Abstract—We study a variant of quantum hypothesis testing wherein an additional ‘inconclusive’ measurement outcome is added, allowing one to abstain from attempting to discriminate the hypotheses. The error probabilities are then conditioned on a successful attempt, with inconclusive trials disregarded. We completely characterise this task in both the single-shot and asymptotic regimes, providing exact formulas for the optimal error probabilities. In particular, we prove that the asymptotic error exponent of discriminating any two quantum states $\rho$ and $\sigma$ is given by the Hilbert projective metric $D_{\text{max}}(\rho||\sigma) + D_{\text{max}}(\sigma||\rho)$ in asymmetric hypothesis testing, and by the Thompson metric $\max\{D_{\text{max}}(\rho||\sigma), D_{\text{max}}(\sigma||\rho)\}$ in symmetric hypothesis testing. This endows these two quantities with fundamental operational interpretations in quantum state discrimination. Our findings extend to composite hypothesis testing, where we show that the asymmetric error exponent with respect to any convex set of density matrices is given by a regularisation of the Hilbert projective metric. We apply our results also to quantum channels, showing that no advantage is gained by employing adaptive or even more general discrimination schemes over parallel ones, in both the asymmetric and symmetric settings. Our state discrimination results make use of no properties specific to quantum mechanics and are also valid in general probabilistic theories.

Index Terms—Hypothesis testing, quantum state discrimination, quantum channel discrimination, relative entropies.

I. INTRODUCTION

Quantum hypothesis testing — a generalisation of the crucial statistical primitive of hypothesis testing to the non-commutative setting — is a fundamental task that directly underlies many protocols in quantum information science [1], [2], [3]. It is concerned with the problem of distinguishing different quantum states or channels, and in particular asks about the ultimate limits of such distinguishability.

In quantum state discrimination, after receiving one of two possible states, $\rho$ (null hypothesis) or $\sigma$ (alternative hypothesis), one aims to determine which of the two was actually obtained. This is typically done by performing a quantum measurement, or positive operator-valued measure (POVM), given by the tuple $M := \{M_1, M_2\}$ where $M_2 = I - M_1$. If measurement outcome 1 is obtained (corresponding to the operator $M_1$), one guesses that the state is $\rho$; if outcome 2 is obtained, one guesses $\sigma$. There are then two types of errors that can occur: the type I error with probability

$$\alpha(M) := \text{Tr} M_2 \rho,$$

which corresponds to incorrectly guessing $\sigma$ when $\rho$ was true (false positive), and the type II error with probability

$$\beta(M) := \text{Tr} M_1 \sigma,$$

which is the case of guessing $\rho$ when $\sigma$ was true (false negative). Two settings naturally emerge here: one is asymmetric hypothesis testing, which asks about how small one of the errors can be subject to constraints on the other error; another setting is symmetric hypothesis testing, where the two errors are treated equally and one aims to minimise their average.

Specifically, the asymmetric case is concerned with the study of the optimised type II error probability

$$\beta_\varepsilon(\rho, \sigma) := \min_{M \in M_2} \left\{ \beta(M) \mid \alpha(M) \leq \varepsilon \right\} \leq \min_{M_1, M_2 \geq 0} \left\{ \text{Tr} M_1 \sigma \mid M_1 + M_2 = I, \text{Tr} M_2 \rho \leq \varepsilon \right\},$$

where $M_2$ denotes the set of all two-outcome measurements. The symmetric error depends also on the prior probabilities associated with the two hypotheses, that is, the probability that the state to be discriminated is $\rho$ or that it is $\sigma$. Denoting the respective priors by $p$ and $q := 1 - p$, we define the symmetric error as

$$p_{\text{err}}(\rho, \sigma \mid p, q) := \min_{M \in M_2} \left\{ p \text{Tr} M_2 \rho + q \text{Tr} M_1 \sigma \mid M_1 + M_2 = I \right\}.$$

The two optimised error probabilities defined above are not too difficult to characterise: they are both efficiently computable semidefinite programs, and the symmetric error even admits an exact solution given by the celebrated Helstrom–Holevo theorem [4], [5] in terms of the trace distance (total variation distance),

$$p_{\text{err}}(\rho, \sigma \mid p, q) = \frac{1}{2} (1 - \| \rho \sigma - p q \|_1),$$

where $\| \cdot \|_1$ denotes the trace norm (Schatten 1-norm).

However, a limitation of the above formulations is that they assume access to only a single copy of the state to be discriminated. This is not reflective of situations encountered in practice, where one typically deals with sources that emit many copies of quantum states, which we can use to our advantage in attempting to discriminate them. That is, we can
assume that we receive either $\rho^{\otimes n}$ or $\sigma^{\otimes n}$ and then perform a joint measurement over all $n$ systems. The crucial question then is: how exactly does the performance in discriminating two states improve when we have access to more copies of them? The ultimate limit of such protocols is described by the asymptotic setting with $n \to \infty$, and the figures of merit then are the decay rates of $\beta_n(\rho^{\otimes n}, \sigma^{\otimes n})$ and $p_{\text{err}}(\rho^{\otimes n}, \sigma^{\otimes n} | p, q)$, known as the error exponents. These two limits give rise to two of the most fundamental quantities in quantum information. The first one is the quantum relative entropy $D(\rho \| \sigma) := \text{Tr} \rho \log \rho - \log \sigma$ [6], which is known to be exactly equal to the error exponent in asymptotic hypothesis testing:

$$\lim_{n \to \infty} -\frac{1}{n} \log \beta_n(\rho^{\otimes n}, \sigma^{\otimes n}) = D(\rho \| \sigma) \quad \forall \varepsilon \in (0, 1).$$

(6)

This was shown in the works of Hiai and Petz [7] (achievability and weak converse) and Ogawa and Nagaoka [8] (strong converse). The above result, known as the quantum Stein’s lemma and the quantum Chernoff bound, is not given simply by i.i.d. quantum states

lish the quantum Stein’s lemma and the quantum Chernoff measure of distinguishability between quantum states.

In symmetric hypothesis testing, it is known that adaptive discrimination of channels can yield strict improvements over parallel protocols, although a very recent line of work [22], [23], [24] established that the advantage disappears asymptotically in asymmetric hypothesis testing, where the (weak converse) error exponent is given by the regularised channel relative entropy:

$$\lim_{n \to \infty} \frac{1}{n} \log \beta_n(\rho_n \otimes N^{\otimes n}) = D^{\infty}(M \| N)$$

$$:= \lim_{n \to \infty} \frac{1}{n} \sup_{\rho, \omega} \text{D}(\text{id} \otimes M(\rho) \| \text{id} \otimes N^{\otimes n}(\omega)) - \text{D}(\rho \| \omega).$$

(8)

In symmetric hypothesis testing, it is known that adaptive strategies can improve over parallel ones both non-asymptotically and asymptotically [25], [26], although in general no exact form of the asymptotic error exponent — and thus no extension of the Chernoff bound — is known in the setting of quantum channels [27]. The landscape of channel discrimination is further complicated by the fact that there exist even more general ways of manipulating quantum channels than adaptive protocols, for instance ones without a definite causal order structure [28], [29], and they can yield strict improvements in some settings [28], [30], [31], [32]; the asymptotic performance of such strategies, however, has not been characterised yet.

We note that all definitions of this section reduce to their corresponding classical counterparts when the two states $\rho$ and $\sigma$ commute (corresponding to probability distributions) and when the channels $M$ and $N$ are classical [33], [34].

### B. Setting

In this work, we propose a variant of quantum hypothesis testing that adds an additional, ‘inconclusive’ measurement outcome, allowing us to abstain from discriminating the states if we are not sufficiently confident in the result. This can be motivated, for instance, by an experimental situation in which a ‘no detection’ event occurs, that is, a detector responsible for distinguishing two states fails to recognise either of them. More generally, a motivation to consider such a setting could be any situation where avoiding a wrong result is of utmost importance, even if this means having to repeat the trial many times, such as would be the case e.g. with medical diagnoses.

To be specific, let us consider the case of quantum state discrimination. Given either of the two states $\rho$ or $\sigma$, we perform a three-outcome measurement $M = \{ M_1, M_2, M_T \}$. The first two outcomes are as before — outcome 1 corresponds to the guess ‘$\rho$’ and outcome 2 corresponds to the guess ‘$\sigma$’ — while the third outcome ‘$\epsilon$’ is designated as an inconclusive result, that is, a case in which we are unable to decisively distinguish the hypotheses. There is therefore some probability that our

\[ n \text{ uses of a channel } M \text{ is not the same as manipulating } n \text{ parallel copies } M^{\otimes n}, \text{ since schemes for channel discrimination much more general than naive parallel protocols can be employed. A common example are the so-called adaptive protocols, which work by processing the channel } n \text{ times, such that information obtained in previous rounds can be used to enhance the successive rounds of processing } [21]. \]
attempt to perform hypothesis testing fails: this probability is $\text{Tr} M_1 \rho$ when measuring $\rho$, and $\text{Tr} M_2 \sigma$ when measuring $\sigma$.

Such an approach dates back to the early works of Ivanovic [35], Dieks [36], and Peres [37], where it was shown that all linearly independent pure states can be discriminated with no error, but only through inconclusive protocols whose probability of success may be strictly less than one. Extensions of this idea were studied in a number of settings [38], [39], [40], [41], [42], [43], [44], [45], [46], but mostly restricted to non-asymptotic, symmetric state discrimination. A related class of problems was also studied in classical hypothesis testing [47], [48], although the way that discrimination errors and the consequent rates were defined there means that the setting is not directly comparable with ours.

Here we establish a complete and rigorous formalisation of such inconclusive state discrimination schemes in quantum hypothesis testing. Our approach is based on characterising the corresponding errors conditioned on a conclusive result; that is, assuming that either of the outcomes ‘1’ or ‘2’ was obtained, how likely is it that we made an incorrect guess? This can be understood as postselecting on a conclusive outcome of the measurement and ignoring all measurement results where the outcome ‘?’ is obtained. Depending on whether discussing the asymmetric or symmetric setting, we are concerned with the error probability when measuring a particular state $\rho$ or $\sigma$, or the average probability when measuring either of them.

To clarify how our setting differs from the conventional one of conclusive hypothesis testing, let us first consider the case of asymmetric error. Observe that the conventional type I error, for instance, is defined as $\alpha(M) = \text{P(error} \mid \rho, M \rangle$, i.e. the probability of guessing incorrectly given that the measured state is $\rho$. In our approach here, we further condition the incorrect guess event on the attainment of a conclusive outcome. We thus define the following counterparts of the conventional hypothesis testing errors: the conditional type I error and conditional type II error probabilities are given by

$$\overline{\alpha}(M) := \text{P(error} \mid \rho, M \rangle, \text{conclusive}) = \frac{\alpha(M)}{1 - \text{Tr} M_1 \rho} = \frac{\text{Tr} M_2 \rho}{\text{Tr}[(M_1 + M_2)\rho]} , \tag{9}$$

$$\overline{\beta}(M) := \text{P(error} \mid \sigma, M \rangle, \text{conclusive}) = \frac{\beta(M)}{1 - \text{Tr} M_2 \sigma} = \frac{\text{Tr} M_1 \sigma}{\text{Tr}[(M_1 + M_2)\sigma]} ,$$

where ‘conclusive’ denotes the event of a conclusive measurement outcome. The minimal type II error probability is then

$$\overline{\beta}_\varepsilon(\rho, \sigma) := \inf_{M \in M_3} \left\{ \overline{\beta}(M) \mid \overline{\alpha}(M) \leq \varepsilon \right\}$$

$$= \inf_{M_1, M_2 \geq 0} \left\{ \frac{\text{Tr} M_1 \sigma}{\text{Tr}[(M_1 + M_2)\sigma]} \mid M_1 + M_2 \leq 1, \frac{\text{Tr} M_2 \rho}{\text{Tr}[(M_1 + M_2)\rho]} \leq \varepsilon \right\} , \tag{10}$$

where $M_3$ denotes the set of all three-outcome measurements of the form $\{M_1, M_2, M_3\}$, and to avoid pathological cases the optimisation is implicitly restricted to be over operators such that $\text{Tr}[(M_1 + M_2)\sigma], \text{Tr}[(M_1 + M_2)\rho] > 0$. By construction, this error can never be larger than the conventional error $\varepsilon$, since choosing $M_2 = 0$ reduces to the usual definitions of $\alpha(M)$ and $\beta(M)$.

