Asymptotic relative submajorization of multiple-state boxes

Gergely Bunth · **Péter Vrana**

Abstract Pairs of states, or "boxes" are the basic objects in the resource theory of asymmetric distinguishability (Wang and Wilde, 2019), where free operations are arbitrary quantum channels that are applied to both states. From this point of view, hypothesis testing is seen as a process by which a standard form of distinguishability is distilled. Motivated by the more general problem of quantum state discrimination, we consider boxes of a fixed finite number of states and study an extension of the relative submajorization preorder to such objects. In this relation a tuple of positive operators is greater than another if there is a completely positive trace nonincreasing map under which the image of the first tuple satisfies certain semidefinite constraints relative to the other one. This preorder characterizes error probabilities in the case of testing a composite null hypothesis against a simple alternative hypothesis, as well as certain error probabilities in state discrimination. We present a sufficient condition for the existence of catalytic transformations between boxes, and a characterization of an associated asymptotic preorder, both expressed in terms of sandwiched Rényi divergences. This characterization of the asymptotic preorder directly shows that the strong converse exponent for a composite null hypothesis is equal to the maximum of the corresponding exponents for the pairwise simple hypothesis testing tasks.

Keywords relative submajorization · composite hypothesis testing · strong converse exponent

Mathematics Subject Classification (2010) 81P18 · 94A17

Gergely Bunth
Institute of Mathematics, Budapest University of Technology and Economics, Egry József u. 1., Budapest, 1111 Hungary;
MTA-BME Lendület Quantum Information Theory Research Group
E-mail: bunthy@math.bme.hu

Péter Vrana
Institute of Mathematics, Budapest University of Technology and Economics, Egry József u. 1., Budapest, 1111 Hungary;
MTA-BME Lendület Quantum Information Theory Research Group E-mail: vranap@math.bme.hu

Declarations

Availability of data and material

Not applicable.

Code availability

Not applicable.

1 Introduction

Resource theories provide a unique viewpoint within numerous areas in quantum information theory and physics, such as entanglement theory and quantum thermodynamics [8]. Building upon the work of Matsumoto [15], Wang and Wilde [25] carried out a systematic development of the resource-theoretic approach to hypothesis testing in the form of a resource theory of asymmetric distinguishability (see also [6], where related results are independently obtained with a different perspective). The objects of this resource theory are pairs of quantum states, ordered by joint transformations with general quantum channels. The task of hypothesis testing is then interpreted as distillation of standard pairs, "bits of asymmetric distinguishability", the quantum min- and max-divergences [10] as well as the quantum relative entropy [14, 19] emerge as the distillable distinguishability and distinguishability costs in single-shot and asymptotic settings.

   In [25] it is also suggested that the resource theoretic study could be extended to more general discrimination tasks, including the discrimination of more than two states, as in the theory of quantum state discrimination [7, 2, 1]. Composite hypothesis testing problems have been studied in the Stein setting[5, 3] and in the strong converse regime[17]. In this work we take a step in this direction, considering boxes consisting of multiple states and studying the strong converse exponent, employing the methods of [20]. With the aim of incorporating probabilities and approximations in the objects compared, we work with tuples of unnormalized states and introduce a generalization of relative submajorization [21] to boxes. We say that a box $(\rho_1, \ldots, \rho_m, \sigma)$ relatively submajorizes $(\rho'_1, \ldots, \rho'_m, \sigma')$ if there is a completely positive trace-nonincreasing map T such that $T(\rho_i) \geq \rho'_i$ and $T(\sigma) \leq \sigma'$ as positive semidefinite matrices. For

normalized boxes this relation is equivalent to the existence of a joint exact transformation of the states (for classical boxes also to matrix majorization in the sense of [9]), and for unnormalized boxes it encodes error probabilities in hypothesis testing and state discrimination tasks.

Our main results concern asymptotic, catalytic and many-copy relaxations of the relative submajorization relation between such boxes (see Section 2 for precise definitions). We find that in these limits the transformations are governed by certain pairwise Rényi divergences, and as in [20], the relevant quantum extensions are the sandwiched Rényi divergences [18,26]. More precisely, given (unnormalized) boxes $(\rho_1, \ldots, \rho_m, \sigma)$ and $(\rho'_1, \ldots, \rho'_m, \sigma')$, where σ and σ' are invertible, we prove the following:

1. $(\rho_1, \ldots, \rho_m, \sigma)$ asymptotically relative submajorizes $(\rho'_1, \ldots, \rho'_m, \sigma')$ iff for all $\alpha \geq 1$ and all $i \in \{1, \ldots, m\}$ the inequalities

$$\mathrm{Tr} \left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho_i \sigma^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha} \geq \mathrm{Tr} \left(\sigma'^{\frac{1-\alpha}{2\alpha}} \rho'_i \sigma'^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha} \tag{1}$$

   hold.
2. If for every $\alpha \geq 1$ and all $i \in \{1, \ldots, m\}$ the *strict* inequalities

$$\mathrm{Tr} \left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho_i \sigma^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha} > \mathrm{Tr} \left(\sigma'^{\frac{1-\alpha}{2\alpha}} \rho'_i \sigma'^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha} \tag{2}$$

   hold and in addition

$$\left\| \sigma^{-1/2} \rho_i \sigma^{-1/2} \right\|_{\infty} > \left\| \sigma'^{-1/2} \rho'_i \sigma'^{-1/2} \right\|_{\infty} \tag{3}$$

   for all $i \in \{1, \ldots, m\}$, then
   1) for all sufficiently large $n \in \mathbb{N}$ the box $(\rho_1^{\otimes n}, \ldots, \rho_m^{\otimes n}, \sigma^{\otimes n})$ relatively submajorizes $(\rho_1'^{\otimes n}, \ldots, \rho_m'^{\otimes n}, \sigma'^{\otimes n})$;
   2) there exists a catalyst $(\omega_1, \ldots, \omega_m, \tau)$ such that $(\rho_1 \otimes \omega_1, \ldots, \rho_m \otimes \omega_m, \sigma \otimes \tau)$ relative submajorizes $(\rho'_1 \otimes \omega_1, \ldots, \rho'_m \otimes \omega_m, \sigma' \otimes \tau)$.

As a special case, the normalized box $(\rho_1, \ldots, \rho_m, \sigma)$ can be viewed as a hypothesis testing problem where the states $\rho_1, \ldots, \rho_m$ form a composite null hypothesis, to be tested against the simple alternative hypothesis σ. In the strong converse regime, a type I error $1 - 2^{-Rn + o(n)}$ with a type II error 2^{-rn} is achievable iff $(\rho_1, \ldots, \rho_m, \sigma)$ asymptotically relative submajorizes the unnormalized box $(2^{-R}, \ldots, 2^{-R}, 2^{-r})$. From the characterization 1 we see that this happens precisely when

$$R \geq \max_i \sup_{\alpha > 1} \frac{\alpha - 1}{\alpha} \left[r - \widetilde{D}_\alpha \left(\rho_i \| \sigma \right) \right]. \tag{4}$$

We prove these results using recent advances in the theory of preordered semirings [12, **?**]. In particular, we introduce the semiring of unnormalized boxes, equipped with the preorder given by relative submajorization, and apply two generalizations of Strassen's characterization theorem [22]. The one given in [**?**] leads to the equivalence 1 after classifying the nonnegative real-valued monotone homomorphisms. On

the other hand, the implication 2 is an application of [12, 1.4. Theorem], and in addition requires the classification of the monotone homomorphisms into the tropical semiring. We find that, somewhat surprisingly, both kinds of monotone homomorphisms are pairwise quantities in the sense that each of them depends on only two states of the box.

The proof of our result on asymptotic relative submajorization uses some of the ideas from [20], where boxes of pairs are studied, but deviates substantially from it in two key steps (in addition to the more obvious differences in the classification of real-valued monotones and the tropical ones that were not considered there). The first difference is that in the case of pairs of states it was possible to find a set of multipliers (the one-dimensional pairs) with the property that every pair can be multiplied by a suitable element in such a way that the product is bounded from above and from below with respect to the natural numbers. This in turn made it possible to use [?, Theorem 1.2.], showing that monotone semiring homomorphisms characterize the asymptotic preorder. With multiple states such a set does not exist, and therefore we must take a different route, effectively applying [?, Corollary 1.3.] to the semifield of fractions of the semiring of boxes. The second difference is that in [20] an application of the $\sigma^{\otimes n}$-pinching map was sufficient to ensure that the resulting states commute and thus reduce the evaluation of the monotones on pairs of quantum states to pairs of classical distributions. With more than two states the pinching map alone is not sufficient as the images of different quantum states under the pinching map need not commute. To get around this problem we make use of the special form of the classical monotones.

The remainder of the paper is structured as follows. In Section 2 we introduce the relevant notions related to preordered semirings and state recent results relating monotone semiring homomorphisms to several relaxations of the preorder. In Section 3 we introduce the semiring of boxes and extend the relative submajorization preorder to obtain a preordered semiring. In Section 4 we provide a classification of the monotone homomorphisms into the real and tropical real semiring. In Section 5 we derive explicit conditions for asymptotic, many-copy and catalytic relative submajorization in terms of sandwiched Rényi divergences. In Section 6 we give applications to asymptotic state discrimination.

2 Preliminaries

A *preordered semiring* is a tuple $(S, +, \cdot, 0, 1, \preccurlyeq)$ where S is a set, $+, \cdot : S \times S \to S$ are commutative and associative binary operations satisfying $(x + y) \cdot z = x \cdot z + y \cdot z$ for all $x, y, z \in S$, $0, 1 \in S$ are the zero element and the unit (i.e. $0 \cdot x = 0$ and $1 \cdot x = x$ for all x), and $\preccurlyeq \subseteq S \times S$ is a transitive and reflexive relation (preorder) such that $x \preccurlyeq y$ implies $x + z \preccurlyeq y + z$ and $x \cdot z \preccurlyeq y \cdot z$ for every $x, y, z \in S$. We will adopt the convention that the binary operations and neutral elements are denoted uniformly with the same symbols $+, \cdot, 0, 1$ (with the multiplication sign often omitted as usual), and preordered semirings will be referred to via the abbreviated notation $(S, \preccurlyeq)$, indicating only the underlying set and the preorder, or even just S when the preorder is clear. This will in

particular be the case in the following examples, where the preorder (in these cases a total order) will be denoted as $\leq$.

