that for all permutation invariant states $\rho_{A^n} \in \mathcal{D}(A^n)$, we have $\rho_{A^n} \leq g_{n,d} \omega_{A^n}^n$ with $g_{n,d} \leq (n+1)^{d^2-1}$. Such a universal state exists and has been explicitly constructed in [14].

Assumption 2. Denote a sequence of sets of quantum states $\mathcal{C} = \{\mathcal{C}_n\}_{n \in \mathbb{N}}$ where each $\mathcal{C}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. (C5) Permutation invariance: For any $n \in \mathbb{N}$, the set $\mathcal{C}_n$ is permutation invariant; (C6) Universal state containment: For any $n \in \mathbb{N}$, the set $\mathcal{C}_n$ contains a universal state.

Theorem 2. Let $\mathcal{H}$ be a finite-dimensional Hilbert space. Let $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ be two sequences of sets of quantum states, where each $\mathcal{A}_n, \mathcal{B}_n \subseteq \mathcal{D}(\mathcal{H}^{\otimes n})$. Let $r > D^\infty(\mathcal{A} \| \mathcal{B})$ be a real number.

- Regardless of the structure of $\mathcal{A}$ and $\mathcal{B}$, we have

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \log(1 - \alpha_{n,r}(\mathcal{A}_n \| \mathcal{B}_n)) \geq \underline{H}_r^{*,\infty}(\mathcal{A} \| \mathcal{B}).$$

- If $\mathcal{A}_n = \{\rho^{\otimes n}\}$ is a singleton i.i.d. state and $\mathcal{B}$ satisfies assumptions (C1), (C5) and (C6), and moreover, $D_{S,\alpha}^\infty(\mathcal{A} \| \mathcal{B})$ exists and is differentiable for $\alpha \geq 1$, then

$$\limsup_{n \rightarrow \infty} -\frac{1}{n} \log(1 - \alpha_{n,r}(\mathcal{A}_n \| \mathcal{B}_n)) \leq \mathfrak{H}_r^{*,\infty}(\mathcal{A} \| \mathcal{B}).$$

Consequently, with the same assumptions for the upper bound and additionally assuming that $\mathcal{B}$ satisfies assumption (C3), then the limit exists and is given by

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log(1 - \alpha_{n,r}(\mathcal{A}_n \| \mathcal{B}_n)) = H_r^{*,\infty}(\mathcal{A} \| \mathcal{B}).$$

VI. APPLICATIONS

A. Refining quantum Stein's lemma between two sets

The generalized quantum Stein's lemma for hypothesis testing between two sets of quantum states in [9, Theorem 32] can be both recovered and strengthened as follows.

Theorem 3. Let $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ be two sequences of sets satisfying the same assumptions in [9, Theorem 32]. For any $0 < r < D^\infty(\mathcal{A} \| \mathcal{B})$, then $\liminf_{n \rightarrow \infty} -\frac{1}{n} \log \alpha_{n,r}(\mathcal{A}_n \| \mathcal{B}_n) \geq \mathfrak{H}_r^\infty(\mathcal{A} \| \mathcal{B}) > 0$. For any $r > D^\infty(\mathcal{A} \| \mathcal{B})$, then $\liminf_{n \rightarrow \infty} -\frac{1}{n} \log(1 - \alpha_{n,r}(\mathcal{A}_n \| \mathcal{B}_n)) \geq \mathfrak{H}_r^{*,\infty}(\mathcal{A} \| \mathcal{B}) > 0$.

These results show that any Type-II error exponent below $D^\infty(\mathcal{A} \| \mathcal{B})$ is achievable, with the Type-I error decaying at least as fast as $\mathfrak{H}_r^\infty(\mathcal{A} \| \mathcal{B})$. Conversely, for Type-II error exponents above $D^\infty(\mathcal{A} \| \mathcal{B})$, the Type-I error converges to one exponentially, at a rate at least $\mathfrak{H}_r^{*,\infty}(\mathcal{A} \| \mathcal{B})$. Thus, $D^\infty(\mathcal{A} \| \mathcal{B})$ serves as a sharp threshold for the asymptotic trade-off in hypothesis testing. Notably, the quantum Hoeffding bound (Theorem 1) and strong converse exponent (Theorem 2) hold under very general conditions, without requiring the polar assumption from [9].