The analogous symmetric error is defined as follows. First, given two states, $\rho$ with prior probability $p$ and $\sigma$ with prior $q$, a measurement $M = \{M_1, M_2, M_3\}$ has the following probability of obtaining an incorrect outcome:

$$p_{\text{err}}(\rho, \sigma \mid p, q \mid M) := \text{P(error} \mid M \rangle = p \text{Tr} M_2 \rho + q \text{Tr} M_1 \sigma , \tag{11}$$

while the probability of obtaining a conclusive outcome is

$$p_{\text{conc}}(\rho, \sigma \mid p, q \mid M) := \text{P(conclusive} \mid M \rangle = 1 - (p \text{Tr} M_2 \rho + q \text{Tr} M_1 \sigma) = p \text{Tr}[(M_1 + M_2)\rho] + q \text{Tr}[(M_1 + M_2)\sigma] = \text{Tr}[(M_1 + M_2)\rho \rho + q \sigma] . \tag{12}$$

We then define the postselected symmetric probability of error $\overline{p_{\text{err}}}$ as the optimal conditional probability of error given a conclusive outcome — in other words, the smallest ratio of incorrect outcomes to all conclusive outcomes on average:

$$\overline{p_{\text{err}}} (\rho, \sigma \mid p, q \mid M) := \inf_{M \in M_3} \frac{p_{\text{err}}(\rho, \sigma \mid p, q \mid M)}{p_{\text{conc}}(\rho, \sigma \mid p, q \mid M)} = \inf_{M_1, M_2 \geq 0, M_1 + M_2 \leq 1} \frac{p \text{Tr} M_2 \rho + q \text{Tr} M_1 \sigma}{\text{Tr}[(M_1 + M_2)\rho \rho + q \sigma]} . \tag{13}$$

Before stating our main results, we need to introduce several quantities which we will find to characterise the hypothesis testing errors defined above.

Underlying all of them is the max-relative entropy [49], defined as

$$D_{\text{max}}(\rho||\sigma) := \log \inf \left\{ \lambda \in \mathbb{R}_+ \mid \rho \leq \lambda \sigma \right\}$$

$$= \left\{ \log \left\| \sigma^{1/2} \rho \sigma^{-1/2} \right\|_\infty \right\} \text{supp}(\rho) \subseteq \text{supp}(\sigma)$$

otherwise. \tag{14}

Here, the inequality between operators is understood in terms of the positive semidefinite cone, i.e. $\rho \leq \lambda \sigma$ if and only if $\lambda \sigma - \rho$ is a positive semidefinite operator, and $\|\|_\infty$ denotes the operator norm (largest singular value). This quantity is typically defined for normalised quantum states $\rho$ and $\sigma$, although we will extend the same definition also to unnormalised positive semidefinite operators. This quantity can be understood as the sandwiched Rényi divergence of order $\infty$ [50]; in the case where $\rho = P$ and $\sigma = Q$ are classical discrete probability distributions, this reduces to the $\infty$–Rényi divergence $D_{\text{max}}(P||Q) = D_{\infty}(P||Q) = \log \sup_x P(x)/Q(x)$. The max-relative entropy gives rise to two important quantities: the Hilbert projective metric [51]

$$D_{\Omega}(\rho||\sigma) := D_{\text{max}}(\rho||\sigma) + D_{\text{max}}(\sigma||\rho) \tag{15}$$
and the Thompson metric \[ D_{\Xi}(\rho,\sigma) := \max \{ D_{\text{max}}(\rho,\sigma), D_{\text{max}}(\sigma,\rho) \}. \] (16)

The two quantities have enjoyed a number of applications in various branches of geometry and analysis \[ [51], [53]. \] Within quantum information theory, the Hilbert projective metric found operational use in characterising the convertibility of quantum states in different scenarios \[ [54], [55], [56], [57]. \] Often constituting the unique function that determines the existence of probabilistic transformations between quantum resources \[ [56], [57]. \] the Thompson metric, on the other hand, was recently identified with the rate of a task known as symmetric distinguishability dilution \[ [58], [59]. \] concerned with transformations of pairs of quantum states. To date, they have not been connected with rates of quantum hypothesis testing tasks. Throughout this work, we assume that the considered quantum systems are finite dimensional.

### C. Results

Our main results are the exact evaluation of the asymptotic error exponents in the setting of postselected hypothesis testing, both for asymmetric and symmetric discrimination, and both for quantum states and channels. The framework is shown to enjoy remarkably simplified properties compared to conventional quantum hypothesis testing, allowing us to completely characterise the errors at the one-shot level as well as their asymptotic exponents. Notably, we show that the asymptotic exponents in asymmetric and symmetric postselected hypothesis testing are given exactly by the Hilbert and Thompson metrics, respectively, endowing the two quantities with operational meanings mirroring that of the quantum relative entropy and the Chernoff divergence. Our methods straightforwardly extend to the setting of composite hypothesis testing and channel discrimination, establishing results that are strictly stronger and more general than corresponding known results in conventional quantum hypothesis testing.

To our knowledge, this is the first time that the asymptotic setting of postselected hypothesis testing has been studied, even in the classical case; our results are therefore new also when the discrimination of quantum states is replaced with the discrimination of probability distributions (equivalently, commuting states).

We provide an overview of our main findings below.

1) **Asymmetric Hypothesis Testing:** In Section II we show that the asymptotic exponent of the conditional type II error in discriminating any two quantum states is given by the Hilbert projective metric \( D_{\text{H}} \) between them; specifically,

\[
\lim_{n \to \infty} -\frac{1}{n} \log \bar{\beta}_n(\rho^{\otimes n},\sigma^{\otimes n}) = D_{\text{H}}(\rho||\sigma) \quad \forall \varepsilon \in (0,1). \tag{17}
\]

This establishes an equivalent of quantum Stein’s lemma in the setting of postselected hypothesis testing. We in fact establish a closed formula for the asymmetric hypothesis testing error probability already at the one-shot level, leading directly to the above asymptotic result. Specifically, our main result in Theorem 1 shows that

\[
\bar{\beta}_n(\rho,\sigma) = \left( \frac{\varepsilon}{1-\varepsilon} 2^{D_{\text{H}}(\rho||\sigma)} + 1 \right)^{-1} \quad \forall \varepsilon \in (0,1). \tag{18}
\]

In Section II-D, we extend the above results to composite hypotheses, showing that when the alternative hypothesis \( \sigma^{\otimes n} \) is replaced by a family of convex sets of density matrices \( (\mathcal{F}_n)_{n} \) that is closed under tensor product, then the asymptotic exponent is given, for all \( \varepsilon \in (0,1) \), by

\[
\lim_{n \to \infty} -\frac{1}{n} \log \bar{\beta}_n(\rho^{\otimes n}) = D_{\text{H}}(\rho||\sigma) \tag{19}
\]

where \( \bar{\beta}_n(\rho^{\otimes n}) \) denotes the least conditional type II error in discriminating a state against all states in the set \( \mathcal{F}_n \).

2) **Symmetric Hypothesis Testing:** In Section III we establish that the asymptotic exponent of the postselected symmetric error in distinguishing any two states equals their Thompson metric \( \forall p,q \in (0,1): \)

\[
\lim_{n \to \infty} -\frac{1}{n} \log \bar{p}_{\text{err}}(\rho^{\otimes n},\sigma^{\otimes n} | p,q) = D_{\Xi}(\rho||\sigma). \tag{20}
\]

This is the equivalent of the Chernoff bound in the setting of postselected quantum hypothesis testing and gives a direct operational interpretation of the Thompson metric in state discrimination. As in the asymmetric case, the result is based on an exact quantification of the one-shot symmetric error probability, which we show in Theorem 6 to be

\[
\bar{p}_{\text{err}}(\rho,\sigma | p,q) = \left( 2^{D_{\Xi}(\rho||\sigma)} + 1 \right)^{-1}. \tag{22}
\]

The above is generalised to quantum channels in Section IV, where we show that

\[
\lim_{n \to \infty} -\frac{1}{n} \log \bar{p}_{\text{err}}(\mathcal{M}^{\otimes n},\mathcal{N}^{\otimes n} | p,q) = D_{\Xi}(\mathcal{M}||\mathcal{N}), \tag{23}
\]
again demonstrating that no advantage is gained by employing protocols more general than parallel ones.

Section VI discusses how the above results in asymmetric and symmetric state discrimination are actually valid in physical theories broader than quantum mechanics, namely, settings under the umbrella of general probabilistic theories. This is, to the best of our knowledge, the first time that asymptotic error exponents in hypothesis testing have been computed in such general theories — previous such results made explicit use of the properties of quantum mechanics or classical probability theory.

II. ASYMMETRIC CASE

A. One-Shot Discrimination Error

Let us recall the definition of the minimal postselected type II error.

\[
\beta_\varepsilon (\rho, \sigma) = \inf_{M_1, M_2 \geq 0} \left\{ \frac{\text{Tr} M_1 \sigma}{\text{Tr}(M_1 + M_2)\sigma} \right\} \left( M_1 + M_2 \leq \mathbb{1}, \frac{\text{Tr} M_2 \rho}{\text{Tr}(M_1 + M_2)\rho} \leq \varepsilon \right\},
\]

(24)

Our first result is to connect it with the Hilbert projective metric. We will frequently encounter the non-logarithmic variant of the latter, for which we introduce the notation

\[
\Omega(\rho\|\sigma) := 2^D_{\text{sym}}(\rho\|\sigma).
\]

(25)

**Theorem 1:** For all \( \varepsilon \in (0, 1) \), we have

\[
\beta_\varepsilon (\rho, \sigma) = \left( \frac{\varepsilon}{1 - \varepsilon} \Omega(\rho\|\sigma) + 1 \right)^{-1}.
\]

(26)

**Proof:** We begin by noticing that the constraint \( M_1 + M_2 \leq \mathbb{1} \) in (24) is superfluous: for all \( M_1, M_2 \geq 0 \) that satisfy \( \frac{\text{Tr}(M_1 + M_2)\rho}{\text{Tr}(M_1 + M_2)\rho} \leq \varepsilon \), one can always rescale them as \( M_1' := M_1/\|M_1 + M_2\|_\infty \) and they are then feasible for the original program with the same value of the objective function. Thus,

\[
\beta_\varepsilon (\rho, \sigma)^{-1} = \sup_{M_1, M_2 \geq 0} \left\{ \frac{\text{Tr}(M_1 + M_2)\sigma}{\text{Tr}(M_1 + M_2)\rho} \right\} \left( \frac{\text{Tr} M_2 \rho}{\text{Tr}(M_1 + M_2)\rho} \leq \varepsilon \right\}.
\]

(27)

In order to relate this optimisation with the Hilbert projective metric, we will use the dual form of the optimisation problem \( \Omega(\rho\|\sigma) \). Writing

\[
\Omega(\rho\|\sigma) = \Omega(\sigma\|\rho) = \inf \left\{ \gamma \in \mathbb{R}_+ \left| \sigma \leq \lambda \rho, \lambda \in \mathbb{R}_+ \right\} \right.,
\]

(28)

the dual optimisation problem can be obtained as [57]

\[
\Omega(\rho\|\sigma) = \sup \left\{ \frac{\text{Tr} A \sigma}{\text{Tr} B \sigma} \right| A, B \geq 0, \frac{\text{Tr} A \rho}{\text{Tr} B \rho} \leq 1 \right\}.
\]

(29)

The similarity between the two problems can be noticed by rewriting the objective function of (27) as

\[
\frac{\text{Tr}(M_1 + M_2)\sigma}{\text{Tr} M_1 \sigma} = 1 + \frac{\text{Tr} M_2 \sigma}{\text{Tr} M_1 \sigma}.
\]

(30)