Example 1 The set $\mathbb{R}_{\geq 0}$ of nonnegative real numbers with its usual addition, multiplication and total order is a preordered semiring.

Example 2 (tropical semiring in the multiplicative picture) As a set, the tropical semiring is $\mathbb{TR} = \mathbb{R}_{\geq 0}$, $x + y$ is defined as the maximum of x and y, while $\cdot$ is the usual multiplication. We equip this semiring with the usual total order of the real numbers. This is a preordered semiring.

We will be interested in preordered semirings satisfying a pair of additional conditions. First, we require that the canonical map $\mathbb{N} \to S$ (the one that sends n to the n-term sum $1 + 1 + \cdots 1$) is an order embedding (i.e. injective and $m \leq n$ as natural numbers iff their images, also denoted by m and n, satisfy $m \preccurlyeq n$). Second, the semiring is assumed to be of *polynomial growth* [**?**]. This means that there exists an element $u \in S$ such that $u \succcurlyeq 1$ and for every nonzero $x \in S$ there is a $k \in \mathbb{N}$ such that $x \preccurlyeq u^k$ and $1 \preccurlyeq u^k x$. Any such element u is called *power universal*. A power universal element need not be unique but the subsequent definitions can be shown not to depend on a particular choice.

Definition 1 Let $x, y \in S$. We write $x \succsim y$ and say that x is asymptotically larger than y if for some sublinear sequence $(k_n)_{n \in \mathbb{N}}$ of natural numbers and for all $n \in \mathbb{N}$ the inequality $u^{k_n} x^n \succcurlyeq y^n$ holds.

A monotone semiring homomorphism between the preordered semirings $(S_1, \preccurlyeq_1)$ and $(S_2, \preccurlyeq_2)$ is a map $\varphi : S_1 \to S_2$ that satisfies $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\varphi(xy) = \varphi(x)\varphi(y)$ and $x \preccurlyeq_1 y \implies \varphi(x) \preccurlyeq_2 \varphi(y)$ for $x, y \in S_1$. We will consider monotone homomorphisms into the real and tropical real semirings. For these we introduce the following notations: given a preordered semiring $(S, \preccurlyeq)$ we let $\Delta(S, \preccurlyeq) = \mathrm{Hom}(S, \mathbb{R}_{\geq 0})$ and $\hat{\Delta}(S, \preccurlyeq) = \Delta(S, \preccurlyeq) \cup \{f \in \mathrm{Hom}(S, \mathbb{TR}) | f(u) = 2\}$. The two parts will be referred to as the real and the tropical part of the *spectrum* of the semiring. It should be noted that while there is an inherent normalization condition in the definition of a homomorphism into the nonnegative reals, there is no such limitation in tropical real valued homomorphisms since one can always rescale in a multiplicative sense by replacing $f(x)$ with $f^c(x)$ for some $c > 0$ (see also [12, Section 13.]). This is the reason for requiring that $f(u) = 2$ in our definition (the number 2 itself is arbitrary, but will be convenient relative to our choice of the power universal element u later).

The evaluation map for an element $s \in S$ is the map $\mathrm{ev}_s : \Delta(S, \preccurlyeq) \to \mathbb{R}_{\geq 0}$ defined as $f \mapsto f(s)$ (one could similarly consider the evaluation map on $\hat{\Delta}(S, \preccurlyeq)$, but it is this restricted form that we will need). It should be noted that both kinds of spectra can be endowed with a topology using the evaluation maps and in general $\hat{\Delta}(S, \preccurlyeq)$ is *not* the disjoint union of its real and tropical part as topological spaces.

Our strategy will be to use the elements of the spectrum to characterize the asymptotic preorder. The main tool will be the following result from [**?**].

Theorem 1 *Let $(S, \preccurlyeq)$ be a preordered semiring of polynomial growth such that $\mathbb{N} \hookrightarrow S$ is an order embedding. The following conditions are equivalent:*

1. *for every $x, y \in S \setminus \{0\}$ such that $\frac{\mathrm{ev}_y}{\mathrm{ev}_x} : \Delta(S, \preccurlyeq) \to \mathbb{R}_{\geq 0}$ is bounded there is an $n \in \mathbb{N}$ such that $nx \gtrsim y$*
2. *$x \gtrsim y$ for every $x, y \in S \iff \forall f \in \Delta(S, \preccurlyeq) : f(x) \geq f(y)$.*

The asymptotic preorder is not the only relaxation that can be investigated with methods based on monotone homomorphisms. In the recent work [12] Fritz has found sufficient conditions for catalytic and multi-copy transformations in terms of monotone homomorphisms into certain semirings including the real and tropical real numbers. We now state a special case of one of these results, specialized to our more restricted setting.

Theorem 2 ([12, second part of 1.4. Theorem, special case]) *Let S be a preordered semiring of polynomial growth with $0 \preccurlyeq 1$. Suppose that $x, y \in S \setminus \{0\}$ such that for all $f \in \hat{\Delta}(S, \preccurlyeq)$ the strict inequality $f(x) > f(y)$ holds. Then also the following hold:*

1. *there is a $k \in \mathbb{N}$ such that $u^k x^n \succcurlyeq u^k y^n$ for every sufficiently large n*
2. *if in addition x is power universal then $x^n \succcurlyeq y^n$ for every sufficiently large n*
3. *there is a nonzero $a \in S$ such that $ax \succcurlyeq ay$.*

In particular, the last condition means that x may be catalytically transformed into y with catalyst a (in [12] a catalyst is given explicitly in terms of the k above). We note that any of the listed conditions implies the non-strict inequalities $f(x) \geq f(y)$ for the monotone homomorphisms.

Despite the apparent similarity between the two results quoted above, there seems to be no simple way of reducing one to the other. In the following sections we will apply both in the context of box transformations and develop the results needed to do so in parallel. In particular, we will classify both the real and the tropical real valued monotones so that the implication in Theorem 2 can be made explicit, and also verify the condition of Theorem 1 so that in the presence of non-strict inequalities between the monotones the characterization of the asymptotic preorder is still available.

3 The semiring of boxes

We consider the number $m \in \mathbb{N}$, $m \geq 1$ fixed from now on. A *box* is an $m+1$-tuple $(\rho_1, \ldots, \rho_m, \sigma)$ of positive operators on a finite dimensional Hilbert space $\mathscr{H}$ where $\mathrm{supp}\, \sigma = \mathscr{H}$. We allow $\dim \mathscr{H} = 0$ in which case there is a unique such tuple. Let us call the boxes $(\rho_1, \ldots, \rho_m, \sigma)$ and $(\rho_1', \ldots, \rho_m', \sigma')$ *equivalent* when there is a unitary $U : \mathscr{H} \to \mathscr{H}'$ such that $\forall i : U \rho_i U^* = \rho_i'$ and $U \sigma U^* = \sigma'$. A box $(\rho_1, \ldots, \rho_m, \sigma)$ will be called *classical* if all pairs of operators commute, and *normalized* if $\mathrm{Tr}\, \rho_i = \mathrm{Tr}\, \sigma = 1$ for all i. A classical box may be identified with a tuple $(p_1, \ldots, p_m, q)$ of measures on a common finite set $\mathscr{X}$ or with a tuple of diagonal positive operators on $\mathbb{C}^{\mathscr{X}}$.

We consider the semiring $\mathscr{B}_m$ of equivalence classes of boxes where addition is induced by the direct sum and multiplication is induced by the tensor product. The zero element is the equivalence class of the unique box on any zero dimensional Hilbert space, and the unit is the equivalence class of the box $(1, 1, \ldots, 1)$ on the Hilbert space $\mathbb{C}$ (here we make the identification $\mathscr{B}(\mathbb{C}) = \mathbb{C}$). We denote the set of equivalence classes of classical boxes by $\mathscr{B}_{c,m}$. $\mathscr{B}_{c,m}$ is a subsemiring of $\mathscr{B}_m$.

We think of a box as a quantum system prepared via an unknown process ("black box"), with $\rho_1, \ldots, \rho_m, \sigma$ representing the possible states the system might be in. This point of view suggests that boxes should be compared by joint transformations, i.e. a box may be transformed into another box precisely when there is a stochastic map (quantum channel) that takes the ith state of the initial box into the ith state of the final box. This represents the ability of an experimenter to perform a physical process on the unknown state, resulting in a quantum system with different possible states. Formally, we write $(\rho_1, \ldots, \rho_m, \sigma) \succcurlyeq_1 (\rho'_1, \ldots, \rho'_m, \sigma')$ iff there is a channel T such that $T(\rho_i) = \rho'_i$ for all i and $T(\sigma) = \sigma'$. This defines a preorder on $\mathscr{B}_m$, but it unfortunately does not satisfy the requirements of Theorem 1 or Theorem 2, in particular $0 \not\preccurlyeq_1 1$.

Remark 1 The general form of Theorem 2 from [12, 1.4. Theorem] does not require $0 \preccurlyeq 1$. However, $\succcurlyeq_1$ would still have $m + 1$ homomorphisms (the traces of each component) that stay constant under the transformations, preventing strict inequality for comparable pairs. A similar situation is covered in [12, 14.7. Theorem], taking into account, intuitively, the infinitesimal neighborhood of *one* such norm-like homomorphism. It is quite possible that an analogous result can be obtained that is able to handle multiple conserved values, and we expect this to be an interesting line of research.

Following a similar route as in [20], we work instead with a relaxed preorder that ensures $0 \preccurlyeq 1$ and that generalizes the relative submajorization preorder defined for pairs of states in [21]:

Definition 2 Let $(\rho_1, \ldots, \rho_m, \sigma)$ and $(\rho'_1, \ldots, \rho'_m, \sigma')$ be boxes on $\mathscr{H}$ and $\mathscr{H}'$, respectively. We write $(\rho_1, \ldots, \rho_m, \sigma) \succcurlyeq (\rho'_1, \ldots, \rho'_m, \sigma')$ iff there exists a completely positive trace non-increasing map $T : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H}')$ such that the following inequalities hold (with the semidefinite partial order):

$$
\begin{aligned}
T(\rho_1) &\geq \rho'_1 \\
&\vdots \\
T(\rho_m) &\geq \rho'_m \\
T(\sigma) &\leq \sigma'
\end{aligned}
\tag{5}
$$

For $m = 1$ the relation is identical to relative submajorization [21, Definition 3].