B. Discontinuity of $D_{P,\alpha}^\infty(\mathcal{A} \| \mathcal{B})$ at $\alpha = 1$

In the i.i.d. setting, the error exponent is viewed as a refinement of the Stein exponent, since the latter can be recovered from the former via the continuity of the Rényi divergence between two fixed states. In the same spirit, our error exponent results would recover the Stein exponent if the regularized Petz Rényi divergence were continuous at $\alpha = 1$, i.e., $\sup_{\alpha \in (0,1)} D_{P,\alpha}^\infty(\mathcal{A} \| \mathcal{B}) = D^\infty(\mathcal{A} \| \mathcal{B})$. However, such continuity may fail in general. In particular, for any sequences of sets $\mathcal{A} = \{\mathcal{A}_n\}_{n \in \mathbb{N}}$ and $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$ that satisfy our error-exponent assumptions but violate the Stein lemma, we must have a strict inequality $\sup_{\alpha \in (0,1)} D_{P,\alpha}^\infty(\mathcal{A} \| \mathcal{B}) <$

$D^\infty(\mathcal{A}\|\mathcal{B})$, i.e., a discontinuity of $D_{P,\alpha}^\infty(\mathcal{A}\|\mathcal{B})$ at $\alpha = 1$. Such examples can be found in [27].

We now give a more explicit example. Denote $H(p) := -p \log p - (1-p) \log(1-p)$ as the binary entropy function and $D(p\|q) := p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q}$ as the classical relative entropy. Denote the set of types with length n by $\mathcal{P}_n$, which is the set of all empirical distributions. Give $P \in \mathcal{P}_n$, the type class of P , denoted as $\mathcal{T}_n(P)$, is the set of bit strings whose empirical distribution is P . We choose two rational numbers $p_1 = \frac{m_1}{m}$ and $p_2 = \frac{m_2}{m}$ such that $p_1 < p_2 \in (0, p_3)$. Let $P_j = (p_j, 1-p_j)$ be the binary distribution. Consider a two-dimensional Hilbert space $\mathcal{H}$ spanned by $\{|0\rangle, |1\rangle\}$ and define the qubit state $\rho(p) := p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$. We denote the uniform distribution over $\mathcal{T}_{km}(P_j)$ in the space $\mathcal{H}^{\otimes km}$ by $\rho_{j,km} := \frac{1}{|\mathcal{T}_{km}(P_j)|} \sum_{x^{km} \in \mathcal{T}_{km}(P_j)} |x^{km}\rangle\langle x^{km}|$ for $j = 1, 2$, where $|\mathcal{T}_{km}(P_j)| = \binom{km}{km_j}$ is the size of the type class. In the following examples, we regard the Hilbert space $\mathcal{H}^{\otimes m}$ as a one-copy system. We define the convex mixture, $\rho_{km} := \lambda \rho_{1,km} + (1-\lambda) \rho_{2,km}$, with the choice of $\lambda \in (0, 1)$, such that $\min_{i \in \{1,2\}} \frac{1}{2} \log \frac{2\pi m_i(m-m_i)}{m} \geq H(\lambda)$. Consider the set of states $\mathcal{A}_n := \{\rho_{k_1 m} \otimes \cdots \otimes \rho_{k_l m} : k_1, \dots, k_l \geq 1, \sum_{i=1}^l k_i = n\}$, and $\mathcal{B}_n := \{\rho(p_3)^{\otimes mn}\}$. Then sequences are stable under tensor product. But we have $\sup_{\alpha \in (0,1)} D_{P,\alpha}^\infty(\mathcal{A}\|\mathcal{B}) < D^\infty(\mathcal{A}\|\mathcal{B})$. More examples can be found in the full paper [26].

C. Adversarial quantum channel discrimination

Adversarial quantum channel discrimination was introduced in [8]. A tester queries an untrusted device n times; the device is guaranteed to be either a channel $\mathcal{N}_{A \rightarrow B}$ or $\mathcal{M}_{A \rightarrow B}$, but may behave adversarially and create correlations across rounds. Let $\mathcal{U}_{A \rightarrow BE}$ and $\mathcal{V}_{A \rightarrow BE}$ be Stinespring dilations of $\mathcal{N}$ and $\mathcal{M}$, respectively, with E an environment system. Denote all CPTP maps from X to Y as $\text{CPTP}(X:Y)$.

