

Against probability:

A quantum state is more than a list of probability distributions

Ladina Hausmann and Renato Renner

Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland

ABSTRACT. The state ρ of a quantum system can be represented by a vector $\mathbf{P}_{\mathcal{M}}(\rho)$ of outcome probabilities for a set of measurements \mathcal{M} . Such representations appear throughout physics, for example, in quantum field theory via correlation functions and in quantum foundations within generalized probabilistic frameworks. In this work, we identify an unavoidable tension: to enable operationally meaningful statements, the map $\rho \mapsto \mathbf{P}_{\mathcal{M}}(\rho)$ must be topologically robust—preserving the notion of closeness between states. Yet, a probability representation that is topologically robust cannot simultaneously retain other essential structure, such as the subsystem structure.

1 Introduction and a first example

Let $P_M(\rho)$ denote the probability distribution obtained by measuring a quantum state $\rho \in \mathcal{D}(\mathcal{H})$ on a separable Hilbert space \mathcal{H} . If one collects these probability distributions for all measurements M from a tomographically complete set \mathcal{M} , the resulting tuple $\mathbf{P}_{\mathcal{M}}(\rho) := (P_M(\rho))_{M \in \mathcal{M}}$ uniquely specifies the quantum state ρ . Such probability representations arise, for instance, when considering correlation functions in quantum field theories [1], and are also widespread in quantum information theory and quantum foundations [2–17].

In this work, we ask the following question: does $\mathbf{P}_{\mathcal{M}}(\rho)$ represent ρ faithfully? If faithfulness meant injectivity, the answer would be yes, as this is precisely the notion of tomographic completeness. However, this criterion is too weak. To be faithful in a physically meaningful sense, a representation must also be *topologically robust*. A main contribution of this paper is to define and explain what this means.

We begin with an example where the use of probability representations appears natural: generating random bits R_1, \dots, R_ℓ from a quantum process. For concreteness, imagine a protocol that produces each bit R_i as follows: prepare n unstable atoms and count the number of decays within a fixed time interval (e.g., one second). Set $R_i = 0$ if this number is even and $R_i = 1$ otherwise.

An ℓ -bit string $R = R_1 \cdots R_\ell$ is said to be *random* if it cannot be predicted with probability greater than $2^{-\ell}$, even by an all-powerful agent with access to any side information E available prior to the process, such as the internal state of the source supplying the atoms. Formally, this means that the joint state $\rho = \rho_{RE}$ of R and E belongs to the set

$$\Sigma^{\text{rand}} := \left\{ \bar{\Pi}_R^{(\ell)} \otimes \sigma_E \mid \ell \in \mathbb{N}, \sigma_E \in \mathcal{D}(E) \right\} \quad (1.1)$$

where $\bar{\Pi}_R^{(\ell)}$ is the uniform state on bit strings of length ℓ , and $\mathcal{D}(E)$ is the set of density operators on E .

In any practical randomness-generation protocol, the output R inevitably has residual correlations with other systems. Moreover, since R is produced by a quantum process, it is not automatically classical: in general, the joint state ρ_{RE} is not a cq-state. Consequently, condition (1.1) cannot be achieved exactly, but only approached asymptotically by investing additional resources [18–20], for instance by increasing the number n of atoms in our example protocol. For this reason, it is standard to adopt an approximate condition of the form

$$\lim_{n \rightarrow \infty} \delta(\rho^{(n)}, \Sigma^{\text{rand}}) = 0, \quad (1.2)$$

where $\delta(\rho^{(n)}, \Sigma^{\text{rand}}) := \inf_{\sigma \in \Sigma^{\text{rand}}} \delta(\rho^{(n)}, \sigma)$, with $\delta(\cdot, \cdot)$ denoting the trace distance. Operationally, this quantifies the maximal probability with which an agent with access to both R and E can distinguish $\rho^{(n)}$ from the ideal behaviour defined by Σ^{rand} [21, 22].

To work at the level of probability representations, one requires that such approximate conditions be expressible via a distance measure defined directly on probability distributions, such as the statistical distance. The non-triviality of this requirement is best illustrated by a concrete example: a sequence of states $\rho^{(n)}$ that violates (1.2), while this violation remains invisible in the corresponding probability representation.