It should be noted that some of the relations in Definition 2 can often be upgraded to equalities by an appropriate modification of the map T. Specifically, this is the case if $\operatorname{Tr} \sigma \geq \operatorname{Tr} \sigma'$:

Proposition 1 *Let* $(\rho_1, \ldots, \rho_m, \sigma)$ *and* $(\rho'_1, \ldots, \rho'_m, \sigma')$ *be boxes such that the inequality* $(\rho_1, \ldots, \rho_m, \sigma) \succcurlyeq (\rho'_1, \ldots, \rho'_m, \sigma')$ *holds. Then there exists a completely positive trace nonincreasing map* $\tilde{T} : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H}')$ *such that the inequalities* (5) *are satisfied with* $T = \tilde{T}$ *and in addition*

1. *if* $\operatorname{Tr} \sigma \geq \operatorname{Tr} \sigma'$ *then* $\tilde{T}(\sigma) = \sigma'$
2. *if* $\operatorname{Tr} \sigma = \operatorname{Tr} \sigma'$ *then* $\tilde{T}$ *is trace preserving*

Moreover, if $\mathrm{Tr}\,\rho_i \leq \mathrm{Tr}\,\rho_i'$ *for some i, then also* $T(\rho_i) = \rho_i'$ *for any map T satisfying* (5).

Proof Let $T : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H}')$ be a completely positive trace non-increasing map satisfying (5). Define the map $\tilde{T}$ as

$$\tilde{T}(X) = T(X) + [\mathrm{Tr}\,X - \mathrm{Tr}\,T(X)]\tau \tag{6}$$

for some $\tau \in \mathscr{S}_{\leq}(\mathscr{H}')$ to be specified later. Then $\tilde{T}$ is a sum of completely positive maps, therefore also completely positive. It is also trace nonincreasing since

$$\mathrm{Tr}\,\tilde{T}(X) = \mathrm{Tr}\,T(X) + [\mathrm{Tr}\,X - \mathrm{Tr}\,T(X)]\,\mathrm{Tr}\,\tau \leq \mathrm{Tr}\,T(X) + [\mathrm{Tr}\,X - \mathrm{Tr}\,T(X)] = \mathrm{Tr}\,X, \tag{7}$$

which also shows that $\tilde{T}$ is trace preserving iff $\mathrm{Tr}\,\tau = 1$. The inequalities involving ρ_i are still satisfied because $\tau \geq 0$:

$$\tilde{T}(\rho_i) = T(\rho_i) + [\mathrm{Tr}\,\rho_i - \mathrm{Tr}\,T(\rho_i)]\tau \geq T(\rho_i) \geq \rho_i'. \tag{8}$$

It remains to choose τ in such a way that (5) is satisfied. If $\mathrm{Tr}\,\sigma = \mathrm{Tr}\,T(\sigma)$ then $T(\sigma) \leq \sigma'$ and $\mathrm{Tr}\,\sigma \geq \mathrm{Tr}\,\sigma'$ implies $T(\sigma) = \sigma'$, in which case any τ will do. Otherwise $\mathrm{Tr}\,T(\sigma) < \mathrm{Tr}\,\sigma$ and we can choose

$$\tau = \frac{\sigma' - T(\sigma)}{\mathrm{Tr}\,\sigma - \mathrm{Tr}\,T(\sigma)}. \tag{9}$$

This choice ensures

$$\tilde{T}(\sigma) = T(\sigma) + [\mathrm{Tr}\,\sigma - \mathrm{Tr}\,T(\sigma)]\frac{\sigma' - T(\sigma)}{\mathrm{Tr}\,\sigma - \mathrm{Tr}\,T(\sigma)} = T(\sigma) + \sigma' - T(\sigma) = \sigma', \tag{10}$$

and in addition $\mathrm{Tr}\,\tau = 1$ iff $\mathrm{Tr}\,\sigma = \mathrm{Tr}\,\sigma'$.

For the last claim we only need to observe that if $T(\rho_i) \geq \rho_i'$ and $\mathrm{Tr}\,\rho_i \leq \mathrm{Tr}\,\rho_i'$ then in fact $\mathrm{Tr}\,\rho_i = \mathrm{Tr}\,T(\rho_i) = \mathrm{Tr}\,\rho_i'$ and therefore also $T(\rho_i) = \rho_i'$.

Proposition 2 $(\mathscr{B}_m)$ *is a preordered semiring.*

Proof We need to verify that the preorder is compatible with the semiring operations. Suppose that $(\rho_1, \ldots, \rho_m, \sigma) \succcurlyeq (\rho_1', \ldots, \rho_m', \sigma')$ and let T be a completely positive trace non-increasing map as in Definition 2. Let $(\omega_1, \ldots, \omega_m, \tau) \in \mathscr{B}_m$ a box on $\mathscr{K}$. Then

$$\begin{aligned}
(T \otimes \mathrm{id}_{\mathscr{B}(\mathscr{K})})(\rho_i \otimes \omega_i) &= T(\rho_i) \otimes \omega_i \geq \rho_1' \otimes \omega_i \\
(T \otimes \mathrm{id}_{\mathscr{B}(\mathscr{K})})(\sigma \otimes \tau) &= T(\sigma) \otimes \tau \leq \sigma' \otimes \tau,
\end{aligned} \tag{11}$$

therefore $(\rho_1, \ldots, \rho_m, \sigma)(\omega_1, \ldots, \omega_m, \tau) \succcurlyeq (\rho_1', \ldots, \rho_m', \sigma')(\omega_1, \ldots, \omega_m, \tau)$.

The map $\tilde{T} : \mathscr{B}(\mathscr{H} \oplus \mathscr{K}) \to \mathscr{B}(\mathscr{H}' \oplus \mathscr{K})$ defined as

$$\tilde{T}\left(\begin{bmatrix} A & B \\ C & D \end{bmatrix}\right) = \begin{bmatrix} T(A) & 0 \\ 0 & D \end{bmatrix} \tag{12}$$

is also completely positive and trace non-increasing, and satisfies

$$\begin{aligned}
\tilde{T}(\rho_i \oplus \omega_i) &= T(\rho_i) \oplus \omega_i \geq \rho_1' \oplus \omega_i \\
\tilde{T}(\sigma \oplus \tau) &= T(\sigma) \oplus \tau \leq \sigma' \oplus \tau,
\end{aligned} \tag{13}$$

therefore $(\rho_1, \ldots, \rho_m, \sigma) + (\omega_1, \ldots, \omega_m, \tau) \succcurlyeq (\rho_1', \ldots, \rho_m', \sigma') + (\omega_1, \ldots, \omega_m, \tau)$.

4 Classification of the monotone homomorphisms

We turn to the classification of monotone real and tropical real valued monotones. First we consider only classical boxes, relying heavily on the special structure of the semiring $\mathscr{B}_{c,m}$. We will see below that the box $u = (2, 2, \ldots, 2, 1)$ on $\mathbb{C}$ is power universal. In this section we do not use this property but we choose this element for the normalization of the tropical real-valued monotontes. A classical box $(p_1, \ldots, p_m, q)$ on $\mathbb{C}^{\mathscr{X}}$ is characterized by the diagonal elements $(p_i)_x$ and q_x ($i \in \{1, \ldots, m\}, x \in \mathscr{X}$).

Theorem 3 $\Delta(\mathscr{B}_{c,m}, \preccurlyeq)$ *consists of the maps*

$$f_{\alpha,i}(p_1, \ldots, p_m, q) = \sum_{x \in \mathscr{X}} (p_i)_x^\alpha q_x^{1-\alpha} \tag{14}$$

where $i \in \{1, \ldots, m\}$ *and* $\alpha \in [1, \infty)$.

The monotone homomorphisms from $\mathscr{B}_{c,m}$ to $\mathbb{TR}$ that send $u = (2, 2, \ldots, 2, 1)$ to 2 are the maps

$$f_{\infty,i}(p_1, \ldots, p_m, q) = \max_{x \in \mathscr{X}} \frac{(p_i)_x}{q_x}. \tag{15}$$

Proof From the expressions above it is clear that $f_{\alpha,i}$ is a semiring-homomorphism into $\mathbb{R}_{\geq 0}$ when $\alpha < \infty$ and into $\mathbb{TR}$ when $\alpha = \infty$. The maps $f_{\alpha,i}$ are related to the Rényi divergences as $f_{\alpha,i}(p_1, \ldots, p_m, q) = 2^{(\alpha-1)D_\alpha(p_i \| q)}$ when $\alpha \in [1, \infty)$ and $f_{\infty,i}(p_1, \ldots, p_m, q) = 2^{D_\infty(p_i \| q)}$, therefore monotone under relations of the form

$$(p_1, \ldots, p_m, q) \succcurlyeq (T(p_1), \ldots, T(p_m), T(q)), \tag{16}$$

where T is completely positive and trace preserving (by the data processing inequality). They are also monotone under projections onto subsets of $\mathscr{X}$, since every term in the sum is nonnegative (and since we take the maximum over $\mathscr{X}$). These two operations generate every completely positive trace nonincreasing map. Finally, one verifies that the maps are increasing in p_i and decreasing in q.

We show that these are the only elements of the spectrum. Let $f : \mathscr{B}_{c,m} \to \mathbb{R}_{\geq 0}$ or $f : \mathscr{B}_{c,m} \to \mathbb{TR}$ be a monotone homomorphism and consider the functions $g(x) = f(x, \ldots, x, x)$ and $h_i(y) = f(1, \ldots, 1, y, 1, \ldots, 1)$ (with y at the ith position), where $x, y \in \mathbb{R}_{>0}$ and the arguments are one-dimensional boxes. g and h_i inherit the multiplicativity of f and are monotone increasing (h_i essentially by definition, while if $0 \leq x_1 < x_2$ then the map $T = \frac{x_1}{x_2} \operatorname{id}_{\mathscr{B}(\mathbb{C})}$ shows that $(x_1, \ldots, x_1) \preccurlyeq (x_2, \ldots, x_2)$). This implies that $g(x) = x^\beta$ and $h_i(y) = y^{\alpha_i}$ for some $\alpha_i, \beta \geq 0$. In addition, the map $x \mapsto f(1, \ldots, 1, x)$ is monotone decreasing, therefore $\beta - \sum_{i=1}^m \alpha_i \leq 0$.