To make the relation explicit, let \( M_1, M_2 \geq 0 \) be arbitrary operators feasible for (27), and define

\[
A := (1 - \varepsilon) M_2, B := \varepsilon M_1.
\]

(31)

Notice now that

\[
\frac{\text{Tr} A \rho}{\text{Tr} B \rho} = \frac{(1 - \varepsilon) \text{Tr} M_2 \rho}{\varepsilon \text{Tr} M_1 \rho} \leq 1,
\]

(32)

using the fact that

\[
\text{Tr} M_2 \rho/\text{Tr} M_1 \rho \leq \varepsilon \iff \frac{\text{Tr} M_1 \rho}{\text{Tr} M_2 \rho} \geq \frac{1 - \varepsilon}{\varepsilon}.
\]

(33)

\( A \) and \( B \) are therefore feasible operators for the dual optimisation problem for \( \Omega(\rho\|\sigma) \) in (29), giving

\[
\Omega(\rho\|\sigma) \geq \frac{1 - \varepsilon}{\varepsilon} \left( \text{Tr}[(M_1 + M_2)\sigma]/\text{Tr} M_1 \sigma \right) - 1.
\]

(34)

Working backwards through the above reasoning, we can analogously show that any feasible solution \{\( A, B \)\} for \( \Omega(\rho\|\sigma) \) in (29) gives a feasible solution \{\( M_1, M_2 \)\} for \( \beta_\varepsilon (\rho, \sigma)^{-1} \) in (27). The two problems are therefore equivalent, in the sense that

\[
\Omega(\rho\|\sigma) = \frac{1 - \varepsilon}{\varepsilon} \left( \beta_\varepsilon (\rho, \sigma)^{-1} - 1 \right),
\]

(35)

which is precisely the statement of the theorem. \( \blacksquare \)

1) Achievability: As long as \( \beta_\varepsilon (\rho, \sigma) \neq 0 \), i.e. \( \Omega(\rho\|\sigma) < \infty \), a measurement that achieves the optimal error \( \beta_\varepsilon (\rho, \sigma) \) can be readily constructed using the fact that \( D_{\text{max}}(\sigma\|\rho) = \log \left( \rho^{-1/2} \sigma^{-1/2} \right) \). Let \( |\psi_{\text{max}}\rangle \) and \( |\psi_{\text{min}}\rangle \) be eigenvectors corresponding, respectively, to the largest and the smallest non-zero eigenvalue of the operator \( \rho^{-1/2} \sigma^{-1/2} \). Then, define

\[
\tilde{M}_1 := \rho^{-1/2} |\psi_{\text{min}}\rangle \langle \psi_{\text{min}}| \rho^{-1/2},
\]

\[
\tilde{M}_2 := \rho^{-1/2} |\psi_{\text{max}}\rangle \langle \psi_{\text{max}}| \rho^{-1/2}.
\]

(36)

Now we only need to rescale these operators into a valid POVM, that is, define the three-outcome measurement

\[
M := \left\{ \frac{\tilde{M}_1}{\|\tilde{M}_1 + \tilde{M}_2\|_\infty}, \frac{\tilde{M}_2}{\|\tilde{M}_1 + \tilde{M}_2\|_\infty}, \mathbb{1} - \frac{\tilde{M}_1 + \tilde{M}_2}{\|\tilde{M}_1 + \tilde{M}_2\|_\infty} \right\}.
\]

(37)
It can be verified that $\pi(M) = \varepsilon$ and 
\[
\bar{\beta}(M) = \left(1 + \frac{\varepsilon}{1 - \varepsilon}\|\rho^{1/2} \sigma^{1/2}\|_{\infty} \|\sigma^{-1/2} \rho \sigma^{-1/2}\|_{\infty}\right)^{-1}
\]
\[
= \bar{\beta}_\varepsilon(\rho, \sigma),
\]
meaning that the measurement is indeed optimal.

An interesting point for the discrimination of many-copy states, i.e., $\rho^{\otimes n}$ and $\sigma^{\otimes n}$, is as follows. An optimal measurement strategy can readily be constructed following the above recipe; remarkably, the operational procedure corresponding to the measurement one obtains in this way is a product strategy, i.e., it involves separate measurements on each individual copy of the state, which is much simpler to implement from a practical and technological perspective. To see this, let us define a single-copy measurement similarly to (37), except that we replace $M_1$ and $M_2$ with 
\[
\bar{M}_1 := \frac{\rho^{1/2} |\psi_{\min}\rangle\langle\psi_{\min}| \rho^{1/2}}{\varepsilon^{1/n}},
\]
\[
\bar{M}_2 := \frac{\rho^{1/2} |\psi_{\max}\rangle\langle\psi_{\max}| \rho^{1/2}}{(1 - \varepsilon)^{1/n}}.
\]
(38)

We then measure each individual copy of $\rho$ or $\sigma$. If the outcome ‘1’ is obtained $n$ times, we guess $\rho^{\otimes n}$; if the outcome ‘2’ is obtained $n$ times, we guess $\sigma^{\otimes n}$; any other combination of outcomes is deemed inconclusive. Conditioned on a conclusive result, the probability of success of such a strategy is clearly the same as if we used the measurement (37) directly.

B. Asymptotic Error Exponent

The extension of Theorem 1 to the asymptotic setting is almost immediate. The crucial property of the Hilbert projective metric, and indeed also the Thompson metric, is that they are additive quantities: for all states $\rho$ and $\sigma$,
\[
D_{\Omega}(\rho^{\otimes n} |\sigma^{\otimes n}) = n D_{\Omega}(\rho |\sigma),
\]
\[
D_{\varepsilon}(\rho^{\otimes n} |\sigma^{\otimes n}) = n D_{\varepsilon}(\rho |\sigma).
\]
(39)

This follows from the additivity of $D_{\text{max}}$, which in turn follows directly from the definition and the fact that 
\[
\|\rho^{\otimes n} (\sigma^{\otimes n})^{-1/2}\|_{\infty} = \|\sigma^{-1/2} \rho \sigma^{-1/2}\|_{\infty}.
\]
(40)

Using this additivity and the two-sided inequality 
\[
\frac{\varepsilon}{1 - \varepsilon} \Omega(\rho |\sigma) \leq \bar{\beta}_\varepsilon(\rho, \sigma)^{-1} \leq \frac{1}{1 - \varepsilon} \Omega(\rho |\sigma),
\]
(41)
itself a consequence of the fact that $\Omega(\rho |\sigma) \geq 1$ for all $\rho, \sigma$, we obtain 
\[
n D_{\Omega}(\rho |\sigma) + \log \frac{\varepsilon}{1 - \varepsilon} \leq - \log \bar{\beta}_\varepsilon(\rho^{\otimes n} |\sigma^{\otimes n})
\]
\[
\leq n D_{\Omega}(\rho |\sigma) + \log \frac{1}{1 - \varepsilon}.
\]
(42)

This immediately yields an expression for the asymptotic error exponent, which is the equivalent of quantum Stein’s lemma in the setting of this work.

Corollary 2 (Asymptotic Error Exponent of Asymmetric Postselected Hypothesis Testing): For all $\varepsilon \in (0, 1)$, we have that 
\[
\lim_{n \to \infty} - \frac{1}{n} \log \bar{\beta}_\varepsilon(\rho^{\otimes n}, \sigma^{\otimes n}) = D_{\Omega}(\rho |\sigma).
\]
(43)

What is noteworthy about the expression in (42) is that there are no lower-order terms in $n$: the convergence to the asymptotic limit of Corollary 2 happens at least as fast as $O(1/n)$, which strongly contrasts with the case encountered in conventional quantum hypothesis testing [59], [60].

C. Properties of the Asymmetric Error

As the asymptotic error exponent is given exactly by $D_{\Omega}$, while the one-shot error $\bar{\beta}_\varepsilon$ is an inversely monotonic function of it, it suffices to characterise the properties of $D_{\Omega}$ to fully understand the behaviour of the errors in both the one-shot and exponential settings.

Proposition 3: For all states $\rho$ and $\sigma$, and for all $\varepsilon \in (0, 1)$:

(i) $D_{\Omega}(\rho |\sigma) \geq 0$, with equality if and only if $\rho = \sigma$. Consequently, $\bar{\beta}_\varepsilon(\rho, \sigma) \leq 1 - \varepsilon$, with equality if and only if $\rho = \sigma$.

(ii) Both $D_{\Omega}(\rho |\sigma)$ and $\bar{\beta}_\varepsilon(\rho, \sigma)$ are symmetric under the exchange of $\rho$ and $\sigma$, i.e., $D_{\Omega}(\rho |\sigma) = D_{\Omega}(\sigma |\rho)$ and $\bar{\beta}_\varepsilon(\rho, \sigma) = \bar{\beta}_\varepsilon(\sigma, \rho)$.

(iii) For all positive numbers $\lambda, \mu$, we have $D_{\Omega}(\lambda \rho |\mu \sigma) = D_{\Omega}(\lambda \rho |\mu \sigma)$, and analogously $\bar{\beta}_\varepsilon(\lambda \rho, \mu \sigma) = \bar{\beta}_\varepsilon(\lambda \rho, \mu \sigma)$.

(iv) $D_{\Omega}(\rho |\sigma) = \infty$ if and only if $\text{supp} \rho \neq \text{supp} \sigma$. Hence, $\bar{\beta}_\varepsilon(\rho, \sigma) = 0$ if and only if $\rho$ and $\sigma$ have non-identical supports.

(v) $D_{\Omega}$ satisfies the data-processing inequality under all positive maps; specifically, for every positive linear map $\mathcal{E}$,
\[
D_{\Omega}\left(\frac{\mathcal{E}(\rho)}{\text{Tr} \mathcal{E}(\rho)} \bigg\| \frac{\mathcal{E}(\sigma)}{\text{Tr} \mathcal{E}(\sigma)} \right) \leq D_{\Omega}(\mathcal{E}(\rho) |\mathcal{E}(\sigma))
\]
\[
\leq D_{\Omega}(\rho |\sigma).
\]
(44)

Hence, $\bar{\beta}_\varepsilon\left(\frac{\mathcal{E}(\rho)}{\text{Tr} \mathcal{E}(\rho)}, \frac{\mathcal{E}(\sigma)}{\text{Tr} \mathcal{E}(\sigma)}\right) \geq \bar{\beta}_\varepsilon(\rho, \sigma)$.

Proof: (i) holds because $\rho \leq \sigma$ and $\sigma \leq \rho$ can only be true if $\rho = \sigma$. (ii) is an immediate consequence of the manifestly symmetric definition (15), together with Theorem 1. (iii) follows from the fact that $D_{\text{max}}(\lambda \rho |\mu \sigma) = \log \frac{\lambda}{\mu} + D_{\text{max}}(\rho |\sigma)$, which is immediate from the definition. (iv) holds because $D_{\text{max}}(\rho |\sigma) < \infty$ if and only if $\text{supp} \rho \subseteq \text{supp} \sigma$. (v) is a consequence of (iii) coupled with the fact that for all $\lambda$ such that $\lambda \rho \leq \sigma$, the positivity of $\mathcal{E}$ ensures that $\mathcal{E}(\sigma) - \mathcal{E}(\rho) = \mathcal{E}(\lambda \sigma - \rho) \geq 0$, so $D_{\text{max}}(\mathcal{E}(\rho) |\mathcal{E}(\sigma)) \leq D_{\text{max}}(\rho |\sigma)$. □

Remark: The symmetry shown in Proposition 3(ii) is a priori highly non-obvious, and indeed one of the remarkable consequences of Theorem 1. Indeed, we started by looking at the error in asymmetric postselected hypothesis testing, but the expression we obtained is symmetric under the exchange of the two states. This can be understood as a consequence of the fact that, for all states $\rho, \sigma$ with $\text{supp} \rho = \text{supp} \sigma$,}
there exists a completely positive map $E$ such that $E(\rho) = \sigma$ and $E(\sigma) = k\rho$ for some $k \in (0, \infty)$ [54, Theorem 21]. Applying the data-processing inequality of Proposition 3(v) together with the scaling invariance (iii), we see that we must have $\beta_\epsilon (\rho|\sigma) = \beta_\epsilon (\sigma|\rho)$.