Example. For any $n \in \mathbb{N}$, let R and E be 2^n -dimensional systems, and the joint state of R and E after the randomness generation protocol be

$$\rho_{RE}^{(n)} \propto \sum_{1 \leq u < v \leq 2^n} \pi_{u,v} \quad (1.3)$$

where $\pi_{u,v}$ denotes the projector on the subspace of RE spanned by $|u\rangle_R |v\rangle_E - |v\rangle_R |u\rangle_E$, for an arbitrary choice of orthonormal bases. This state is entangled and thus distinct from the states in Σ^{rand} , which are separable. Concretely, as shown in [23, Example II.9.],

$$\forall n \in \mathbb{N} : \delta(\rho^{(n)}, \Sigma^{\text{rand}}) \geq \frac{1}{4}. \quad (1.4)$$

Therefore, R is not approximately random according to criterion (1.2).

Before resuming this example at the level of the probability representation $\mathbf{P}_{\mathcal{M}}$, we must clarify the requirements on the underlying set \mathcal{M} of measurements. While one could, in principle, allow arbitrary measurements on the joint system RE , these generally fail to respect the subsystem structure, thus erasing the distinction between R and E . Yet, this distinction is precisely what allows us to phrase definitions like (1.1). Accordingly, it is common to restrict \mathcal{M} to measurements acting locally on R and E .

Example (continued). For illustrative purposes, we focus on measurements of the form $M \otimes M$ where M consists of rank-1 projectors only.¹ Exploiting the antisymmetry of $\rho_{RE}^{(n)}$, it is straightforward to verify that the joint probability distribution $P_{M \otimes M} = P_{M \otimes M}(\rho_{RE}^{(n)})$ of the outcomes X and Y is given by

$$P_{M \otimes M}(x, y) = \begin{cases} 0 & \text{if } x = y \\ \frac{1}{2^n(2^n - 1)} & \text{else.} \end{cases} \quad (1.5)$$

¹The conclusions of this example can be easily generalized to any measurement acting locally on R and E . For this, it suffices to observe that the state on E conditioned on any outcome of a rank-1 measurement applied to R is maximally mixed on a subspace of dimension $2^n - 1$, which is 2^{-n} -close to $\bar{\Pi}_E^{(n)}$.

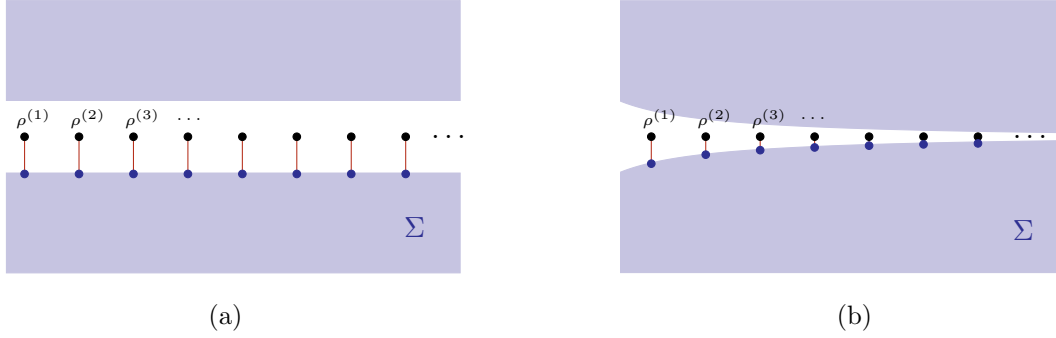


Figure 1: **Non-robustness of $\mathbf{P}_{\mathcal{M}_{\otimes}}$.** A region of the quantum state space $\mathcal{D}(\mathcal{H})$ is shown, containing the sequence of states $\rho^{(n)}$ from the example (black) and the corresponding closest points in $\Sigma = \Sigma^{\text{rand}}$ (blue). Panel (a) uses the trace distance δ , for which the distance to Σ stays constant. Panel (b) uses the metric $d_{\mathcal{M}_{\otimes}}$ induced by the product-measurement representation $\mathbf{P}_{\mathcal{M}_{\otimes}}$, for which the distance to $\mathbf{P}_{\mathcal{M}_{\otimes}}(\Sigma)$ shrinks with increasing n .