From this point we reason for the two types of homomorphisms separately, the most obvious difference being that the value of β depends on the type. For elements in the real part of the spectrum we derive a convexity condition that is necessary for a homomorphism to be monotone, while for the tropical part it is replaced by quasiconvexity. With hindsight one can see that the formally weaker joint quasiconvexity constraint already excludes every combination of the exponents that is not allowed by joint convexity, but we find it instructive to include both arguments.

Consider first a homomorphism f into $\mathbb{R}_{\geq 0}$ and boxes $(p_1, \ldots, p_m, q)$ with full support ($\operatorname{supp} p_1 = \cdots = \operatorname{supp} p_m = \operatorname{supp} q = \mathbb{C}^{\mathscr{X}}$). We have

$$
\begin{aligned}
f(p_1, \ldots, p_m, q) &= \sum_{x \in \mathscr{X}} f((p_1)_x, \ldots, (p_m)_x, q_x) \\
&= \sum_{x \in \mathscr{X}} g(q_x) \prod_{i=1}^{m} h_i \left(\frac{(p_i)_x}{q_x} \right) \qquad (17) \\
&= \sum_{x \in \mathscr{X}} q_x^{\beta - \sum_{i=1}^{m} \alpha_i} \prod_{i=1}^{m} (p_i)_x^{\alpha_i}.
\end{aligned}
$$

In $\mathscr{B}_{c,m}$ the elements $(2, 2, \ldots, 2)$ and $1 + 1 = (I_2, \ldots, I_2)$ are equivalent in the sense that $(2, 2, \ldots, 2) \succcurlyeq (I_2, \ldots, I_2)$ (choose $T(x) = x \frac{I_2}{2}$) and $(I_2, \ldots, I_2) \succcurlyeq (2, 2, \ldots, 2)$ (choose $T(x) = \operatorname{Tr} x$). Applying monotonicity and additivity we get $g(2) = 2g(1)$, and therefore $\beta = 1$.

Let $p_1, \ldots, p_m, q, p'_1, \ldots, p'_m, q' > 0$ and $\lambda \in (0, 1)$. Choosing $T = \operatorname{Tr}$ we see that

$$
\begin{aligned}
&\left(\begin{bmatrix} \lambda p_1 & 0 \\ 0 & (1-\lambda)p'_1 \end{bmatrix}, \ldots, \begin{bmatrix} \lambda p_m & 0 \\ 0 & (1-\lambda)p'_m \end{bmatrix}, \begin{bmatrix} \lambda q & 0 \\ 0 & (1-\lambda)q' \end{bmatrix} \right) \\
&\qquad \succcurlyeq (\lambda p_1 + (1-\lambda)p'_1, \ldots, \lambda p_m + (1-\lambda)p'_m, \lambda q + (1-\lambda)q'), \quad (18)
\end{aligned}
$$

and therefore

$$
\begin{aligned}
&\lambda f(p_1, \ldots, p_m, q) + (1-\lambda) f(p'_1, \ldots, p'_m, q') \\
&\quad = f(\lambda p_1, \ldots, \lambda p_m, \lambda q) + f((1-\lambda)p'_1, \ldots, (1-\lambda)p'_m, (1-\lambda)q') \\
&\quad \geq f(\lambda p_1 + (1-\lambda)p'_1, \ldots, \lambda p_m + (1-\lambda)p'_m, \lambda q + (1-\lambda)q'), \quad (19)
\end{aligned}
$$

i.e. f is jointly convex on boxes on $\mathbb{C}$ (thought of as a map $\mathbb{R}_{>0}^{m+1} \to \mathbb{R}_{>0}$). With the abbreviation $\delta = (1 - \sum_i \alpha_i)$ its Hesse matrix at $(p_1, \ldots, p_m, q) = (1, \ldots, 1)$ is

$$
\begin{bmatrix}
\alpha_1^2 - \alpha_1 & \alpha_1 \alpha_2 & \cdots & \alpha_1 \alpha_m & \alpha_1 \delta \\
\alpha_2 \alpha_1 & \alpha_2^2 - \alpha_2 & \cdots & \alpha_2 \alpha_m & \alpha_2 \delta \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
\alpha_m \alpha_1 & \alpha_m \alpha_2 & \cdots & \alpha_m^2 - \alpha_m & \alpha_m \delta \\
\delta \alpha_1 & \delta \alpha_2 & \cdots & \delta \alpha_m & \delta^2 - \delta
\end{bmatrix} = A - D, \qquad (20)
$$

where $A = \begin{bmatrix} \alpha_1 & \cdots & \alpha_m & \delta \end{bmatrix}^T \cdot \begin{bmatrix} \alpha_1 & \cdots & \alpha_m & \delta \end{bmatrix}$ and D is a diagonal matrix with entries $\alpha_1, \ldots, \alpha_m, \delta$. The difference must be positive semidefinite. Since A has rank 1, D can have at most one strictly positive eigenvalue. If there are none, then $\delta = 1 > 0$, a contradiction. Therefore there is a unique index i such that $\alpha_i > 0$ and for $i' \neq i$ we have $\alpha_{i'} = 0$. From the condition $1 - \alpha_i = \delta \leq 0$ we get $\alpha_i \geq 1$, i.e. (14) is the only possible form.

Now let f be a homomorphism into $\mathbb{TR}$. Then for boxes with full support we have

$$
\begin{aligned}
f(p_1,\ldots,p_m,q) &= \max_{x\in\mathscr{X}} f((p_1)_x,\ldots,(p_m)_x,q_x) \\
&= \max_{x\in\mathscr{X}} g(q_x)\prod_{i=1}^{m} h_i\left(\frac{(p_i)_x}{q_x}\right) \\
&= \max_{x\in\mathscr{X}} q_x^{\beta-\sum_{i=1}^{m}\alpha_i}\prod_{i=1}^{m}(p_i)_x^{\alpha_i}.
\end{aligned}
\tag{21}
$$

Comparing $(2,2,\ldots,2)$ and $1+1$ again, we now get $g(2)=g(1)$, and therefore $\beta=0$. From the normalization condition $f(u)=2$ we get $\sum_{i=1}^{m}\alpha_i=1$. Applying f to (18) results in the inequality

$$
\begin{aligned}
\max\{f(p_1,\ldots,&p_m,q),f(p_1',\ldots,p_m',q)\} \\
&\geq f(\lambda p_1+(1-\lambda)p_1',\ldots,\lambda p_m+(1-\lambda)p_m',\lambda q+(1-\lambda)q'), \quad (22)
\end{aligned}
$$

i.e. this time f is jointly quasiconvex on one-dimensional boxes (again, as a map $\mathbb{R}_{>0}^{m+1}\to\mathbb{R}_{>0}$). In particular, if we restrict f to a line segment then it is not possible to have a zero directional derivative and negative second derivative (strict local maximum). Suppose that there are two distinct indices $i<j$ such that $\alpha_i,\alpha_j>0$. We consider the point $(1,\ldots,1,1)$ and the direction $(0,\ldots,0,\alpha_j,0,\ldots,0,-\alpha_i,0,\ldots,0)$, where α_j is the ith component and $-\alpha_i$ is the jth component. The derivaties are

$$
\frac{\mathrm{d}}{\mathrm{d}s}f(1,\ldots,1,1+s\alpha_j,1,\ldots,1,1-s\alpha_i,1,\ldots,1)\bigg|_{s=0} = \alpha_i\alpha_j+\alpha_j(-\alpha_i)=0 \quad (23)
$$

$$
\begin{aligned}
\frac{\mathrm{d}^2}{\mathrm{d}s^2}&f(1,\ldots,1,1+s\alpha_j,1,\ldots,1,1-s\alpha_i,1,\ldots,1)\bigg|_{s=0} \\
&= \alpha_j^2\alpha_i(\alpha_i-1)+\alpha_i^2\alpha_j(\alpha_j-1)+2\alpha_j(-\alpha_i)\alpha_i\alpha_j = -\alpha_i\alpha_j(\alpha_i+\alpha_j)<0, \quad (24)
\end{aligned}
$$

a contradiction. Thus there is only one nonzero α_i which, by normalization, has to be 1.

Finally, the extension to general classical boxes with possibly unequal supports follows from a continuity argument as in [20]: if $(p_1,\ldots,p_m,q)$ is any classical box, then we have

$$
\begin{aligned}
(p_1+\varepsilon q,\ldots,p_m+\varepsilon q,q) &\succcurlyeq (p_1,\ldots,p_m,q) \\
&\succcurlyeq \left(\varepsilon\frac{\|p_1\|_1}{\|q\|_1}q+(1-\varepsilon)p_1,\ldots,\varepsilon\frac{\|p_1\|_1}{\|q\|_1}q+(1-\varepsilon)p_1,q\right) \quad (25)
\end{aligned}
$$

for every $\varepsilon\in(0,1)$ (in the first inequality choosing $T=\mathrm{id}$, in the second one $T(x)=\varepsilon\mathrm{Tr}(x)\frac{q}{\|q\|_1}+(1-\varepsilon)x$ in the definition). Let f be an element of the $\hat{\Delta}(\mathscr{B}_c,\preccurlyeq)$ and apply to (25) to get an upper and a lower bound on $f(p_1,\ldots,p_m,q)$. The bounds are of the form found above since all the supports are now equal to $\mathrm{supp}\,q$ and we can see that they converge to the same value as $\varepsilon\to 0$.

We turn to the semiring of quantum boxes, using that any monotone homomorphism on $\mathscr{B}_m$ must restrict to a monotone homomorphism on $\mathscr{B}_{c,m}$. As in [20], we show that there is only one possible extension. In that case it was possible to reduce the evaluation at a quantum pair to a classical one using the pinching map. However, that argument needs to be modified because it is not possible to transform a quantum box of multiple states into a classical one using a pinching map alone, since different pinched states need not commute with each other.