In all of the above, we have assumed that $\epsilon \in (0, 1)$. The case $\epsilon = 0$ requires a separate treatment.

**Proposition 4:** It holds that

$$\beta_0 (\rho, \sigma) = \begin{cases} 
1 & \text{supp } \sigma \subseteq \text{supp } \rho, \\
0 & \text{otherwise.}
\end{cases} (45)$$

**Proof:** If $\text{supp } \sigma \subseteq \text{supp } \rho$, then $\text{Tr } M_2 \sigma = 0$. Any feasible pair $\{M_1, M_2\}$ such that $\text{Tr } M_1 \sigma \neq 0$ then satisfies

$$\frac{\text{Tr } M_1 \sigma}{\text{Tr } [(M_1 + M_2) \sigma]} = \frac{\text{Tr } M_1 \sigma}{\text{Tr } M_1 \sigma} = 1. \ \ (46)$$

For the case $\text{supp } \sigma \not\subseteq \text{supp } \rho$, by hypothesis we know that there exists a pure state $\psi$ such that $\text{Tr } \psi \sigma > 0$ but $\text{Tr } \rho \psi = 0$. Pick $M_1 = 1 \mathbb{1}$, $M_2 = (1 - \delta) \psi$ for some $\delta \in (0, 1)$ to conclude that any value of

$$\frac{\text{Tr } M_1 \sigma}{\text{Tr } [(M_1 + M_2) \sigma]} = \frac{\delta}{\delta + (1 - \delta) \text{Tr } \psi \sigma} \ \ (47)$$

is achievable. Taking the limit $\delta \to 0$ gives the stated result. \hfill \blacksquare

It is a curious fact that $\beta_\epsilon (\rho, \sigma)$ is symmetric in its arguments for $\epsilon > 0$ (Proposition 3(ii)), but no longer so for $\epsilon = 0$. This asymmetry is due to the situation where $\text{supp } \sigma$ is strictly contained in $\text{supp } \rho$. In this case, $\rho$ can be distinguished from $\sigma$, but not the other way around: consider the POVM $\{1 - \Pi_n, 0, \Pi_n\}$ which allows us to conclude, whenever we obtain a conclusive outcome, that the state in our possession is $\rho$; however, the probability of a conclusive outcome when measuring $\sigma$ is zero. This problem is avoided for $\epsilon > 0$.

**D. Composite Postselected Hypothesis Testing**

In the setting of composite hypothesis testing, we wish to distinguish between a given state $\rho$ and a whole set of quantum states, denoted $F$. Let us first consider the case of conventional (non-postselected) hypothesis testing. Here, for a given measurement $M$, the performance is quantified with the worst-case type II error, i.e.

$$\beta_{\epsilon, F}(M) := \sup_{\sigma \in F} \beta(\sigma) = \sup_{\sigma \in F} \text{Tr } M_1 \sigma, \ \ (48)$$

and the optimised error is defined as $\beta_{\epsilon, F}(\rho) := \inf_{\sigma \in F} \left\{ \beta_{\epsilon, F}(M) : \alpha(M) \leq \epsilon \right\}$. Brandão and Plenio [15] conjectured a remarkable extension of the quantum Stein’s lemma to composite hypothesis testing: namely, that for every family of sets $(F_n)_n$ satisfying a small number of regularity properties (including convexity and closedness under tensor product, partial trace, and permutations of systems), it holds that

$$\lim_{n \to \infty} -\frac{1}{n} \log \beta_{\epsilon, F_n}(\rho^{\otimes n}) \geq D_{\xi}^\infty (\rho), (49)$$

where $D_{\xi}^\infty$ is the regularised relative entropy, $D_{\xi}^\infty (\rho) := \lim_{n \to \infty} \frac{1}{n} \min_{\sigma_n \in F_n} D(\rho^{\otimes n} \| \sigma_n)$. Although a proof of this result was claimed in [15], issues with the derivation were recently uncovered [16], and (49) is therefore not known to hold in general.

We show that an analogue of the above result holds true in the setting of postselected hypothesis testing. To this end, define

$$\beta_{\epsilon, F}(\rho) := \inf_{M \in M_1} \left\{ \beta_{\epsilon, F}(M) : \alpha(M) \leq \epsilon \right\} = \inf_{M_1, M_2 \geq 0} \left\{ \sup_{\sigma \in F} \frac{\text{Tr } M_1 \sigma}{\text{Tr } [(M_1 + M_2) \sigma]} : M_1 + M_2 \leq 1, \ \ \frac{\text{Tr } M_2 \rho}{\text{Tr } [(M_1 + M_2) \rho]} \leq \epsilon \right\} \ \ (50)$$

We then show that the asymptotic error exponent of composite postselected hypothesis testing is given exactly by the regularisation of the Hilbert projective metric $D_{\Omega}(\rho\|\sigma)$ optimised over the sets $F_n$.

**Theorem 5:** For every convex and closed set of quantum states $F$,

$$\beta_{\epsilon, F}(\rho) = \left( \frac{\epsilon}{1 - \epsilon} \min_{\sigma \in F} \Omega(\rho\|\sigma) + 1 \right)^{-1}. \ \ (51)$$

As a consequence, for every family of sets $(F_n)_n$ that are convex and closed, we have that

$$\liminf_{n \to \infty} -\frac{1}{n} \log \beta_{\epsilon, F_n}(\rho^{\otimes n}) = D_{\Omega}^\infty (\rho), \ \ (52)$$

where

$$D_{\Omega}^\infty (\rho) = \liminf_{n \to \infty} \frac{1}{n} \min_{\sigma_n \in F_n} D_{\Omega}(\rho^{\otimes n}\|\sigma_n). \ \ (53)$$

If the sets $(F_n)_n$ are closed under tensor product, i.e. if $\sigma_n \otimes \sigma_m \in F_{n+m}$ for all $\sigma_n \in F_n$ and $\sigma_m \in F_m$, then $\liminf$ in (52)–(53) can be replaced with $\lim$, because the limits are achieved.

We remark here that the quantity $\min_{\sigma \in F} \Omega(\rho\|\sigma)$ can be computed as the optimal value of a conic linear optimisation problem [57]; when membership in the set $F$ can be expressed using linear matrix inequalities, this reduces to a semidefinite program.

**Proof:** The basic idea is exactly the same as in the proof of Theorem 1. Let us first consider the one-shot case. We have that

$$\beta_{\epsilon, F}(\rho) \overset{(w)}{=} \inf_{M_1, M_2 \geq 0} \left\{ \sup_{\sigma \in F} \frac{\text{Tr } M_1 \sigma}{\text{Tr } [(M_1 + M_2) \sigma]} : \frac{\text{Tr } M_2 \rho}{\text{Tr } [(M_1 + M_2) \rho]} \leq \epsilon \right\}$$

$$\overset{(w)}{=} \inf_{M_1, M_2 \geq 0} \left\{ \frac{\text{Tr } M_1 \sigma}{\text{Tr } [(M_1 + M_2) \sigma]} : \frac{\text{Tr } M_2 \rho}{\text{Tr } [(M_1 + M_2) \rho]} \leq \epsilon \right\}$$

$$\overset{(w)}{=} \inf_{t \geq 0} \left\{ \frac{\text{Tr } M_2 \sigma}{\text{Tr } M_1 \sigma} > \frac{1}{t} - 1 : \forall \sigma \in F, \right\}$$

$$\overset{(w)}{=} \inf_{t \geq 0} \left\{ \frac{\text{Tr } M_2 \sigma}{\text{Tr } M_1 \sigma} > \frac{1}{t} - 1 : \forall \sigma \in F, \right\}$$

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
established an interesting connection between quantum hypothesis testing and operational aspects of quantum resource transformations. It was shown, in particular, that the asymptotic error exponent in (conventional) asymmetric hypothesis testing (Eq. (49)) gives exactly the rate at which quantum entanglement can be distilled, i.e. converted to pure maximally entangled states, under the class of non-entangling quantum channels. This relation is mirrored exactly in postselected hypothesis testing: the quantity $D_{\Omega}^{\text{err}}(\rho)$ in Theorem 5 was recently shown to give the rate of distillation under probabilistic non-entangling operations [56], and here we have shown that it is also precisely the asymptotic error exponent.

### III. Symmetric Case

#### A. One-Shot Symmetric Hypothesis Testing Error

Consider the discrimination of two states, $\rho$ and $\sigma$, with their respective priors being $p$ and $q$. Let us recall the definition of the postselected probability of error $\overline{p}_{\text{err}}$:

$$
\overline{p}_{\text{err}}(\rho, \sigma | p, q) = \frac{\inf_{M_1, M_2 \geq 0, M_1 + M_2 \leq 1} \{ \frac{\text{Tr} M_1 \rho}{\text{Tr} M_2 \sigma} \} \geq 1 - \varepsilon \forall \sigma \in \mathcal{F},}
$$

therefore, the asymptotic properties of this quantity were not studied, nor was its relation with the Thompson metric observed.

Our first result establishes that the one-shot postselected discrimination error is given by a simple function of the Thompson metric, or rather its non-logarithmic variant

$$
\Xi(\rho \| \sigma) := 2D_{\Xi}(\rho \| \sigma).
$$

Note that below we will apply the Thompson metric also to rescaled quantum states as $\Xi(\rho p \| \sigma q)$. In such a case, we use the exact same definition of the max-relative entropy as for normalised states, which gives

$$
D_{\text{max}}(\rho \| \sigma) = \log \inf \left\{ \lambda \in \mathbb{R}^+ \mid p \lambda \leq q \lambda \right\} = \frac{p}{q} + D_{\text{max}}(\rho \| \sigma).
$$

**Theorem 6:** For all states $\rho, \sigma$ and for all priors $p, q = 1 - p \in (0, 1)$, we have

$$
\overline{p}_{\text{err}}(\rho, \sigma | p, q) = \left( \Xi(\rho p \| \sigma q) + 1 \right)^{-1}.
$$

**Proof:** We first derive the dual formulation of the Thompson metric. Writing

$$
\Xi(\rho p \| \sigma q) = \inf \left\{ \max \left\{ \lambda_1, \lambda_2 \right\} \mid \frac{1}{\lambda_1} q \sigma \leq p \rho \leq \lambda_2 q \sigma \right\}
$$

In addition to the conjectured generalisation of quantum Stein’s lemma, the works of Brandão and Plenio [15], [62]
we obtain the dual program as
\[
\Xi(p\rho\|q\sigma) = \sup \left\{ q \Tr A\sigma + p \Tr B\rho \bigg| A, B \geq 0, q \Tr B\sigma + p \Tr A\rho = 1 \right\}
\]
\[
= \sup_{A, B \geq 0} \frac{q \Tr A\sigma + p \Tr B\rho}{q \Tr B\sigma + p \Tr A\rho}.
\tag{65}
\]

The fact that we were justified in claiming that the optimal value of \eqref{64} equals the optimal value of \eqref{65} follows from the strong duality of the optimisation problem, easily seen by noticing that \(A = B = 1\) are strongly feasible solutions and invoking Slater’s theorem \cite[Thm. 28.2]{63}.

As before, we see that the constraint \(M_1 + M_2 \leq 1\) in the definition of \(\overline{\mathcal{P}}_{\text{err}}\) is superfluous and we can ignore it without loss of generality. Notice then that
\[
\overline{\mathcal{P}}_{\text{err}}(\rho, \sigma \mid p, q)^{-1}
= \sup_{M_1, M_2 \geq 0} \frac{q \Tr [(M_1 + M_2)\sigma] + p \Tr [(M_1 + M_2)\rho]}{q \Tr M_1\sigma + p \Tr M_2\rho}
= \sup_{M_1, M_2 \geq 0} \left( 1 + \frac{q \Tr M_2\sigma + p \Tr M_1\rho}{q \Tr M_1\sigma + p \Tr M_2\rho} \right)
= (1 + \Xi(p\rho\|q\sigma)),
\tag{66}
\]

For large enough \(n\), the maximum on the right-hand side will be determined only by the maximum between \(D_{\text{max}}(\rho\|\sigma)\) and \(D_{\text{max}}(\sigma\|\rho)\), which implies that
\[
\lim_{n \to \infty} \frac{1}{n} D_{\Xi}(p\rho^{\otimes n}\|q\sigma^{\otimes n}) = D_{\Xi}(\rho\|\sigma),
\tag{70}
\]
as long as the priors \(p, q\) are non-zero. Theorem 6 then immediately gives the asymptotic regularisation of the symmetric distinguishability error.