In round i , the adversary applies a CPTP map $\mathcal{P}_{R_{i-1}E_{i-1} \rightarrow A_i R_i} \in \text{CPTP}(R_{i-1}E_{i-1} : A_i R_i)$, (where $R_0 E_0$ are trivial) and then sends A_i through $\mathcal{U}$, producing $B_i E_i$. After n rounds, the tester holds $B^n := B_1 \cdots B_n$ and the resulting (possibly correlated) output state is $\rho[\{\mathcal{P}^i\}_{i=1}^n] := \text{Tr}_{R_n E_n} [\prod_{i=1}^n (\mathcal{U}_{A_i \rightarrow B_i E_i} \circ \mathcal{P}_{R_{i-1}E_{i-1} \rightarrow A_i R_i}^i)]$. If instead the device implements $\mathcal{M}$ with internal maps $\mathcal{Q}^i$, the tester receives $\sigma[\{\mathcal{Q}^i\}_{i=1}^n] := \text{Tr}_{R_n E_n} [\prod_{i=1}^n (\mathcal{V}_{A_i \rightarrow B_i E_i} \circ \mathcal{Q}_{R_{i-1}E_{i-1} \rightarrow A_i R_i}^i)]$. The tester performs a binary POVM $\{M_n, I - M_n\}$ on B^n . Due to the uncertainty of adversary's behavior, the tester's knowledge is naturally modeled by the two sets of achievable output states $\mathcal{A}_n := \{\rho[\{\mathcal{P}^i\}_{i=1}^n] : \mathcal{P}^i \in \text{CPTP}(R_{i-1}E_{i-1} : A_i R_i), \forall i, \forall R_i\}$ or $\mathcal{B}_n := \{\sigma[\{\mathcal{Q}^i\}_{i=1}^n] : \mathcal{Q}^i \in \text{CPTP}(R_{i-1}E_{i-1} : A_i R_i), \forall i, \forall R_i\}$. A non-adaptive strategy by adversary is a standard subclass that ignores the environments and does not update between rounds. In this case the attainable sets by the tester reduce to the image sets of tensor-power channels: $\mathcal{A}'_n := \{\mathcal{N}^{\otimes n}(\rho_n) : \rho_n \in \mathcal{D}(A^{\otimes n})\}$ and $\mathcal{B}'_n := \{\mathcal{M}^{\otimes n}(\sigma_n) : \sigma_n \in \mathcal{D}(A^{\otimes n})\}$. It was shown in [8] that the optimal Stein exponent (for both

adaptive and non-adaptive settings) is given by the regularized minimum output channel divergence $D^{\text{inf},\infty}(\mathcal{N}\|\mathcal{M})$.

Here, we can check that $\{\mathcal{A}_n\}, \{\mathcal{A}'_n\}, \{\mathcal{B}_n\}, \{\mathcal{B}'_n\}$ are all stable sequences of convex and compact sets of states (the convexity of $\{\mathcal{A}_n\}, \{\mathcal{B}_n\}$ is proved in [8]). Therefore, our error exponent result directly applies to adversarial quantum channel discrimination. In particular, for any $0 < r < D^{\text{inf},\infty}(\mathcal{N}\|\mathcal{M})$, the optimal Type-I error exponent under an exponential constraint on the Type-II error is given by $\lim_{n \rightarrow \infty} -\frac{1}{n} \log \alpha_{n,r}(\mathcal{A}_n\|\mathcal{B}_n) = H_r^\infty(\mathcal{A}\|\mathcal{B})$ and $\lim_{n \rightarrow \infty} -\frac{1}{n} \log \alpha_{n,r}(\mathcal{A}'_n\|\mathcal{B}'_n) = H_r^\infty(\mathcal{A}'\|\mathcal{B}') > 0$ where we can ensure the strict positivity as the continuity of the regularized Petz Rényi divergence holds in this case [8].

D. Error exponents in quantum resource detection

As Theorem 1 and 2 require minimal assumptions, they can be readily applied to the detection problem in various quantum resource theories (see e.g. [10]), where the stability of the set of free states is naturally satisfied [28], [29], including entanglement [11], [30]–[32], coherence [33]–[37], and magic [38]–[41]. We showcase coherence theory and entanglement theory as two illustrative examples with explicit expressions. In particular, let $\mathcal{I}_n$ be the set of incoherent states on n subsystems. Then, in the resource theory of coherence, our results yield explicit expressions for the error exponent as $\lim_{n \rightarrow \infty} -\frac{1}{n} \log \alpha_{n,r}(\rho^{\otimes n}\|\mathcal{I}_n) = \sup_{\alpha \in (0,1)} \frac{\alpha-1}{\alpha} (r - D_{P,\alpha}(\rho\|\mathcal{I}_1))$ and the strong converse exponent as $\lim_{n \rightarrow \infty} -\frac{1}{n} \log(1 - \alpha_{n,r}(\rho^{\otimes n}\|\mathcal{I}_n)) = \sup_{\alpha > 1} \frac{\alpha-1}{\alpha} (r - D_{S,\alpha}(\rho\|\mathcal{I}_1))$. Similar expressions hold in the resource theory of entanglement for maximally correlated states in the full paper [26].