From this, one finds that $\frac{1}{2}\|P_{M \otimes M}(\rho_{RE}^{(n)}) - P^{(n)} \times P^{(n)}\|_1 \leq 2^{-n}$, where $P^{(n)}$ is the uniform distribution on an alphabet of size 2^n . Consequently, at the level of such probability representations, $\rho_{RE}^{(n)}$ is approximately indistinguishable from Σ^{rand} ; see also Fig. 1.

The result of the example means that, with respect to the metric defined by

$$d_{\mathcal{M}}(\rho, \sigma) := \frac{1}{2} \sup_{M \in \mathcal{M}} \|P_M(\rho) - P_M(\sigma)\|_1, \quad (1.6)$$

when we choose $\mathcal{M} = \mathcal{M}_{\otimes}$ to be the set of local measurements, the sequence $(\rho_{RE}^{(n)})_{n \in \mathbb{N}}$ converges to Σ^{rand} . Yet the same is not true for the metric δ . This motivates the following definition. (Throughout, we assume that \mathcal{M} is a tomographically complete measurement set, i.e., the map $\mathbf{P}_{\mathcal{M}}$ from the space of density matrices $\mathcal{D}(\mathcal{H})$ to the representation space is injective.)

Definition 1. We say that $\mathbf{P}_{\mathcal{M}}$ is topologically robust (or simply robust) if for all subsets Σ and sequences $(\rho^{(n)})_{n \in \mathbb{N}}$ of states

$$\lim_{n \rightarrow \infty} d_{\mathcal{M}}(\rho^{(n)}, \Sigma) = 0 \implies \lim_{n \rightarrow \infty} \delta(\rho^{(n)}, \Sigma) = 0. \quad (1.7)$$

Because the opposite implication always holds, robustness implies that it does not matter which metric one uses. However, the example showed that robustness does not always hold. This raises the question: which of the two metrics is more operationally relevant? To decide this, we use the *principle of composability* [24]. The principle demands that the underlying distance measure is stable under the addition of auxiliary systems in any state Ψ , i.e.,

$$\delta(\rho_{RE}, \Sigma_{RE}) = \delta(\rho_{RE} \otimes \Psi_{R'E'}, \Sigma_{RE} \otimes \Psi_{R'E'}). \quad (1.8)$$

To see the significance of this principle, consider an agent, Alice, with access to the randomness R , and another agent, Eve, with access to side information E . If R is approximately random in the sense of (1.2), then criterion (1.8) ensures that this property is preserved when Alice and Eve have access to additional systems R' and E' , respectively.

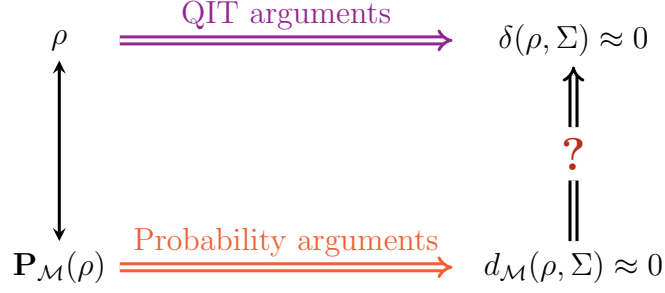


Figure 2: **State-space versus representation-space approximations.** Physical properties are often expressed by the proximity of a state ρ to a set Σ . The diagram illustrates the requirement that approximate statements established at the level of a probability representation remain valid when pulled back to the level of density operators. According to Definition 1, this is the case whenever the representation is topologically robust.

While the trace distance δ satisfies the composability principle (1.8), the metric $d_{\mathcal{M}_{\otimes}}$ does not. The former is a consequence of the monotonicity of the trace distance under data-processing [21, Theorem 9.2]. For the latter, note that our example implies $d_{\mathcal{M}_{\otimes}}(\rho, \Sigma) \ll \delta(\rho \otimes \Psi, \Sigma \otimes \Psi)$; yet, as shown in [25], $d_{\mathcal{M}_{\otimes}}(\rho \otimes \Psi, \Sigma \otimes \Psi) \approx \delta(\rho \otimes \Psi, \Sigma \otimes \Psi)$ when Ψ contains sufficient entanglement. Therefore, the composability principle forbids the use of $d_{\mathcal{M}_{\otimes}}$ as the operationally relevant distance to quantify approximations.