**Corollary 7 (Asymptotic Error Exponent of Symmetric Postselected Hypothesis Testing):** For all states \(\rho, \sigma\) and for all priors \(p, q = 1 - p \in (0, 1)\),
\[
\lim_{n \to \infty} \frac{1}{n} \log \overline{\mathcal{P}}_{\text{err}}(\rho^{\otimes n}, \sigma^{\otimes n} \mid p, q) = D_{\Xi}(\rho\|\sigma).
\tag{71}
\]

As in the asymmetric case, the expression for \(-\log \overline{\mathcal{P}}_{\text{err}}(\rho^{\otimes n}, \sigma^{\otimes n} \mid p, q)\) contains no \(n\)-dependent terms of order lower than 1. Furthermore, and again in analogy with what happens in the asymmetric case, there is a product strategy achieving the asymptotically optimal conditional error probability in symmetric discrimination. It consists in making the measurement \(\{M_1, M_2, M_3\}\) detailed in \eqref{68} on each copy of the state, guessing \(\rho\) if the outcome ‘1’ is obtained \(n\) times, and declaring an inconclusive result in any other case.

Finally, we remark that the exact expression for many-copy discrimination error simplifies slightly for the case \(p = q = \frac{1}{2}\), where the fact that \(D_{\Xi}(\rho^{\otimes n}\|\sigma^{\otimes n}) = n D_{\Xi}(\rho\|\sigma)\) yields
\[
-\log \overline{\mathcal{P}}_{\text{err}}(\rho^{\otimes n}, \sigma^{\otimes n} \mid \frac{1}{2}, \frac{1}{2}) = \log (\Xi(\rho\|\sigma)^n + 1)
\tag{72}
\]
for every \(n\).

**C. Properties of the Symmetric Error**

**Proposition 8:** For all states \(\rho\) and \(\sigma\), and all priors \(p, q = 1 - p \in (0, 1)\):

(i) \(D_{\Xi}(p\rho\|q\sigma) \geq 0\), with equality if and only if \(\rho = \sigma\) and \(p = q\). Hence, \(\overline{\mathcal{P}}_{\text{err}}(\rho, \sigma \mid p, q) \leq \frac{1}{2}\), with equality if and only if \(\rho = \sigma\) and \(p = q\).

(ii) \(D_{\Xi}(p\rho\|q\sigma) = \infty\) if and only if \(\supp \rho \neq \supp \sigma\). Hence, \(\overline{\mathcal{P}}_{\text{err}}(\rho, \sigma \mid p, q) = 0\) if and only if \(\rho\) and \(\sigma\) have different supports.

(iii) For every positive linear map \(E\), the inequality \(D_{\Xi}(pE(\rho)\|qE(\sigma)) \leq D_{\Xi}(p\rho\|q\sigma)\) holds true.

We note that our conclusion in point (ii) was previously shown in \cite{40}.

**Proof:** (i) follows from the fact that \(p\rho \leq q\sigma\) and \(p\rho \geq q\sigma\) can both be true iff \(p\rho = q\sigma\), which is possible if and only if \(p = q\) and \(\rho = \sigma\) due to \(\rho\) and \(\sigma\) being normalised states. (ii) is a consequence of the fact that \(D_{\text{max}}(\rho\|\sigma) < \infty \iff \supp \rho \subseteq \supp \sigma\). (iii) is immediate because \(E(\lambda p\rho - p\sigma) = \lambda E(\rho) - pE(\sigma) \geq 0\) for every \(\lambda\) such that \(pp \leq \lambda q\sigma\) due to the positivity of \(E\).
asymmetric error. Indeed, in such a case we only get the inequality
\[
\Xi \left( \frac{\mathcal{E}(\rho)}{\operatorname{Tr} \mathcal{E}(\rho)}, \frac{\mathcal{E}(\sigma)}{\operatorname{Tr} \mathcal{E}(\sigma)} \right) \leq \max \left\{ \frac{\operatorname{Tr} \mathcal{E}(\sigma)}{\operatorname{Tr} \mathcal{E}(\rho)}, \frac{\mathcal{E}(\rho)}{\operatorname{Tr} \mathcal{E}(\sigma)} \right\} \Xi(q \sigma | p \rho) . \tag{73}
\]

To see that \( \Xi \left( \frac{\mathcal{E}(\rho)}{\operatorname{Tr} \mathcal{E}(\rho)}, \frac{\mathcal{E}(\sigma)}{\operatorname{Tr} \mathcal{E}(\sigma)} \right) \leq \Xi(\rho | \sigma) \) in general, consider e.g. \( \rho = \begin{pmatrix} 2/3 & 0 \\ 0 & 1/3 \end{pmatrix} \) and \( \sigma = 1/2 \), in which case it is easy to verify that \( \Xi(\rho | \sigma) = 3/2 \). Setting \( \mathcal{E}(\cdot) := D(\cdot) D \) with \( D := \begin{pmatrix} \sqrt{\gamma} & 0 \\ 0 & 1/\sqrt{\gamma} \end{pmatrix} \) and \( \gamma < 1 \), we find
\[
\Xi \left( \frac{\mathcal{E}(\rho)}{\operatorname{Tr} \mathcal{E}(\rho)}, \frac{\mathcal{E}(\sigma)}{\operatorname{Tr} \mathcal{E}(\sigma)} \right) = \frac{2\gamma^2 + 1}{\gamma^2 + 1} > 3/2 = \Xi(\rho | \sigma) .
\]

IV. QUANTUM CHANNEL DISCRIMINATION

A. One-Shot Channel Hypothesis Testing

We will now consider quantum channels, that is, completely positive and trace-preserving (CPTP) linear maps acting between the spaces of operators on the Hilbert spaces of two quantum systems, \( A \) and \( B \). We denote such channels as \( M : A \to B \). Completeness property refers here to the property that not only is the map \( M \) positive, i.e. it maps positive operators to positive operators, but so is \( \text{id} \otimes M \), where \( \text{id} \) denotes the identity channel on an ancillary space of an arbitrary dimension. The set of quantum states of systems \( A \) and \( B \) will be denoted \( \mathcal{D}_A \) and \( \mathcal{D}_B \), respectively.

If we only have access to a single copy of two channels \( M, N : A \to B \), there is only one thing we can do to discriminate them: feed in some state \( \rho \) into the channel, and then perform a distinguishing measurement at the output. However, a crucial insight here is that using a larger, entangled state and measurement can help discriminate the channels better than simply measuring \( N(\rho) \) for some \( \rho \in \mathcal{D}_A \). Because of this, one performs channel hypothesis testing by measuring \( \text{id} \otimes M(\rho) \) for some state \( \rho \in \mathcal{D}_R A \), where the ancillary space \( R \) is arbitrary. We therefore define the postselected asymmetric and symmetric hypothesis testing errors as
\[
\overline{\beta}(M, N) := \inf_{\rho \in \mathcal{D}_R A} \overline{\beta}(\text{id} \otimes M(\rho), \text{id} \otimes N(\rho) ) ,
\]
\[
\overline{p}_{\text{err}}(M, N | p, q) := \inf_{\rho \in \mathcal{D}_R A} \overline{p}_{\text{err}}(\text{id} \otimes M(\rho), \text{id} \otimes N(\rho) | p, q) . \tag{74}
\]

From Theorems 1 and 6, we immediately have that
\[
\overline{\beta}(M, N) = \inf_{\rho \in \mathcal{D}_R A} \left[ \frac{\varepsilon}{1 - \varepsilon} \Omega(\text{id} \otimes M(\rho) | \text{id} \otimes N(\rho)) + 1 \right]^{-1} , 
\]
\[
\overline{p}_{\text{err}}(M, N | p, q) = \inf_{\rho \in \mathcal{D}_R A} \left[ \Xi(p \text{id} \otimes M(\rho) | q \text{id} \otimes N(\rho)) + 1 \right]^{-1} . \tag{75}
\]

B. Asymptotic Channel Hypothesis Testing

When given \( n \) uses of a channel, the basic strategy is the so-called parallel channel discrimination, which simply puts the channel to be discriminated in a tensor product \( M \otimes n \) and

It may not be immediately obvious if these optimisation problems can be evaluated. However, by exploiting a property of the max-relative entropy noticed in [22], we can show that it suffices to take as input the maximally entangled state \( \Phi^+ = \Phi^+ \Phi^+ \) with \( \Phi^+ = \frac{1}{\sqrt{d}} \sum_{i=1}^d | i i \rangle \), which reduces the problem to evaluating \( D_{\max} \) between two fixed states. We state this in the form of the following lemma.

Lemma 9: For all channels \( M, N : A \to B \), define
\[
\Omega(M | N) := \sup_{\rho \in \mathcal{D}_R A} \Omega(\text{id} \otimes M(\rho) | \text{id} \otimes N(\rho))
\]
\[
\Xi(M | N) := \sup_{\rho \in \mathcal{D}_R A} \Xi(\text{id} \otimes M(\rho) | \text{id} \otimes N(\rho)) . \tag{76}
\]

Then,
\[
\Omega(M | N) = \Omega(J_M | J_N) ,
\]
\[
\Xi(M | N) = \Xi(J_M | J_N) , \tag{77}
\]

where \( J_M \) and \( J_N \) denote the Choi states of the channels, defined as \( J_M := \text{id} \otimes M(\Phi^+) \).

Proof: We will consider the Hilbert projective metric \( \Omega \), with the case of the Thompson metric \( \Xi \) being analogous.

First, the bound \( \Omega(M | N) \geq \Omega(J_M | J_N) \) follows from the definition. For the other direction, observe that for any state \( \rho \) it holds that
\[
D_{\Omega}(\text{id} \otimes M(\rho) | \text{id} \otimes N(\rho)) = D_{\max}(\text{id} \otimes M(\rho) | \text{id} \otimes N(\rho)) + D_{\max}(\text{id} \otimes N(\rho) | \text{id} \otimes M(\rho)) \leq \sup_{\rho'} D_{\max}(\text{id} \otimes M(\rho) | \text{id} \otimes N(\rho)) + \sup_{\rho'} D_{\max}(\text{id} \otimes N(\rho') | \text{id} \otimes M(\rho')) = D_{\max}(J_M | J_N) + D_{\max}(J_N | J_M) = D_{\Omega}(J_M | J_N) , \tag{78}
\]

where the second-to-last line follows because
\[
\sup_{\rho'} D_{\max}(\text{id} \otimes M(\rho) | \text{id} \otimes N(\rho)) = D_{\max}(J_M | J_N) \tag{79}
\]
holds for all channels \( M, N \) [22, Lemma 12]. Since this upper bound applies to any \( \rho \), it holds also for the supremum, thus matching the lower bound.

Lemma 9 then immediately gives the following result, which establishes closed-form expressions for the asymmetric and symmetric error in postselected channel hypothesis testing.