The pinching map is defined as follows (see [13] or [23, Section 2.6.3]). Let $\mathscr{H}$ be a finite dimensional Hilbert space and $A \in \mathscr{B}(\mathscr{H})$ a normal operator with spectral decomposition

$$A = \sum_{\lambda \in \mathrm{spec}(A)} \lambda P_\lambda, \tag{26}$$

where $(P_\lambda)_{\lambda \in \mathbb{C}}$ are pairwise disjoint orthogonal projections summing to I. The pinching map $\mathscr{P}_A : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H})$ is defined as

$$\mathscr{P}_A(X) = \sum_{\lambda \in \mathrm{spec}(A)} P_\lambda X P_\lambda. \tag{27}$$

Any operator in the image commutes with A and for $X \geq 0$ it satisfies the pinching inequality $|\mathrm{spec}(A)| \mathscr{P}_A(X) \geq X$.

Theorem 4 $\Delta(\mathscr{B}_m, \preccurlyeq)$ *consists of the maps*

$$\tilde{f}_{\alpha,i}(\rho_1, \ldots, \rho_m, \sigma) = \mathrm{Tr}\left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho_i \sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha \tag{28}$$

where $i = 1, 2, \ldots, m$ and $\alpha \in [1, \infty)$.

The monotone homomorphisms from $\mathscr{B}_m$ to $\mathbb{TR}$ that send $u = (2, 2, \ldots, 2, 1)$ to 2 are the maps

$$\tilde{f}_{\infty,i}(\rho_1, \ldots, \rho_m, \sigma) = \left\| \sigma^{-1/2} \rho_i \sigma^{-1/2} \right\|_\infty. \tag{29}$$

Proof It is readily verified that the expressions above give homomorphisms into the respective semirings, monotone by the data processing inequality for the sandwiched (or minimal) Rényi divergences [16]. We will show that these are the only possible extensions of the elements of $\hat{\Delta}(\mathscr{B}_{c,m}, \preccurlyeq)$ to $\mathscr{B}_m$.

Let $\alpha \in [1, \infty)$ and $i \in \{1, \ldots, m\}$, and let $\tilde{f}$ be any extension of $f_{\alpha,i}$. For a large enough $c \in \mathbb{R}_{>0}$ and every $n \in \mathbb{N}$ we have from the pinching inequality

$$(c^n I^{\otimes n}, \ldots, c^n I^{\otimes n}, |\mathrm{spec}(\sigma^{\otimes n})| \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n}), c^n I^{\otimes n}, \ldots, c^n I^{\otimes n}, \sigma^{\otimes n}) \succcurlyeq (\rho_1^{\otimes n}, \ldots, \rho_m^{\otimes n}, \sigma^{\otimes n}), \tag{30}$$

where the left hand side is classical, therefore

$$\tilde{f}(\rho_1, \ldots, \rho_m, \sigma) \leq \sqrt[n]{f_{\alpha,i}(c^n I^{\otimes n}, \ldots, c^n I^{\otimes n}, |\mathrm{spec}(\sigma^{\otimes n})| \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n}), c^n I^{\otimes n}, \ldots, c^n I^{\otimes n}, \sigma^{\otimes n}}$$

$$= \sqrt[n]{|\mathrm{spec}(\sigma^{\otimes n})|^\alpha \mathrm{Tr}\, \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n})^\alpha (\sigma^{\otimes n})^{1-\alpha}} \tag{31}$$

For a matching lower bound we consider the inequality ($|0\rangle$ is an additional orthogonal direction)

$$
\begin{aligned}
&(|0\rangle\langle 0| \oplus \rho_1^{\otimes n}, \ldots, |0\rangle\langle 0| \oplus \rho_m^{\otimes n}, C|0\rangle\langle 0| \oplus \sigma^{\otimes n}) \\
&\succcurlyeq (|0\rangle\langle 0|, \ldots, |0\rangle\langle 0|, |0\rangle\langle 0| \oplus \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n}), |0\rangle\langle 0|, \ldots, |0\rangle\langle 0|, C|0\rangle\langle 0| \oplus \sigma^{\otimes n}), \quad (32)
\end{aligned}
$$

which follows from the definition with $T = \mathrm{id}_{\mathbb{C}|0\rangle\langle 0|} \oplus \mathscr{P}_{\sigma^{\otimes n}}$. The right hand side is classical, therefore

$$
\begin{aligned}
C^{1-\alpha} + \tilde{f}(\rho_1, \ldots, \rho_m, \sigma)^n &\geq \mathrm{Tr}(|0\rangle\langle 0| \oplus \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n}))^\alpha (|0\rangle\langle 0| \oplus \sigma^{\otimes n})^{1-\alpha} \\
&= C^{1-\alpha} + \mathrm{Tr}\, \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n})^\alpha (\sigma^{\otimes n})^{1-\alpha},
\end{aligned} \quad (33)
$$

which leads to

$$
\tilde{f}(\rho_1, \ldots, \rho_m, \sigma) \geq \sqrt[n]{\mathrm{Tr}\, \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n})^\alpha (\sigma^{\otimes n})^{1-\alpha}}. \quad (34)
$$

From (31) and (34) and using $|\mathrm{spec}(\sigma^{\otimes n})|^{\alpha/n} \to 1$ we get

$$
\tilde{f}(\rho_1, \ldots, \rho_m, \sigma) = \lim_{n\to\infty} \sqrt[n]{\mathrm{Tr}\, \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n})^\alpha (\sigma^{\otimes n})^{1-\alpha}} = \mathrm{Tr}\left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha, \quad (35)
$$

where the last equality follows from [23, Proposition 4.12.] (see also [20, Theorem 4.4.]).

Consider now an extension $\tilde{f} : \mathscr{B}_m \to \mathbb{TR}$ of $f_{\infty,i}$. From (30) we get

$$
\tilde{f}(\rho_1, \ldots, \rho_m, \sigma) \leq \sqrt[n]{\left\| (\sigma^{\otimes n})^{-1/2} |\mathrm{spec}(\sigma^{\otimes n})| \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n})(\sigma^{\otimes n})^{-1/2} \right\|_\infty} \quad (36)
$$

and from (32) we get

$$
\max\{C, \tilde{f}(\rho_1, \ldots, \rho_m, \sigma)^n\} \geq \max\{C, \left\| (\sigma^{\otimes n})^{-1/2} \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n})(\sigma^{\otimes n})^{-1/2} \right\|_\infty\}. \quad (37)
$$

For small enough C the maximum equals the second argument on both sides, therefore

$$
\tilde{f}(\rho_1, \ldots, \rho_m, \sigma) \geq \sqrt[n]{\left\| (\sigma^{\otimes n})^{-1/2} \mathscr{P}_{\sigma^{\otimes n}}(\rho_i^{\otimes n})(\sigma^{\otimes n})^{-1/2} \right\|_\infty}. \quad (38)
$$

The upper and lower bounds converge as $n \to \infty$ and single out the unique quantum max-divergence (see [10] and [23, Section 4.2.4]), i.e.

$$
\tilde{f}(\rho_1, \ldots, \rho_m, \sigma) = 2^{D_{\max}(\rho_i\|\sigma)} = \left\| \sigma^{-1/2} \rho_i \sigma^{-1/2} \right\|_\infty. \quad (39)
$$

5 Conditions for catalytic, multi-copy, and asymptotic relative submajorization

We now specialize Theorem 2 to the preordered semiring $\mathscr{B}_m$. First we verify the polynomial growth condition by exhibiting a power universal element.

Proposition 3 *The box $u = (2,2,\ldots,2,1)$ on $\mathbb{C}$ is power universal.*

Proof Choosing $T = \mathrm{id}_{\mathscr{B}(\mathbb{C})}$ in Definition 2 we verify that $u \succcurlyeq 1$.

Let $(\rho_1,\ldots,\rho_m,\sigma)$ be a box on $\mathscr{H}$. We first find $k_1 \in \mathbb{N}$ such that $u^{k_1} \succcurlyeq (\rho_1,\ldots,\rho_m,\sigma)$. Let $T_1 : \mathscr{B}(\mathbb{C}) \to \mathscr{B}(\mathscr{H})$ be the map $T_1(x) = 2^{-k_1/2}x\sigma$. By choosing k_1 large enough we can ensure that T_1 is a completely positive trace nonincreasing map. It satisfies $T_1(1) = 2^{-k_1/2}\sigma \le \sigma$ and $T_1(2^{k_1}) = 2^{k_1/2}\sigma$, which is greater than ρ_i when k_1 is large, since $\mathrm{supp}\,\rho_i \subseteq \mathrm{supp}\,\sigma$.

To find a k_2 such that $u^{k_2}(\rho_1,\ldots,\rho_m,\sigma) \succcurlyeq 1$ we consider the map $T_2 : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathbb{C})$ given by $T_2(x) = 2^{-k_2/2}\frac{\mathrm{Tr}\,x}{\mathrm{Tr}\,\sigma}$. This is completely positive and also trace nonincreasing provided that k_2 is large enough. By construction, $T_2(\sigma) = 2^{-k_2/2} \le 1$. The remaining inequalities

$$1 \le T_2(2^{k_2}\rho_i) = 2^{k_2/2}\frac{\mathrm{Tr}\,\rho_i}{\mathrm{Tr}\,\sigma} \tag{40}$$

can also be ensured by choosing k_2 large enough.

With $k = \max\{k_1, k_2\}$ we have both $u^k \succcurlyeq (\rho_1,\ldots,\rho_m,\sigma)$ and $u^k(\rho_1,\ldots,\rho_m,\sigma) \succcurlyeq 1$ $\qquad\square$

Note that in addition to being a power universal element, the box u is also invertible: its multiplicative inverse is the box $u^{-1} = (\frac{1}{2},\ldots,\frac{1}{2},1)$. A consequence is that the implications of Theorem 2 can be simplified in that one may choose $k = 0$ or equivalently, there is no need to assume that x is power universal. Together with Theorem 4 this leads to the following condition.