VII. DISCUSSION

We have established a framework for analyzing error exponents in quantum hypothesis testing between two sets of quantum states, extending beyond the conventional i.i.d. setting to encompass composite correlated hypotheses. Compared to recent advances on the Stein exponent [9], [20], [21], our error exponent requires substantially weaker assumptions. In particular, it does not rely on permutation invariance or full-rank assumptions as in [20], [21], nor on the polar assumption used in [9], which are essential in those works for their proofs. The broad applicability of our framework is demonstrated through concrete applications to adversarial quantum channel discrimination and various quantum resource theories, highlighting its potential for further advances across quantum information theory. A full version of this paper is available at [26], which provides details and proofs of all results.

REFERENCES

- [1] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *The Annals of Mathematical Statistics*, pp. 493–507, 1952.
- [2] F. Hiai and D. Petz, "The proper formula for relative entropy and its asymptotics in quantum probability," *Communications in Mathematical Physics*, vol. 143, pp. 99–114, 1991.

- [3] T. Ogawa and H. Nagaoka, "Strong converse and Stein's lemma in quantum hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, pp. 2428–2433, feb 2000.
- [4] M. Hayashi, "Optimal sequence of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing," *Journal of Physics A: Mathematical and General*, vol. 35, no. 50, p. 10759, 2002.
- [5] M. Hayashi, "Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 76, no. 6, p. 062301, 2007.
- [6] M. Mosonyi and T. Ogawa, "Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies," *Communications in Mathematical Physics*, vol. 334, pp. 1617–1648, 2015.
- [7] X. Wang and M. M. Wilde, "Resource theory of asymmetric distinguishability for quantum channels," *Physical Review Research*, vol. 1, p. 033169, dec 2019.
- [8] K. Fang, H. Fawzi, and O. Fawzi, "Adversarial quantum channel discrimination," *Physical Review Letters*, vol. 135, p. 260201, Dec 2025.
- [9] K. Fang, H. Fawzi, and O. Fawzi, "Generalized quantum asymptotic equipartition," *arXiv preprint arXiv:2411.04035*, 2024.
- [10] M. Hayashi and Y. Ito, "Entanglement measures for detectability," *IEEE Transactions on Information Theory*, vol. 71, p. 4385–4405, Apr. 2025.
- [11] F. G. Brandao and M. B. Plenio, "A generalization of quantum Stein's lemma," *Communications in Mathematical Physics*, vol. 295, no. 3, pp. 791–828, 2010.
- [12] M. Berta, F. G. Brandão, and C. Hirche, "On composite quantum hypothesis testing," *Communications in Mathematical Physics*, vol. 385, no. 1, pp. 55–77, 2021.
- [13] M. Mosonyi, Z. Szilágyi, and M. Weiner, "On the error exponents of binary state discrimination with composite hypotheses," *IEEE Transactions on Information Theory*, vol. 68, p. 1032–1067, Feb. 2022.
- [14] M. Hayashi and M. Tomamichel, "Correlation detection and an operational interpretation of the Rényi mutual information," *Journal of Mathematical Physics*, vol. 57, no. 10, 2016.
- [15] A. Dasgupta, N. A. Warsi, and M. Hayashi, "Universal tester for multiple independence testing and classical-quantum arbitrarily varying multiple access channel," *IEEE Transactions on Information Theory*, vol. 71, no. 5, pp. 3719–3765, 2025.
- [16] K. Watanabe and R. Takagi, "Black box work extraction and composite hypothesis testing," *Physical Review Letters*, vol. 133, no. 25, p. 250401, 2024.
- [17] F. Hiai, M. Mosonyi, and T. Ogawa, "Large deviations and chernoff bound for certain correlated states on a spin chain," *Journal of Mathematical Physics*, vol. 48, no. 12, 2007.