Corollary 10: For all \( \varepsilon \in (0, 1) \) and \( p, q = 1 - p \in (0, 1) \), we have that
\[
\overline{\beta}(M, N) = \left( \frac{\varepsilon}{1 - \varepsilon} \Omega(J_M | J_N) + 1 \right)^{-1} ,
\]
\[
\overline{p}_{\text{err}}(M, N | p, q) = \left( \Xi(p J_M | q J_N) + 1 \right)^{-1} . \tag{80}
\]
optimises over all input states and measurements. Let us then define the $n$-copy parallel distinguishability errors as

$$\overline{\beta}_{err}^{\parallel} \left( \mathcal{M}, \mathcal{N} \mid n \right)$$

$$\begin{array}{rcl}
& := & \inf_{\rho \in D_{R^{\otimes n}}} \overline{\beta}_{err} \left( \mathcal{M}^{\otimes n}, \mathcal{N}^{\otimes n} \mid \rho \right), \\
& := & \inf_{\rho \in D_{R^{\otimes n}}} \overline{\beta}_{err} \left( \mathcal{M}^{\otimes n}, \mathcal{N}^{\otimes n} \mid \rho \right) \left( \rho \otimes \mathcal{N}^{\otimes n} \right), \\
& := & \inf_{\rho \in D_{R^{\otimes n}}} \overline{\beta}_{err} \left( \mathcal{M}^{\otimes n}, \mathcal{N}^{\otimes n} \mid \rho \right) \left( \rho \otimes \mathcal{N}^{\otimes n} \right) \mid p, q, n \right), \quad (81)
\end{array}$$

where the ancillary space $R$ is a priori arbitrary. We stress that, although the channels are in a tensor product as $\mathcal{M}^{\otimes n}$ and $\mathcal{N}^{\otimes n}$, the input states $\rho$ may be entangled, and the measurements at the output may be joint over all systems. Exact expressions for these quantities follow immediately from Corollary 10, showing also that it suffices to take the $n$-copy maximally entangled input state $\Phi^{\otimes n}$ in the above. In particular, no entanglement between different copies is required in the preparation of the optimal input states. Furthermore, due to the discussion in Sections II-A and III-B, we know that also joint measurements at the output may be joint over all systems.

To consider more general channel discrimination schemes, most works employ the formalism of adaptive discrimination schemes [21], [22], [25], [34], [65], [66], [67]. However, as we mentioned previously, it is known that broader types of channel manipulation protocols — in particular, ones that use more exotic transformation structures such as superposition of causal orders — can provide advantages over adaptive protocols [28], [30], [31], [32]. We will therefore aim to characterise the most general protocols allowed by the laws of quantum physics, without assuming anything whatsoever about their structure.

To discuss a general $n$-channel manipulation protocol, let us consider an $n$-linear map $\Upsilon$ that takes $n$ channels as input and outputs a single quantum state. Specifically, using $(A \rightarrow B)$ to denote the space of all linear maps from $A$ to $B$, the map $\Upsilon$ can be considered as a map from the space $(A \rightarrow B)^{\otimes n}$ to $(C \rightarrow R)$, where the latter is just the space of linear operators on some quantum system $R$ of arbitrary dimension. In order for $\Upsilon$ to be a valid channel transformation, we assume that it satisfies

$$M_1, \ldots, M_n \in \text{CP}(A \rightarrow B) \Rightarrow \Upsilon(\mathcal{M}_1, \ldots, \mathcal{M}_n) \geq 0,$$

(82)

with $\text{CP}(A \rightarrow B)$ denoting the set of all completely positive maps between the two spaces. That is, the sole assumption we make is that the map $\Upsilon$ is positive: it maps any $n$-tuple of completely positive maps into a positive operator. We do not enforce any form of complete positivity of this transformation, nor do we assume normalisation (trace preservation). By construction, any adaptive protocol is included under such a definition. We will use $\mathbb{P}_n$ to denote the set of all $n$-linear maps $\Upsilon : (A \rightarrow B)^{\otimes n} \rightarrow (C \rightarrow R)$ satisfying (82).

We then define

$$\overline{\beta}_{err}^{\text{any}} \left( \mathcal{M}, \mathcal{N} \mid n \right)$$

$$\begin{array}{rcl}
& := & \inf_{\Upsilon \in \mathbb{P}_n} \overline{\beta}_{err} \left( \Upsilon(\mathcal{M}^{\otimes n}), \Upsilon(\mathcal{N}^{\otimes n}) \mid \rho \right), \\
& := & \inf_{\Upsilon \in \mathbb{P}_n} \overline{\beta}_{err} \left( \Upsilon(\mathcal{M}^{\otimes n}), \Upsilon(\mathcal{N}^{\otimes n}) \mid p, q, n \right), \quad (83)
\end{array}$$

where $\mathcal{M}^{\otimes n}$ denotes the $n$-tuple $(\mathcal{M}, \ldots, \mathcal{M})$. With these definitions in place, we are ready to state our main result on channel discrimination.

**Theorem 11.** For all $n \in \mathbb{N}$, we have that

$$\overline{\beta}_{err}^{\text{any}} \left( \mathcal{M}, \mathcal{N} \mid n \right) = \overline{\beta}_{err}^{\parallel} \left( \mathcal{M}, \mathcal{N} \mid n \right),$$

$$\overline{\beta}_{err}^{\text{any}} \left( \mathcal{M}, \mathcal{N} \mid p, q, n \right) = \overline{\beta}_{err}^{\parallel} \left( \mathcal{M}, \mathcal{N} \mid p, q, n \right). \quad (84)$$

In particular, the asymptotic exponent of asymmetric postselected channel discrimination is given by the Hilbert projective metric between the Choi operators of the channels, regardless of whether only parallel or any general discrimination schemes are employed: for all $\varepsilon \in (0, 1),

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \overline{\beta}_{err}^{\text{any}} \left( \mathcal{M}, \mathcal{N} \mid n \right)$$

$$\begin{array}{rcl}
& = & \lim_{n \rightarrow \infty} -\frac{1}{n} \log \overline{\beta}_{err}^{\parallel} \left( \mathcal{M}, \mathcal{N} \mid n \right) \\
& = & D_{\Omega}(M \| N) \\
& = & D_{\Omega}(J_M \| J_N). \quad (85)
\end{array}$$

Similarly, for all types of discrimination protocols, the asymptotic exponent of symmetric postselected channel discrimination is given by the Thompson metric between the Choi operators of the channels. That is, for all priors $p, q = 1 - p \in (0, 1),

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \overline{\beta}_{err}^{\text{any}} \left( \mathcal{M}, \mathcal{N} \mid p, q, n \right)$$

$$\begin{array}{rcl}
& = & \lim_{n \rightarrow \infty} -\frac{1}{n} \log \overline{\beta}_{err}^{\parallel} \left( \mathcal{M}, \mathcal{N} \mid p, q, n \right) \\
& = & D_{\Xi}(M \| N) \\
& = & D_{\Xi}(J_M \| J_N). \quad (86)
\end{array}$$

The result establishes a complete equivalence of parallel discrimination strategies and more general protocols, not only at the asymptotic level but also for any finite number of channel uses. The computation of the asymmetric (Stein) exponent is an analogue of a corresponding result in conventional discrimination of quantum channels [22], [23], [24], but strictly stronger: Theorem 11 applies even beyond adaptive discrimination strategies, and furthermore proves the strong converse property of postselected channel discrimination, which is not known to hold in the conventional setting. The evaluation of the symmetric (Chernoff) exponent has no known analogue in conventional hypothesis testing of quantum channels.
The equalities in the above follow from Corollary 10.

For the other direction, we employ the result of
[68, Theorem 13], which states that

\[
D_{\text{max}}(\Upsilon(M^\times n)\|\Upsilon(N^\times n)) \leq n D_{\text{max}}(J_M\|J_N). \tag{88}
\]

for every \(\Upsilon \in \mathbb{P}_n\). To see that Eq. (88) is true, and in particular that the assumptions of linearity and positivity of the channel transformations are sufficient, consider any feasible \(\lambda\) such that \(J_M \leq \lambda J_N\), i.e. \(\lambda N - M\) is a completely positive map. We can then follow [68] by writing

\[
\begin{align*}
\lambda^n \Upsilon(N, \ldots, N) &= \Upsilon(\lambda N, \ldots, \lambda N) \\
&= \Upsilon(\lambda N - M, \lambda N, \ldots, \lambda N) + \Upsilon(M, \lambda N, \ldots, \lambda N) \\
&= \Upsilon(\lambda N - M, \lambda N, \ldots, \lambda N) \\
&\quad + \Upsilon(M, \lambda N - M, \lambda N, \ldots, \lambda N) \\
&\quad + \Upsilon(M, M, \lambda N, \ldots, \lambda N) \\
&\quad \vdots \\
&= \Upsilon(\lambda N - M, \lambda N, \ldots, \lambda N) \\
&\quad + \ldots + \Upsilon(M, M, M, M, \lambda N - M) \\
&\quad + \Upsilon(M, M, \ldots, M),
\end{align*}
\]

where we only used the \(n\)-linearity of \(\Upsilon\). By the properties of \(\mathbb{P}_n\) (Eq. (82)), all of the terms on the right-hand side are positive operators, ensuring that \(\lambda^n \Upsilon(N, \ldots, N) \geq \Upsilon(M, \ldots, M)\) and thus \(D_{\text{max}}(\Upsilon(M^\times n)\|\Upsilon(N^\times n)) \leq n \log \lambda\). Optimising over all feasible \(\lambda\) gives Eq. (88).

We thus get

\[
\begin{align*}
\beta_{\epsilon}^{\text{any}}(M, N | n) &= \inf_{\Upsilon \in \mathbb{P}_n} \left( \frac{\epsilon}{1 - \epsilon} \Omega(\Upsilon(M^\times n)\|\Upsilon(N^\times n)) + 1 \right)^{-1} \\
&\geq \left( \frac{\epsilon}{1 - \epsilon} \Omega(J_M\|J_N) + 1 \right)^{-1} \\
&= \left( \frac{\epsilon}{1 - \epsilon} \Omega(J_M^\otimes n\|J_N^\otimes n) + 1 \right)^{-1} \\
&= \beta_{\epsilon}^{\text{parallel}}(M, N | n),
\end{align*}
\]

where we used the additivity property

\[
D_{\text{max}}(J_M^\otimes n\|J_N^\otimes n) = D_{\text{max}}(J_M^\otimes n\|J_N^\otimes n) = n D_{\text{max}}(J_M\|J_N). \tag{90}
\]

Analogously,

\[
\begin{align*}
\beta_{\epsilon,\mathcal{F}}^{\text{any}}(M, N | p, q | n) &= \inf_{\Upsilon \in \mathbb{P}_n} \left( p \Upsilon(M^\times n)\|q \Upsilon(N^\times n)) + 1 \right)^{-1} \\
&\geq \left( \max \left\{ \frac{p}{q} D_{\text{max}}(J_M\|J_N), \frac{q}{p} D_{\text{max}}(J_M\|J_N) \right\} + 1 \right)^{-1} \\
&= \beta_{\epsilon,\mathcal{F}}^{\text{parallel}}(M, N | p, q | n).
\end{align*}
\]

C. Composite Channel Hypothesis Testing

The case of composite channel discrimination can be considered very similarly. Given some subset of channels \(\mathcal{F} \subseteq \text{CPTP}(A \rightarrow B)\), we define

\[
\begin{align*}
\beta_{\epsilon,\mathcal{F}}(M) := \inf_{\rho \in \text{D}_{\text{RA}}} & \inf_{M_1, M_2 \geq 0} \left\{ \sup_{N \in \mathcal{F}} \frac{\text{Tr} M_1 (\text{id} \otimes N(\rho))}{\text{Tr} [(M_1 + M_2)(\text{id} \otimes N(\rho))]} \right\} \\
&\quad \frac{\text{Tr} M_2 (\text{id} \otimes M(\rho))}{\text{Tr} [(M_1 + M_2)(\text{id} \otimes M(\rho))]} \leq \epsilon \}
\end{align*}
\]

Using the result for the state case (Theorem 5), we immediately get that

\[
\beta_{\epsilon,\mathcal{F}}(M) = \left( \frac{\epsilon}{1 - \epsilon} \Omega_{\mathcal{F}}(M) + 1 \right)^{-1}, \tag{94}
\]

where

\[
\Omega_{\mathcal{F}}(M) := \sup_{\rho \in \text{D}_{\text{RA}}} \inf_{N \in \mathcal{F}} \Omega(\text{id} \otimes M(\rho)\|\text{id} \otimes N(\rho)). \tag{95}
\]

The following Lemma can then be established in full analogy with Lemma 9.

**Lemma 12:** Let \(\mathcal{M} : A \rightarrow B\) be a channel and \(\mathcal{F}\) a convex and closed set of quantum channels. Then

\[
\Omega_{\mathcal{F}}(M) = \min_{N \in \mathcal{F}} \Omega(J_M\|J_N). \tag{96}
\]

As a consequence, we obtain the following generalisation of quantum Stein’s lemma for parallel quantum channel discrimination.