Corollary 1 *Let $(\rho_1,\ldots,\rho_m,\sigma)$ and $(\rho'_1,\ldots,\rho'_m,\sigma')$ be elements of $\mathscr{B}_m$. Suppose that for every $i \in \{1,\ldots,m\}$ and $\alpha \in [1,\infty)$ the inequalities*

$$\mathrm{Tr}\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho_i\sigma^{\frac{1-\alpha}{2\alpha}}\right)^{\alpha} > \mathrm{Tr}\left(\sigma'^{\frac{1-\alpha}{2\alpha}}\rho'_i\sigma'^{\frac{1-\alpha}{2\alpha}}\right)^{\alpha} \tag{41}$$

as well as

$$\left\|\sigma^{-1/2}\rho_i\sigma^{-1/2}\right\|_{\infty} > \left\|\sigma'^{-1/2}\rho'_i\sigma'^{-1/2}\right\|_{\infty} \tag{42}$$

hold. Then

1. *for every sufficiently large n there is a completely positive trace nonincreasing map T such that*

$$\begin{aligned}\forall i \in \{1,\ldots,m\} : T(\rho_i^{\otimes n}) &\ge \rho'^{\otimes n} \\ T(\sigma^{\otimes n}) &\le \sigma'^{\otimes n},\end{aligned} \tag{43}$$

2. *there is a box $(\tau_1,\ldots,\tau_m,\omega)$ and a completely positive trace nonincreasing map T such that*

$$\begin{aligned}\forall i \in \{1,\ldots,m\} : T(\rho_i \otimes \tau_i) &\ge \rho'_i \otimes \tau_i \\ T(\sigma_i \otimes \omega_i) &\le \sigma'_i \otimes \omega_i.\end{aligned} \tag{44}$$

Our next goal is to apply Theorem 1. We start with a simple lemma.

Lemma 1 *Let $A \in \mathscr{B}(\mathscr{H})$, $A' \in \mathscr{B}(\mathscr{H}')$, $A, A' \geq 0$ and $\|A'\|_\infty \leq \|A\|_\infty$. Then there exists a completely positive unital map $\Phi : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H}')$ such that $\Phi(A) \geq \Phi(A')$.*

Proof Let ψ be an eigenvector of A with eigenvalue $\|A\|_\infty$ with $\|\psi\| = 1$. Let $\Phi(X) = \langle \psi | X | \psi \rangle I$. This map is completely positive and unital and satisfies

$$\Phi(A) = \langle \psi | A | \psi \rangle I = \|A\|_\infty I \geq \|A'\|_\infty I \geq A'. \tag{45}$$

Proposition 4 *Let $(\rho_1, \ldots, \rho_m, \sigma)$ and $(\rho_1', \ldots, \rho_m', \sigma)$ be boxes and suppose that*

$$\frac{\tilde{f}_{i,\alpha}(\rho_1', \ldots, \rho_m', \sigma')}{\tilde{f}_{i,\alpha}(\rho_1, \ldots, \rho_m, \sigma)} \tag{46}$$

is bounded for every i as $\alpha \to \infty$. Then there exists an $r \in \mathbb{N}$ such that $(\rho_1', \ldots, \rho_m', \sigma') \precsim r \cdot (\rho_1, \ldots, \rho_m, \sigma)$.

Proof Under the assumptions of the proposition,

$$\begin{aligned}
\infty > \lim_{\alpha \to \infty} \log & \frac{\tilde{f}_{i,\alpha}(\rho_1', \ldots, \rho_m', \sigma')}{\tilde{f}_{i,\alpha}(\rho_1, \ldots, \rho_m, \sigma)} \\
&= \lim_{\alpha \to \infty} (\alpha - 1) \left(\widetilde{D}_\alpha \left(\rho_i' \| \sigma' \right) - \widetilde{D}_\alpha \left(\rho_i \| \sigma \right) \right).
\end{aligned} \tag{47}$$

The limit of the first factor is ∞, therefore the limit of the second factor (which is known to exist) must be at most 0, i.e. $\widetilde{D}_\infty(\rho_i' \| \sigma') \leq \widetilde{D}_\infty(\rho_i \| \sigma)$. Using the explicit form of the Rényi divergence of order ∞ we conclude

$$\left\| \sigma'^{-1/2} \rho_i' \sigma'^{-1/2} \right\|_\infty \leq \left\| \sigma^{-1/2} \rho_i \sigma^{-1/2} \right\|_\infty. \tag{48}$$

Let $\tilde{\Phi}_i : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H}')$ be a completely positive unital map such that $\tilde{\Phi}_i(\sigma^{-1/2} \rho_i \sigma^{-1/2}) \geq \sigma'^{-1/2} \rho_i' \sigma'^{-1/2}$ (from Lemma 1) and consider the maps

$$\Phi_i(X) = \sigma'^{1/2} \tilde{\Phi}_i(\sigma^{-1/2} X \sigma^{-1/2}) \sigma'^{1/2}. \tag{49}$$

These are completely positive and satisfy $\Phi_i(\sigma) = \sigma'$ and $\Phi_i(\rho_i) \geq \rho_i'$. Choose $r \in \mathbb{N}$ such that

$$r \geq \max_i \|\Phi_i\|_{1-1} \tag{50}$$

and let

$$T_n = \frac{1}{mr^n} \sum_{i=1}^m \Phi_i^{\otimes n}. \tag{51}$$

For every n this map is trace nonincreasing and therefore

$$\begin{aligned}
u^{\lfloor \log m \rfloor} \left(r \cdot (\rho_1, \ldots, \rho_m, \sigma) \right)^n &\succsim (mr^n \rho_1^{\otimes n}, \ldots, mr^n \rho_m^{\otimes n}, r^n \sigma^{\otimes n}) \\
&\succsim (T_n(mr^n \rho_1^{\otimes n}), \ldots, T_n(mr^n \rho_m^{\otimes n}), T_n(r^n \sigma^{\otimes n})) \\
&\succsim (\Phi_1^{\otimes n}(\rho_1^{\otimes n}), \ldots, \Phi_m^{\otimes n}(\rho_m^{\otimes n}), T_n(r^n \sigma^{\otimes n})) \\
&\succsim (\rho_1', \ldots, \rho_m', \sigma').
\end{aligned} \tag{52}$$

This proves that $r \cdot (\rho_1, \ldots, \rho_m, \sigma) \succsim (\rho_1', \ldots, \rho_m', \sigma')$.

Together with Theorem 1 the last proposition and the classification in Theorem 4 leads to the following explicit condition.

Corollary 2 *Let* $(\rho_1,\ldots,\rho_m,\sigma)$ *and* $(\rho'_1,\ldots,\rho'_m,\sigma')$ *be elements of* $\mathscr{B}_m$. *The following are equivalent:*

1. for every $i \in \{1,\ldots,m\}$ *and* $\alpha \in [1,\infty)$ *the inequalities*

$$\mathrm{Tr}\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho_i\sigma^{\frac{1-\alpha}{2\alpha}}\right)^{\alpha} \geq \mathrm{Tr}\left(\sigma'^{\frac{1-\alpha}{2\alpha}}\rho'_i\sigma'^{\frac{1-\alpha}{2\alpha}}\right)^{\alpha} \tag{53}$$

hold,
2. $(\rho_1,\ldots,\rho_m,\sigma) \succsim (\rho'_1,\ldots,\rho'_m,\sigma')$.

6 Application to state discrimination

6.1 Composite null hypothesis

One interpretation of a (normalized) box is that the states $\rho_1,\ldots,\rho_m$ form a composite null hypothesis which is to be tested again the simple alternative hypothesis σ. In this hypothesis testing problem one considers a two-outcome POVM $(\Pi, I - \Pi)$, or *test*, and the decision is based on the measurement result, rejecting the null hypothesis if the second outcome is observed. Such a test is uniquely specified by an operator Π such that $0 \leq \Pi \leq I$ and every such operator gives rise to a valid POVM.

A type I error occurs when the null hypothesis is falsely rejected. For every member in the family $\rho_1,\ldots,\rho_m$ we define a probability of type I error,

$$\alpha_i(\Pi) = \mathrm{Tr}\,\rho_i(I - \Pi) = 1 - \mathrm{Tr}\,\rho_i\Pi, \tag{54}$$

and the maximum

$$\alpha(\Pi) = \max_i \alpha_i(\Pi) \tag{55}$$

is the *significance level* of the test.

In contrast, a type II error means that the correct state was σ but the null hypothesis does not get rejected. The probability of a type II error is

$$\beta(\Pi) = \mathrm{Tr}\,\sigma\Pi. \tag{56}$$

In general it is not possible to have a low probability for both types of errors but there is a trade-off between the two quantities. The possible values are exactly characterized by the preordered semiring $(\mathscr{B}, \preccurlyeq)$ as follows.

Proposition 5 *Let* $(\rho_1,\ldots,\rho_m,\sigma)$ *be a normalized box and* $\alpha,\beta \in [0,1]$. *The following are equivalent:*

1. there exists a test Π *with* $\alpha(\Pi) \leq \alpha$ *and* $\beta(\Pi) \leq \beta$
2. $(\rho_1,\ldots,\rho_m,\sigma) \succcurlyeq ((1-\alpha),\ldots,(1-\alpha),\beta)$

Proof Let $(\rho_1,\ldots,\rho_m,\sigma)$ be a normalized box on $\mathscr{H}$ and suppose that a test exists with the properties above. Consider the map $T : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathbb{C})$ given by $T(X) = \mathrm{Tr}(X\Pi)$. T is completely positive because $\Pi \geq 0$ and trace nonincreasing because $\Pi \leq I$. We apply T to the box:

$$\begin{aligned} T(\rho_i) &= \mathrm{Tr}(\rho_i \Pi) = 1 - \alpha_i(\Pi) \geq 1 - \alpha(\Pi) \geq 1 - \alpha \\ T(\sigma) &= \mathrm{Tr}(\sigma \Pi) = \beta(\Pi) \leq \beta, \end{aligned} \tag{57}$$

therefore $(\rho_1,\ldots,\rho_m,\sigma) \succcurlyeq ((1-\alpha),\ldots,(1-\alpha),\beta)$.