- [18] F. Hiai, M. Mosonyi, and T. Ogawa, "Error exponents in hypothesis testing for correlated states on a spin chain," *Journal of Mathematical Physics*, vol. 49, no. 3, 2008.
- [19] M. Mosonyi and T. Ogawa, "Two approaches to obtain the strong converse exponent of quantum hypothesis testing for general sequences of quantum states," *IEEE Transactions on Information Theory*, vol. 61, no. 12, pp. 6975–6994, 2015.
- [20] M. Hayashi and H. Yamasaki, "The generalized quantum Stein's lemma and the second law of quantum resource theories," *Nature Physics*, pp. 1–6, 2025.
- [21] L. Lami, "A solution of the generalized quantum Stein's lemma," *IEEE Transactions on Information Theory*, vol. 71, p. 4454–4484, June 2025.
- [22] H. Umegaki, "Conditional expectation in an operator algebra," *Tohoku Mathematical Journal, Second Series*, vol. 6, no. 2-3, pp. 177–181, 1954.
- [23] D. Petz, "Quasi-entropies for finite quantum systems," *Reports on Mathematical Physics*, vol. 23, no. 1, pp. 57–65, 1986.
- [24] M. Müller-Lennert, F. Dupuis, O. Szechr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," *Journal of Mathematical Physics*, vol. 54, no. 12, 2013.
- [25] M. M. Wilde, A. Winter, and D. Yang, "Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy," *Communications in Mathematical Physics*, vol. 331, pp. 593–622, 2014.
- [26] K. Fang and M. Hayashi, "Error exponents of quantum state discrimination with composite correlated hypotheses," *arXiv preprint: 2508.12901*, 2025.
- [27] M. Hayashi, "General detectability measure," *Communications in Mathematical Physics*, vol. 406, no. 12, p. 289, 2025.
- [28] F. G. Brandao and G. Gour, "Reversible framework for quantum resource theories," *Physical Review Letters*, vol. 115, no. 7, p. 070503, 2015.
- [29] E. Chitambar and G. Gour, "Quantum resource theories," *Reviews of Modern Physics*, vol. 91, no. 2, p. 025001, 2019.
- [30] K. Fang, X. Wang, M. Tomamichel, and R. Duan, "Non-asymptotic entanglement distillation," *IEEE Transactions on Information Theory*, vol. 65, no. 10, pp. 6454–6465, 2019.
- [31] B. Regula, K. Fang, X. Wang, and M. Gu, "One-shot entanglement distillation beyond local operations and classical communication," *New Journal of Physics*, vol. 21, no. 10, p. 103017, 2019.
- [32] T. Theurer, K. Fang, and G. Gour, "Single-shot entanglement manipulation of states and channels revisited," *IEEE Transactions on Information Theory*, 2025.
- [33] A. Winter and D. Yang, "Operational resource theory of coherence," *Physical Review Letters*, vol. 116, Mar. 2016.
- [34] M. G. Díaz, K. Fang, X. Wang, M. Rosati, M. Skotiniotis, J. Calsamiglia, and A. Winter, "Using and reusing coherence to realize quantum processes," *Quantum*, vol. 2, p. 100, 2018.
- [35] K. Fang, X. Wang, L. Lami, B. Regula, and G. Adesso, "Probabilistic distillation of quantum coherence," *Physical Review Letters*, vol. 121, no. 7, p. 070404, 2018.
- [36] B. Regula, K. Fang, X. Wang, and G. Adesso, "One-shot coherence distillation," *Physical Review Letters*, vol. 121, no. 1, p. 010401, 2018.
- [37] M. Hayashi, K. Fang, and K. Wang, "Finite block length analysis on quantum coherence distillation and incoherent randomness extraction," *IEEE Transactions on Information Theory*, vol. 67, no. 6, pp. 3926–3944, 2021.
- [38] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancillas," *Physical Review A*, vol. 71, Feb. 2005.
- [39] K. Fang and Z.-W. Liu, "No-go theorems for quantum resource purification," *Physical Review Letters*, vol. 125, no. 6, p. 060405, 2020.
- [40] K. Fang and Z.-W. Liu, "No-go theorems for quantum resource purification: New approach and channel theory," *PRX Quantum*, vol. 3, no. 1, p. 010337, 2022.
- [41] K. Fang and Z.-W. Liu, "One-shot distillation with constant overhead using catalysts," *arXiv preprint arXiv: 2410.14547*, 2025.