**Corollary 13:** For all \(\epsilon \in (0, 1)\), every channel \(\mathcal{M} : A \rightarrow B\), and every family \((\mathcal{F}_n)_n\) of convex and closed sets \(\mathcal{F}_n \subseteq \text{CPTP}(A^\otimes n \rightarrow B^\otimes n)\), we have

\[
\lim_{n \rightarrow \infty} \inf \frac{1}{n} \log \beta_{\epsilon,\mathcal{F}}(M^\otimes n) = D_{\Omega_{\mathcal{F}}}^{\otimes n}(M) \tag{97}
\]

where

\[
D_{\Omega_{\mathcal{F}}}^{\otimes n}(M) = \lim_{n \rightarrow \infty} \frac{1}{n} \min_{N \in \mathcal{F}} D_{\Omega} \left( J_M^\otimes n \| J_N^\otimes n \right). \tag{98}
\]

If the sets \(\mathcal{F}_n\) are closed under tensor product, i.e. \(N_n \in \mathcal{F}_n, N_m \in \mathcal{F}_m \Rightarrow N_n \otimes N_m \in \mathcal{F}_{n+m}\), then \(\lim \inf\) can be replaced with \(\lim\) in the above.
V. Resource Theory of Asymmetric Distinguishability

The resource theory of asymmetric distinguishability was introduced in [69] and [70] as a way to treat the distinguishability of quantum states operationally. Just as general resource theories [71] are concerned with transforming quantum states under some set of restricted, ‘free’ operations, the theory of distinguishability studies the transformations of pairs of quantum states (‘boxes’) under channels that act as \((\rho, \sigma) \rightarrow (\mathcal{M}(\rho), \mathcal{M}(\sigma))\), and therefore do not increase the distinguishability between the two states. The standard resourceful box, representing a unit of ‘perfect distinguishability’, is represented by the pair \(|0\rangle\langle 0| \otimes \frac{1}{2} \mathbb{I}_2\). In this context, the task of distinguishability distillation was defined as transforming a given box \(|0\rangle\langle 0| \otimes \frac{1}{2} \mathbb{I}_2\) into tensor powers of the standard box, \((|0\rangle\langle 0| \otimes \frac{1}{2} \mathbb{I}_2)^m\). An equivalent variant of this task can be defined by considering the transformation \((\rho, \sigma) \rightarrow (|0\rangle\langle 0|, \pi_{2^m})\) instead, where \(\pi_k := \frac{1}{k} |0\rangle\langle 0| + \frac{k-1}{k} |1\rangle\langle 1|\), with the advantage that the latter approach allows the parameter \(m\) to vary continuously.

A result of [70] was to identify the one-shot distillable distinguishability with the hypothesis testing relative entropy \(D^\sigma_H(\rho, \sigma) := -\log \mathcal{F}(\rho, \sigma)\). A natural extension of this result to the asymptotic case \(D^\sigma_H(\rho, \sigma) := -\log \mathcal{F}(\rho, \sigma)\) was obtained. In an analogous way, in the conceptually related resource theory of symmetric distinguishability [58], the corresponding task of dilution was connected with the Thompson metric \(D^\varepsilon_{\text{TPNI}}\). In contrast, in our probabilistic setting, the task of dilution trivialises — any state can be obtained from a pure state probabilistically [57].

VI. General Probabilistic Theories

The framework of general probabilistic theories (GPTs) [75], [76], [77] encompasses both quantum and classical probability theory, providing a natural way to study the properties of very general physical theories, and in particular to formalise the similarities and differences between them. Although concepts such as states and measurements can be defined in any such setting, studying the optimal errors in the asymptotic regime did not appear possible — the optimal error exponents encountered in classical and quantum theory involve quantities such as the quantum relative entropy \(D(\cdot|\cdot)\) and the Chernoff divergence \(\varepsilon(\cdot|\cdot)\), both of which require the properties of classical or quantum theory even to be defined. Because of this, no results whatsoever have been known about asymptotic hypothesis testing in broader GPTs. Our framework, however, can be straightforwardly adapted also to such general theories, and we will see that our findings on state discrimination in Sections II and III hold in arbitrary GPTs verbatim.

A. Definitions

To define a GPT, one first identifies the compact and convex set \(S\) of states within a real vector space \(\mathcal{V}\), here assumed to be finite dimensional. In analogy with the geometry of quantum theory, the affine hull of the set \(S\) is required to have codimension 1 within \(\mathcal{V}\), and to not contain the zero vector.³ The cone generated by \(S\), namely \(C := \{\lambda \rho\ | \lambda \in \mathbb{R}_+, \rho \in S\}\), is used to induce a partial order on the space \(\mathcal{V}\) as \(y \leq_C y \iff y-x \in C\). The compactness of \(S\), which implies that \(C\) is pointed, or \(C \cap (-C) = \{0\}\), indeed means that this is a partial order. Furthermore, the fact that the affine hull of \(S\) is full dimensional entails that \(C\) is generating, i.e. \(\text{span}(C) = \mathcal{V}\).

³This seemingly ad hoc set of axioms is actually well justified from a foundational perspective. We refer the interested reader to [78, Chapters 1–2] for more details on these points as well as complete derivations.
The dual space $V^*$, i.e., the space of continuous linear functionals $M: V \to \mathbb{R}$, then has a partial order $X \leq_{C^*} Y \iff Y - X \in C^*$ induced by the dual cone $C^* := \left\{ M \in V^* \mid \langle M, \rho \rangle \geq 0 \forall \rho \in S \right\}$, where we write $(M, x) = M(x)$ for every $x \in V$, $M \in V^*$. We use the notation $X \in C^*$ to denote $Y - X \in \text{int}(C^*)$.

In order to define measurements in this theory, we also need to identify the set of effects, that is, elements of the dual space which yield physical measurement outcomes. First, a fixed unit effect $U >_{C^*} 0$ is defined as the unique element of $V^*$ such that $\langle U, \rho \rangle = 1$ for all $\rho \in S$. The so-called no restriction hypothesis then allows us to assume that any element $M \in V^*$ such that $\langle M, \rho \rangle \in [0, 1]$ for all $\rho \in S$ is a valid effect, and thus a valid measurement operator; this can be equivalently understood as $0 \leq_{C^*} M \leq_{C^*} U$. A measurement is then a collection of effects $\{M_i\}$ such that $\sum_{i=1}^n M_i = U$ — in other words, a collection such that the measurement outcome probabilities $\langle M_i, \rho \rangle$ sum to unity for every state $\rho$.

We remark that both quantum and classical probability theory are special cases of the above. Although the Hilbert space underlying the setting of quantum mechanics is complex, the space where density operators live — corresponding to $V$ here — is nevertheless a real vector space, which is why the general assumptions of GPTs encompass quantum mechanics. Specifically, in the quantum case $\mathcal{V}$ is the space of self-adjoint operators acting on some complex Hilbert space, $\mathcal{C}$ and $\mathcal{C}^*$ are both cones of positive semidefinite operators, and the unit effect $U$ is the identity.

We will use the tuple $(\mathcal{V}, \mathcal{C}, U)$ to denote a GPT as above, as the theory is uniquely determined by the three choices. Given two GPTs, $(\mathcal{V}_A, \mathcal{C}_A, U_A)$ and $(\mathcal{V}_B, \mathcal{C}_B, U_B)$, we then wish to define a bipartite structure that combines the two. Under natural assumptions including the so-called local tomography principle, which states that bipartite states should be fully determined by the statistics of local measurements, it holds that $\mathcal{V}_{AB}$ is isomorphic to $\mathcal{V}_A \otimes \mathcal{V}_B$ [81], [82], which means that we can identify $\mathcal{V}_{AB} = \mathcal{V}_A \otimes \mathcal{V}_B$ and $U_{AB} = U_A \otimes U_B$ without loss of generality. Interestingly, this does not uniquely determine a bipartite cone $\mathcal{C}_{AB}$; the only thing that can be concluded is that [83]

$$\mathcal{C}_A \otimes \mathcal{C}_B \subseteq \mathcal{C}_{AB} \subseteq \mathcal{C}_A \otimes \mathcal{C}_B$$

where the minimal tensor product and the maximal tensor product are defined, respectively, as

$$\mathcal{C}_A \otimes \mathcal{C}_B := \text{conv}(\mathcal{C}_A \otimes \mathcal{C}_B),$$

$$\mathcal{C}_A \otimes \mathcal{C}_B := \left( \mathcal{C}_A \otimes \mathcal{C}_B \right)^*.$$  

(103)

For every pair of non-classical GPTs, it holds that $\mathcal{C}_A \otimes \mathcal{C}_B \neq \mathcal{C}_A \otimes \mathcal{C}_B$ [84], and the difference between these two cones is paramount to understanding properties of multipartite GPTs, in particular the existence of phenomena such as entanglement [83], [85].

Despite the fact that many aspects of GPTs crucially depend on the specific choice of a multipartite cone $\mathcal{C}_{AB}$, our results will apply to any choice of $\mathcal{C}_{AB}$ as in (103), making them universally applicable. We remark in particular that $\mathcal{C}_A \otimes \mathcal{C}_B \subseteq \mathcal{C}_{AB}$ and $\mathcal{C}_A \otimes \mathcal{C}_B^* \subseteq \mathcal{C}_{AB}$ for all valid choices of $\mathcal{C}_{AB}$.

The extension of the above to the tensor product of more than two GPTs is immediate.

B. Extension of Results

The task of state discrimination, in both the conventional and postselected settings, can be formulated in exactly the same way as we have done it in Section I; specifically,

$$\beta_\epsilon (\rho, \sigma) = \inf_{M_1, M_2 \geq_{C^*} 0} \left\{ \frac{\langle M_1, \sigma \rangle}{\langle M_1 + M_2, \sigma \rangle} \left| M_1 + M_2 \leq_{C^*} U, \right. \frac{\langle M_2, \rho \rangle}{\langle M_1 + M_2, \rho \rangle} \leq \epsilon \right\}$$

$$\overline{p}_{\text{err}}(\rho, \sigma | p, q) = \inf_{M_1, M_2 \geq_{C^*} 0} \frac{p \langle M_2, \rho \rangle + q \langle M_1, \sigma \rangle}{p \langle M_1 + M_2, \rho \rangle} + q \langle M_1 + M_2, \sigma \rangle$$

(105)

where $\rho, \sigma \in S$ and $p, q = 1 - p \in (0, 1)$ as before. The equivalent of the max-relative entropy can also be defined in the same way,

$$D_{\text{max}}(\rho | | \sigma) := \log \inf \left\{ \lambda \in \mathbb{R}_+ \mid \rho \leq \lambda \sigma \right\}$$

(106)

with the definitions of $D_\Omega$ and $D_\Xi$ naturally extending to the GPT formalism using the above quantity.

The results of our Theorem 1 (asymmetric error) and Theorem 6 (symmetric error) then apply to any GPT exactly as stated under the replacement $\text{Tr}(M \cdot) \mapsto \langle M, \cdot \rangle$ — there is no need to adjust any of the proofs, as we have not made use of any properties of quantum mechanics, with our proofs resting on the linearity of the trace and convex (Lagrange) duality, both of which hold for arbitrary GPTs defined as in Section VI-A.

This correspondence is not too surprising, given that many results on one-shot state discrimination can be mapped between quantum mechanics and GPTs [86], [87]. What is more remarkable about the setting of postselected hypothesis testing is that the asymptotic results — namely, Corollary 2 and Corollary 7 — are also valid in arbitrary GPTs, with no other assumptions needed. This is because of the easily verified additivity of $D_{\text{max}}$, which we formalise below.