Conversely, suppose that $(\rho_1,\ldots,\rho_m,\sigma) \succcurlyeq ((1-\alpha),\ldots,(1-\alpha),\beta)$. This means that there exists a completely positive trace nonincreasing map $T : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathbb{C})$ such that $T(\rho_i) \geq 1 - \alpha$ and $T(\sigma) \leq \beta$. Pick such a map and let $\Pi = T^*(1)$ (where $1 = \mathrm{id}_{\mathbb{C}}$ is the identity map of $\mathbb{C}$). Then $0 \leq \Pi \leq I$ and

$$\begin{aligned} \alpha_i(\Pi) &= \mathrm{Tr}\,\rho_i(I - \Pi) = 1 - \mathrm{Tr}\,\rho_i T^*(1) = 1 - T(\rho_i) \leq \alpha \\ \beta(\Pi) &= \mathrm{Tr}\,\sigma\Pi = \mathrm{Tr}\,\sigma T^*(1) = T(\sigma) \leq \beta, \end{aligned} \tag{58}$$

therefore also $\alpha(\Pi) \leq \alpha$.

Suppose that we have access to n copies of such identically prepared boxes. The resource object describing this situation is the power $(\rho_1,\ldots,\rho_m,\sigma)^n = (\rho_1^{\otimes n},\ldots,\rho_m^{\otimes n},\sigma^{\otimes n})$. If we are allowed to perform a joint measurement then we expect to be able to achieve lower probabilities of both types of errors than with a single copy. In particular, an extension of the quantum Stein lemma says that when $n \to \infty$ and the probability of the type I error is required to go to 0, it is possible to achieve an exponential decay of the type II error, where the exponent is given by the minimum of the relative entropies $D(\rho_i\|\sigma)$ [4].

The asymptotic preorder $\succsim$ is able to capture the exponential decay of the type II error and the exponential convergence of the type I error to *one*, called the strong converse regime. More precisely, we have the following characterization.

Proposition 6 *The following are equivalent*

1. *there is a sequence of tests Π_n on $\mathscr{H}^{\otimes n}$ for which the type I error is less than $1 - 2^{-Rn+o(n)}$ and at the same time the type II error decreases as fast as 2^{-rn}*
2. $(\rho_1,\ldots,\rho_m,\sigma) \succsim (2^{-R},\ldots,2^{-R},2^{-r})$.

Proof Since u is invertible, the condition appearing in the definition of the asymptotic preorder may be written as

$$\begin{aligned} (\rho_1^{\otimes n},\ldots,\rho_m^{\otimes n},\sigma^{\otimes n}) &\succcurlyeq u^{-k_n}(2^{-R},\ldots,2^{-R},2^{-r})^n \\ &= (2^{-Rn-k_n},\ldots,2^{-Rn-k_n},2^{-rn}) \end{aligned} \tag{59}$$

where $k_n/n \to 0$. According to Proposition 5, this is equivalent to the existence of a sequence of tests Π_n such that $\alpha(\Pi_n) \leq 1 - 2^{-Rn-k_n}$ and $\beta(\Pi_n) \leq 2^{-rn}$ with $k_n \in o(n)$ as claimed.

To achieve asymptotically the smallest type II error probability for a given exponent r, we need to find the smallest R satisfying the equivalent conditions. Denoting this value by $R^*(r)$, Proposition 6 and Corollary 2 implies

$$R^*(r) = \max_i \sup_{\alpha > 1} \frac{\alpha - 1}{\alpha} \left[r - \widetilde{D}_\alpha \left(\rho_i \| \sigma \right) \right]. \tag{60}$$

In particular, the exponent is given by the minimum of the pairwise exponents [16] similarly as in the extended Stein lemma. Note that this result can also be obtained from the simple null hypothesis case by an averaging argument. For completeness we include this proof in the appendix, see Proposition 9.

6.2 Multiple hypotheses

In a multiple state discrimination problem one performs a measurement with multiple outcomes, one corresponding to each of the possible states. Mathematically, such a measurement is described by a POVM $(\Pi_1, \ldots, \Pi_m, I - (\Pi_1 + \cdots + \Pi_m))$ on a set of size $m + 1$. Upon observing the outcome $i \in [m + 1]$, the experimenter concludes that the unknown state was ρ_i (σ). In such a setting one can define $(m + 1)m$ different error probabilities depending on which state is incorrectly identified as which other state. Alternatively, one may form $m + 1$ probabilities of successful detections (these are of course functionally related to the error probabilities). In our framework it is possible to control $2m$ of these probabilities as follows.

Proposition 7 *Let* $(\rho_1, \ldots, \rho_m, \sigma)$ *be a normalized box and* $a_1, \ldots, a_m, b_1, \ldots, b_m \in [0,1]$. *Let* $|1\rangle, \ldots, |m\rangle$ *be an orthonormal basis in* $\mathbb{C}^m$ *and consider the operator*

$$b = \sum_{i=1}^m b_i |i\rangle\langle i|. \tag{61}$$

Then the following are equivalent:

1. *there exists a POVM* $(\Pi_1, \ldots, \Pi_m, I - (\Pi_1 + \cdots + \Pi_m))$ *with*

$$\mathrm{Tr}\, \rho_i \Pi_i \geq a_i \tag{62}$$

   and

$$\mathrm{Tr}\, \sigma \Pi_i \leq b_i \tag{63}$$

   for every $1 \leq i \leq m$.
2. $(\rho_1, \ldots, \rho_m, \sigma) \succcurlyeq (a_1 |1\rangle\langle 1|, \ldots, a_m |m\rangle\langle m|, b)$.

Proof Suppose that $(\Pi_1, \ldots, \Pi_m, I - (\Pi_1 + \cdots + \Pi_m))$ is a POVM satisfying the conditions. Consider the channel $T : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathbb{C}^m)$

$$T(X) = \sum_{j=1}^m \left(\mathrm{Tr}\, X \Pi_j \right) |j\rangle\langle j|. \tag{64}$$

It satisfies

$$T(\rho_i) = \sum_{j=1}^{m} (\mathrm{Tr}\,\rho_i \Pi_j) \, |j\rangle\langle j| \geq (\mathrm{Tr}\,\rho_i \Pi_i) \, |i\rangle\langle i| \geq a_i \, |i\rangle\langle i|$$

$$T(\sigma) = \sum_{j=1}^{m} (\mathrm{Tr}\,\sigma \Pi_j) \, |j\rangle\langle j| \leq \sum_{j=1}^{m} b_j \, |j\rangle\langle j| = b,$$

therefore $(\rho_1, \ldots, \rho_m, \sigma) \succcurlyeq (a_1 \, |1\rangle\langle 1|, \ldots, a_m \, |m\rangle\langle m|, b)$.

Conversely, suppose that $(\rho_1, \ldots, \rho_m, \sigma) \succcurlyeq (a_1 \, |1\rangle\langle 1|, \ldots, a_m \, |m\rangle\langle m|, b)$. This means that there is a channel $T : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathbb{C}^m)$ satisfying

$$T(\rho_i) \geq a_i \, |i\rangle\langle i|$$
$$T(\sigma) \leq b.$$

Let T be such a channel and consider the operators $\Pi_i = T^*(|i\rangle\langle i|)$. These are positive and satisfy

$$\sum_i \Pi_i = T^*(\sum_i |i\rangle\langle i|) = T^*(I) \leq I, \tag{65}$$

therefore $(\Pi_1, \ldots, \Pi_m, I - (\Pi_1 + \cdots + \Pi_m))$ is a POVM. We estimate the probabilities as

$$\mathrm{Tr}\,\rho_i \Pi_i = \mathrm{Tr}\,\rho_i T^*(|i\rangle\langle i|) = \langle i| \, T(\rho_i) \, |i\rangle \geq \langle i| \, a_i \, |i\rangle \, \langle i|i\rangle = a_i$$
$$\mathrm{Tr}\,\sigma \Pi_i = \mathrm{Tr}\,\sigma T^*(|i\rangle\langle i|) = \langle i| \, T(\sigma) \, |i\rangle \leq \langle i| \, b \, |i\rangle = b_i. \tag{66}$$

Next we relate the asymptotic preorder to measurements on multiple copies of the same unknown state. This is not as straightforward as the extension in the case of a composite hypothesis, because the powers of a box of the form $(a_1 \, |1\rangle\langle 1|, \ldots, a_m \, |m\rangle\langle m|, B)$ are not of the same form.

Lemma 2 *Let* $a_1, \ldots, a_m, b_1, \ldots, b_m \in [0, 1]$ *and*

$$B = \sum_{i=1}^{m} b_i \, |i\rangle\langle i|. \tag{67}$$

as in Proposition 7. Then for every $n \in \mathbb{N}$, $n \geq 1$ *the inequalities*

$$(a_1 \, |1\rangle\langle 1|, \ldots, a_m \, |m\rangle\langle m|, B)^{\otimes n} \succcurlyeq (a_1^n \, |1\rangle\langle 1|, \ldots, a_m^n \, |m\rangle\langle m|, B^n) \tag{68}$$

and

$$(a_1 \, |1\rangle\langle 1|, \ldots, a_m \, |m\rangle\langle m|, B)^{\otimes n} \preccurlyeq (a_1^n \, |1\rangle\langle 1|, \ldots, a_m^n \, |m\rangle\langle m|, B^n) \tag{69}$$

hold.

Proof For the first inequality, consider the map $T : \mathscr{B}(\mathbb{C}^{m \otimes n}) \to \mathscr{B}(\mathbb{C}^m)$ given as

$$T(X) = \sum_{j=1}^{m} |j\rangle\langle jj \ldots j| \, X \, |jj \ldots j\rangle\langle j|. \tag{70}$$

Then T is completely positive and trace nonincreasing, $T((a_i|i\rangle\langle i|)^{\otimes n}) = a_i^n |i\rangle\langle i|$ and $T(B^{\otimes n}) = B^n$.

For the second inequality, consider the map $T : \mathscr{B}(\mathbb{C}^m) \to \mathscr{B}((\mathbb{C}^m)^{\otimes n})$ defined as

$$T(X) = \sum_{j=1}^m |jj\ldots j\rangle\langle j|Xj|jj\ldots j\rangle\langle .| \tag{71}$$

Then T is completely positive and trace nonincreasing, $T(a_i^n|i\rangle\langle i|) = a_i^n|ii\ldots i\rangle\langle ii\ldots i| = (a_i|i\rangle\langle i|)^{\otimes n}$ and

$$\begin{aligned}
T(B^n) &= \sum_{j=1}^m |jj\ldots j\rangle\langle j| \left(\sum_{i=1}^m b_i^n |i\rangle\langle i| \right) |j\rangle\langle jj\ldots j| \\
&= \sum_{i=1}^m b_i^n |ii\ldots i\rangle\langle ii\ldots i| \\
&\leq B^{\otimes n}.
\end{aligned} \tag{72}$$

With the help of Lemma 2 we can prove the analogue of Proposition 6.

Proposition 8 *Let $(\rho_1,\ldots,\rho_m,\sigma)$ be a box and $r_1,\ldots,r_m,R_1,\ldots,R_m \geq 0$, and consider the operator $r = \sum_{i=1}^m r_i |i\rangle\langle i|$. The following are equivalent*

1. *there exists a sequence of POVMs $(\Pi_{n,1},\ldots,\Pi_{n,m},I-(\Pi_{n,1}+\cdots+\Pi_{n,m}))$ such that for all $i \in \{1,\ldots,m\}$ the observed probabilities behave as*

$$\begin{aligned}
\mathrm{Tr}\,\rho_i^{\otimes n}\Pi_{n,i} &\geq 2^{-R_i n + o(n)} \\
\mathrm{Tr}\,\sigma^{\otimes n}\Pi_{n,i} &\leq 2^{-r_i n}.
\end{aligned} \tag{73}$$

2. $(\rho_1,\ldots,\rho_m,\sigma) \succsim (2^{-R_1}|1\rangle\langle 1|,\ldots,2^{-R_m}|m\rangle\langle m|,2^{-r})$.

Proof The asymptotic relation is equivalent to

$$\begin{aligned}
(\rho_1^{\otimes n},\ldots,\rho_m^{\otimes n},\sigma^{\otimes n}) &\succsim u^{-k_n}(2^{-R_1}|1\rangle\langle 1|,\ldots,2^{-R_m}|m\rangle\langle m|,2^{-r})^n \\
&\succsim (2^{-R_1 n-k_n}|1\rangle\langle 1|,\ldots,2^{-R_m n-k_n}|m\rangle\langle m|,2^{-rn})
\end{aligned} \tag{74}$$

by Lemma 2, where $k_n/n \to 0$. Proposition 7 in turn says that this is equivalent to the existence of a sequence of POVMs $(\Pi_{n,1},\ldots,\Pi_{n,m},I-(\Pi_{n,1}+\cdots+\Pi_{n,m}))$ such that $\mathrm{Tr}\,\rho_i^{\otimes n}\Pi_{n,i} \geq 2^{-R_i n-k_n}$ and $\mathrm{Tr}\,\sigma^{\otimes n}\Pi_{n,i} \leq 2^{-r_i n}$ for all $i \in \{1,\ldots,m\}$ with $k_n \in o(n)$.

From Corollary 2 we get that the exponents $R_1,\ldots,R_m,r_1,\ldots,r_m$ are achievable iff for all $i \in \{1,\ldots,m\}$ the inequality

$$R_i \geq \sup_{\alpha>1} \frac{\alpha-1}{\alpha} \left[r_i - \widetilde{D}_\alpha(\rho_i\|\sigma) \right] \tag{75}$$

holds.

7 Appendix: composite null hypothesis

Proposition 9 *Let* $(\rho_1, \ldots, \rho_m, \sigma)$ *be a normalized box and suppose that for every* $i \in [m]$ *there is a sequence of tests* Π_n^i *such that* $\alpha_i\left(\Pi_n^i\right) = \text{Tr}\,\rho_i^{\otimes n}\left(I - \Pi_n^i\right) \leq 1 - 2^{-nR_i + o(n)}$ *and at the same time* $\beta\left(\Pi_n^i\right) = \text{Tr}\,\sigma^{\otimes n}\Pi_n^i \leq 2^{-nr}$. *Then for the sequence of tests* $\tilde{\Pi}_n = \frac{1}{m}\sum_{i=1}^{m}\Pi_n^i$ *we have* $\alpha\left(\tilde{\Pi}_n\right) = \max_i \alpha_i\left(\tilde{\Pi}_n\right) \leq 1 - 2^{-n\max(R_i) + o(n)}$ *and* $\beta\left(\tilde{\Pi}_n\right) \leq 2^{-nr}$.

Proof

$$\beta\left(\tilde{\Pi}_n\right) = \text{Tr}\left(\sigma^{\otimes n}\tilde{\Pi}_n\right) = \frac{1}{m}\sum_{i=1}^{m}\text{Tr}\left(\sigma^{\otimes n}\Pi_n^i\right) = \frac{1}{m}\sum_{i=1}^{m}\beta\left(\Pi_n^i\right) \leq 2^{-nr}, \tag{76}$$

and

$$\begin{aligned}
\alpha\left(\tilde{\Pi}_n\right) = \max_i \alpha_i\left(\tilde{\Pi}_n\right) &= \max_i \text{Tr}\,\rho_i^{\otimes n}\left(I - \frac{1}{m}\sum_{j=1}^{m}\Pi_n^j\right) \\
&\leq \max_i \text{Tr}\,\rho_i^{\otimes n}\left(I - \frac{1}{m}\Pi_n^i\right) \leq \frac{1}{m}\left[(m-1) + \max_i\left(1 - 2^{-nR_i + o(n)}\right)\right] \\
&= 1 - 2^{-n\max(R_i) + o(n) - \log m} = 1 - 2^{-n\max(R_i) + o(n)}.
\end{aligned} \tag{77}$$

Conflict of interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Bae, J., Kwek, L.C.: Quantum state discrimination and its applications. Journal of Physics A: Mathematical and Theoretical **48**(8), 083001 (2015). DOI 10.1088/1751-8113/48/8/083001
2. Barnett, S.M., Croke, S.: Quantum state discrimination. Advances in Optics and Photonics **1**(2), 238–278 (2009). DOI 10.1364/AOP.1.000238
3. Mario Berta, Fernando G. S. L. Brandao, and Christoph Hirche. On Composite Quantum Hypothesis Testing. *arXiv:1709.07268 [math-ph, physics:quant-ph]*, September 2017.
4. Bjelaković, I., Deuschel, J.D., Krüger, T., Seiler, R., Siegmund-Schultze, R., Szkoła, A.: A quantum version of Sanov's theorem. Communications in mathematical physics **260**(3), 659–671 (2005). DOI 10.1007/s00220-005-1426-2
5. Fernando G. S. L. Brandao and Martin B. Plenio. A Generalization of Quantum Stein's Lemma. *Communications in Mathematical Physics*, 295(3):791–828, May 2010.
6. Buscemi, F., Sutter, D., Tomamichel, M.: An information-theoretic treatment of quantum dichotomies. Quantum **3**, 209 (2019). DOI 10.22331/q-2019-12-09-209
7. Chefles, A.: Quantum state discrimination. Contemporary Physics **41**(6), 401–424 (2000). DOI 10.1080/00107510010002599
8. Chitambar, E., Gour, G.: Quantum resource theories. Reviews of Modern Physics **91**(2), 025001 (2019). DOI 10.1103/RevModPhys.91.025001
9. Dahl, G.: Matrix majorization. Linear Algebra and Its Applications **288**, 53–73 (1999). DOI 10.1016/S0024-3795(98)10175-1

10. Datta, N.: Min-and max-relative entropies and a new entanglement monotone. IEEE Transactions on Information Theory **55**(6), 2816–2826 (2009). DOI 10.1109/TIT.2009.2018325

11. Tobias Fritz. A generalization of Strassen's Positivstellensatz. *Communications in Algebra*, **49**(2):482–499, February 2021. DOI 10.1080/00927872.2020.1803344

12. Fritz, T.: A local-global principle for preordered semirings and abstract Positivstellensätze (2020)

13. Hayashi, M.: Optimal sequence of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing. Journal of Physics A: Mathematical and General **35**(50), 10759 (2002). DOI 10.1088/0305-4470/35/50/307

14. Hiai, F., Petz, D.: The proper formula for relative entropy and its asymptotics in quantum probability. Communications in mathematical physics **143**(1), 99–114 (1991). DOI 10.1007/BF02100287

15. Matsumoto, K.: Reverse test and characterization of quantum relative entropy (2010)

16. Mosonyi, M., Ogawa, T.: Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies. Communications in Mathematical Physics **334**(3), 1617–1648 (2015). DOI 10.1007/s00220-014-2248-x

17. Milán Mosonyi, Zsombor Szilágyi, and Mihály Weiner. On the error exponents of binary state discrimination with composite hypotheses. *arXiv:2011.04645 [math-ph, physics:quant-ph]*, May 2021.

18. Müller-Lennert, M., Dupuis, F., Szehr, O., Fehr, S., Tomamichel, M.: On quantum Rényi entropies: A new generalization and some properties. Journal of Mathematical Physics **54**(12), 122203 (2013). DOI 10.1063/1.4838856

19. Ogawa, T., Nagaoka, H.: Strong converse and Stein's lemma in quantum hypothesis testing. In: Asymptotic Theory Of Quantum Statistical Inference: Selected Papers, pp. 28–42. World Scientific (2005). DOI 10.1142/9789812563071_0003

20. Perry, C., Vrana, P., Werner, A.H.: The semiring of dichotomies and asymptotic relative submajorization (2020)

21. Renes, J.M.: Relative submajorization and its use in quantum resource theories. Journal of Mathematical Physics **57**(12), 122202 (2016). DOI 10.1063/1.4972295

22. Strassen, V.: The asymptotic spectrum of tensors. Journal für die reine und angewandte Mathematik **384**, 102–152 (1988). DOI 10.1515/crll.1988.384.102

23. Tomamichel, M.: Quantum Information Processing with Finite Resources: Mathematical Foundations, vol. 5. Springer (2015). DOI 10.1007/978-3-319-21891-5

24. Péter Vrana. A Generalization of Strassen's Theorem on Preordered Semirings. *Order*, July 2021. DOI 10.1007/s11083-021-09570-7

25. Wang, X., Wilde, M.M.: Resource theory of asymmetric distinguishability. Physical Review Research **1**(3), 033170 (2019). DOI 10.1103/PhysRevResearch.1.033170

26. Wilde, M.M., Winter, A., Yang, D.: Strong converse for the classical capacity of entanglement-breaking and hadamard channels via a sandwiched Rényi relative entropy. Communications in Mathematical Physics **331**(2), 593–622 (2014). DOI 10.1007/s00220-014-2122-x