**Lemma 15:** Given a local GPT $(\mathcal{V}, \mathcal{C}, U)$, consider any $n$-copy GPT $(\mathcal{V}_n, \mathcal{C}_n, U_n)$, where $\mathcal{V}_n = \bigotimes_{i=1}^n \mathcal{V}$, $U_n = \bigotimes_{i=1}^n U$, and $\mathcal{C}_n = \bigotimes_{i=1}^n \mathcal{C} \subseteq \bigotimes_{i=1}^n \mathcal{C}$. Then, for all $\rho, \sigma \in S$,

$$D_{\text{max}}(\rho^n \| | \sigma^n) = n D_{\text{max}}(\rho | | \sigma).$$

(107)

**Proof:** Consider any feasible $\lambda$ such that $\rho \leq \lambda \sigma$. Then, $\rho^n \leq \lambda^n \sigma^n = \lambda^n \rho^n \lambda \sigma^n$, this can be seen by using the fact that $\mathcal{C} \otimes \mathcal{C} \subseteq \mathcal{C} \otimes \mathcal{C}$ to show that

$$\lambda^2 (\sigma \otimes \sigma) - \rho \otimes \rho = (\lambda \sigma - \rho) \otimes \lambda \sigma + \rho \otimes (\lambda \sigma - \rho) \geq_{c_2} 0$$

(108)
and extending to arbitrary \( n \) by induction. This implies that 
\[ D_{\max}(\rho^\otimes n) \leq n \log \lambda, \] 
and hence 
\[ D_{\max}(\rho^\otimes n\|\sigma^\otimes n) \leq nD_{\max}(\rho\|\sigma). \]

For the other direction, we write \( D_{\max} \) in its dual form as 
\[ D_{\max}(\rho\|\sigma) = \log \sup_{W \geq 0} \frac{\langle W, \rho \rangle}{\langle W, \sigma \rangle}. \tag{109} \]

The fact that \( \bigotimes_{i=1}^n C^\ast \subseteq C^\ast_n \) immediately implies that any feasible solution \( W \) to \( D_{\max}(\rho\|\sigma) \) gives a feasible solution to 
\[ D_{\max}(\rho^\otimes n\|\sigma^\otimes n) \] 
as \( W^\otimes n \), concluding the proof. \[ \square \]

The above lemma tells us that 
\[ D_{\Omega}(\rho^\otimes n\|\sigma^\otimes n) = nD_{\Omega}(\rho\|\sigma) \] 
and 
\[ D_{\Xi}(\rho^\otimes n\|\sigma^\otimes n) = nD_{\Xi}(\rho\|\sigma) \] 
for all normalised \( \rho, \sigma \in \mathcal{S} \). The asymptotic results of Corollaries 2 and 7 thus follow immediately; namely, we have that 
\[ \lim_{n \to \infty} -\frac{1}{n} \log \beta_D(\rho^\otimes n, \sigma^\otimes n) = D_{\Omega}(\rho\|\sigma) \tag{110} \]
and 
\[ \lim_{n \to \infty} -\frac{1}{n} \log \beta_{\xi}(\rho^\otimes n, \sigma^\otimes n | p, q) = D_{\Xi}(\rho\|\sigma) \tag{111} \]
for all \( \rho, \sigma \in \mathcal{S}, \varepsilon \in (0, 1) \), and all \( p, q = 1 - p \in (0, 1) \).

Theorem 5, which establishes a postselected generalisation of the quantum Stein’s lemma in the composite setting, also immediately holds in every GPT. The proof is, once again, noticed not to use any assumptions save for linearity and convex duality.

We thus see that virtually all of our results on state discrimination immediately extend to GPTs, without requiring any restrictive assumptions on the latter. On the other hand, although we expect at least some of our channel discrimination results to also be generalisable to GPTs under some reasonable assumptions, we should note that this is far from immediate — even defining a ‘channel’ is no trivial task in a framework so general, and tools such as the Choi–Jamiołkowski isomorphism might no longer be available to us. We thus leave the question of investigating channel discrimination in this setting as an open problem.

VII. DISCUSSION

The approach of our work is inherently different from conventional quantum hypothesis testing, yet we hope that it can ultimately prove helpful in shedding light also on the latter. The distinguishing feature of our results, and perhaps an unexpected finding, is how significantly the whole framework simplifies in the postselected setting: the optimal probabilities can be given straightforward closed-form expressions; the case of composite hypothesis testing reduces to a simple extension of the i.i.d. case; all terms but those of order \( 1/n \) disappear from the asymptotic expansions; and, importantly, the task of channel discrimination not only admits efficiently computable error probabilities and exponents, but in fact reduces all discrimination strategies to the much simpler case of parallel protocols. This allowed us to essentially characterise completely the task of postselected quantum hypothesis testing with just a few concise proofs — something that, in the conventional setting, has been a multi-decade endeavour requiring significant effort and the development of highly specialised methods.

An underlying property of our framework is the need to condition on a conclusive outcome of the measurement. This is an easily realisable operation: simply repeat the measurement protocol, disregarding measurement data corresponding to inconclusive outcomes. It is, however, conceivable that the conclusive outcome may have a low probability of occurrence, meaning that many repetitions of the measurement protocol would be needed to successfully discriminate the states or channels. Such a difference indeed makes direct comparisons between \( n \)-copy distinguishability protocols in the postselected and conventional settings difficult to perform. However, as we argued in [56], allowing postselection is much more easily justified in the limit of infinitely many i.i.d. copies, where the definition of a rate may be adjusted depending on what ‘cost function’ we wish to employ: if we are interested in error rates per number of copies of states generated, then the conventional setting appears more appropriate; if, however, we instead focus on how many copies of states need to be manipulated at once, then any protocol may be repeated without incurring an additional cost, and a postselected setting is thus perfectly natural. The latter assumption is not necessarily an extravagant one — generating many copies of states is far easier than coherently manipulating them with current technologies.

The idea of postselection has previously appeared in a range of contexts in quantum information, including — besides the aforementioned state discrimination [35], [36], [37] — quantum computing [88], metrology [89], [90], [91], [92], [93], connections with spacetime geometry [94], [95], [96], and manipulation of quantum entanglement [97], [98], [99] as well as more general quantum resources [54], [56], [57]. In such settings, our results can be viewed as ultimate limits that cannot be exceeded even if postselection is permitted: the optimal discrimination error bounds shown in our work cannot be beat by any measurement strategy, postselected or not, even in permissive frameworks such as ones allowing the increased distinguishing power of postselected closed timelike curves [94], [96].

Ultimately, although it might be contentious to claim that it has directly led to practical advancements, postselection has unquestionably contributed to the understanding of the foundations of quantum mechanics [100], [101], [102], and even formed the conceptual basis of the first proposals for quantum supremacy experiments [103]. In a similar manner, we hope that our results can find use both in the formalisation of the foundations of quantum information, as well as in the study of the limits of practical state and channel discrimination protocols.

REFERENCES

[1] M. Hayashi, Quantum Information Theory: Mathematical Foundation. Cham, Switzerland: Springer, 2017.
[2] J. Watrous, The Theory of Quantum Information. Cambridge, U.K.: Cambridge Univ. Press, 2018.
[3] M. M. Wilde, Quantum Information Theory, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2017.
[4] C. W. Helstrom, “Quantum detection and estimation theory,” J. Statist. Phys., vol. 1, no. 2, pp. 231–252, 1969.
[5] A. S. Holevo, “An analogue of statistical decision theory and non-commutative probability theory,” Trudy Moskovskogo Matematicheskogo Obshchestva, vol. 26, p. 133–149, Oct. 1972.
M. Tomamichel and M. Hayashi, “A hierarchy of information quantities for finite block length analysis of quantum tasks,” IEEE Trans. Inf. Theory, vol. 59, no. 11, pp. 7693–7710, Nov. 2013.

M. Fekete, “Über die verteilung der Wurzeln bei gewissen algebraischen gleichungen mit ganzzahligen koeffizienten,” Mathematische Zeitschrift, vol. 17, no. 1, pp. 228–249, Dec. 1923.

F. G. S. L. Brandão and M. B. Plenio, “A reversible theory of entanglement and its relation to the second law,” Commun. Math. Phys., vol. 295, no. 3, pp. 829–851, May 2010.

R. T. Rockafellar, Convex Analysis. Princeton, NJ, USA: Princeton Univ. Press, 1970.

A. Y. Kitaev, “Quantum computations: Algorithms and error correction,” in Convex Analysis, vol. 1, R. T. Rockafellar, Ed. Boston, MA, USA: Amer. Math. Soc., 1998, pp. 1–100.

S. Aaronson, “Quantum computing, postselection, and probabilistic computation assisted,” Commun. Math. Phys., vol. 344, no. 3, pp. 797–829, Jun. 2016.

S. Pirandola, S. R. Laing, J. C. Walther, and T. C. Ralph, “Fundamental limits on quantum channel discrimination,” NPJ Quantum Inf., vol. 5, no. 1, pp. 1–8, June 2019.

B. Regula and R. Tagaki, “Fundamental limitations on distillation of quantum channel resources,” Nature Commun., vol. 12, no. 1, p. 4411, Jul. 2021.

K. Matsumoto, “Reverse test and characterization of quantum relative entropy,” 2010, arXiv:1010.1030.

X. Wang and M. M. Wilde, “Resource theory of asymmetric distinguishability,” Phys. Rev. Lett., vol. 106, no. 3, Dec. 2012, Art. no. 030401.

E. Chitambar and G. Gour, “Quantum resource theories,” Rev. Modern Phys., vol. 91, no. 2, Apr. 2019, Art. no. 025001.

L. Wang and R. Renner, “One-shot classical-quantum capacity and hypothesis testing,” Phys. Rev. Lett., vol. 19, no. 20, May 2019, Art. no. 200501.

F. Buscemi and N. Datta, “The quantum capacity of channels with arbitrarily correlated noise,” IEEE Trans. Inf. Theory, vol. 56, no. 3, pp. 1447–1460, Mar. 2010.

F. Buscemi, D. Sutter, and M. Tomamichel, “An information-theoretic treatment of quantum dichotomies,” Quantum, vol. 3, p. 209, Dec. 2019.

G. Ludwig, An Axiomatic Basis for Quantum Mechanics: Volume 1 Derivation of Hilbert Space Structure. Berlin, Germany: Springer-Verlag, 1985.

A. Hartkämper and H. Neumann, Foundations of Quantum Mechanics and Ordered Linear Spaces. Cham, Switzerland: Springer, 1974.

E. B. Davies and J. T. Lewis, “An operational approach to quantum probability,” Commun. Math. Phys., vol. 17, no. 3, pp. 239–260, Sep. 1970.

L. Lami, “Non-classical correlations in quantum mechanics and beyond,” Ph.D. dissertation, Dept. Phys., Universitat Autònoma de Barcelona, Bellaterra, Spain, 2017.

J. Barrett, “Information processing in generalized probabilistic theories,” J. Phys. A, vol. 75, no. 3, Mar. 2007, Art. no. 032304.

G. Chiribella, G. M. D’Ariano, and P. Perinotti, “Probabilistic theories with purification,” Phys. Rev. A, vol. 81, no. 6, Jun. 2010, Art. no. 062348.

M. Kläy, C. Randall, and D. Foulis, “Tensor products and probability weights,” Int. J. Theor. Phys., vol. 26, no. 3, pp. 199–219, Mar. 1987.

A. Wilce, “Tensor products in generalized measure theory,” Int. J. Theor. Phys., vol. 31, no. 21, pp. 1915–1928, Nov. 1992.

I. Namioka and R. Phelps, “Tensor products of compact convex sets,” Pacific J. Math., vol. 31, no. 2, pp. 469–480, Nov. 1969.

G. Aubrun, L. Lami, C. Palazuelos, and M. Plávala, “Entangleability of cones,” Geometric Funct. Anal., vol. 21, no. 2, pp. 181–205, Apr. 2021.

G. Aubrun, L. Lami, C. Palazuelos, and M. Plávala, “Entanglement and superposition are equivalent concepts in any physical theory,” Phys. Rev. Lett., vol. 128, no. 16, Apr. 2022, Art. no. 160402.

S. Aaronson, “Quantum computing, postselection, and probabilistic polynomial-time,” Proc. Roy. Soc. A, Math. Phys. Eng. Sci., vol. 461, no. 2063, pp. 3473–3482, Nov. 2005.