We have thus answered the question posed at the outset: injectivity alone does not suffice to ensure that a representation $\mathbf{P}_{\mathcal{M}}$ is faithful; robustness in the sense of Definition 1 is also required. Without this property, approximate statements established at the level of probability representations cannot, in general, be “pulled back” to the level of density operators. This is illustrated by the commuting diagram in Fig. 2.²

2 A topological characterization of robustness

Definition 1 concerns the convergence of sequences and therefore has a topological character. One might expect that a failure of robustness thus means that the topologies induced by the metrics $d_{\mathcal{M}}$ and δ are inequivalent. As we show next, this intuition is correct, but only if one extends the analysis beyond the space of density operators $\mathcal{D}(\mathcal{H})$.

We begin with a proposition showing why we need to go beyond $\mathcal{D}(\mathcal{H})$. It applies to any measurement set \mathcal{M} satisfying a stability condition, which fails only in pathological cases. Product measurements, in particular, are stable.³

Proposition 2. *The topologies induced by $d_{\mathcal{M}}$ and δ are identical on the space of density matrices $\mathcal{D}(\mathcal{H})$, except when \mathcal{M} is not stable.*

While this proposition tells us that the topologies on $\mathcal{D}(\mathcal{H})$ are not an indicator of robustness, we now show that a topological characterization is possible on the larger space

²This problem does not affect exact statements. These can be proved at the level of the probability representation and then directly pulled back to density operators. A beautiful example is the proof of the quantum de Finetti theorem for infinitely exchangeable states proposed in [26].

³See Definition A.1 and Remark A.2. Moreover, all technical proofs are deferred to the appendix.

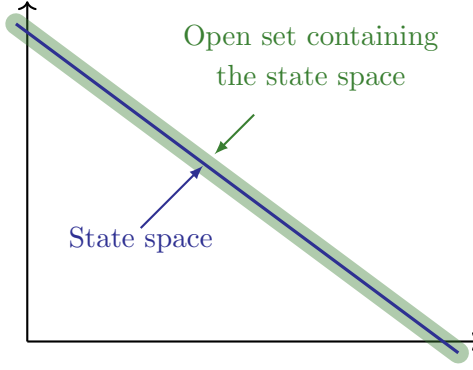


Figure 3: **Sketch of the topological problem.** The state space $\mathcal{D}(\mathcal{H})$ (in blue) is embedded into $\text{span}(\mathcal{D}(\mathcal{H}))$. While for stable \mathcal{M} the topologies induced by $\|\cdot\|_{\mathcal{M}}$ and $\|\cdot\|_1$ agree on $\mathcal{D}(\mathcal{H})$, they generally disagree on an open region (in green) around it.

$\text{span}(\mathcal{D}(\mathcal{H}))$, on which we define the norm $\|\cdot\|_{\mathcal{M}} := \sup_{M \in \mathcal{M}} \|P_M(\cdot)\|_1$; see also Fig. 3.

Proposition 3. *The following statements are equivalent:*

- (1) *The representation $\mathbf{P}_{\mathcal{M}}$ is robust.*
- (2) *The topologies induced by $\|\cdot\|_{\mathcal{M}}$ and $\|\cdot\|_1$ are identical on $\text{span}(\mathcal{D}(\mathcal{H}))$.⁴*
- (3) *$\text{span}(\mathcal{D}(\mathcal{H}))$ is complete with respect to $\|\cdot\|_{\mathcal{M}}$.*

Hence, whether a representation is robust is indeed a purely topological question.

3 Structure is incompatible with robustness

The example discussed above implies that representations based on the set of local measurements \mathcal{M}_{\otimes} are not robust. This raises the question of whether the issue can be avoided by relaxing the locality condition. As we show below, the answer is negative: non-robustness is in fact a generic feature of any representation that preserves structure.

To make this precise, we quantify the “structure” of a given measurement set \mathcal{M} using tools from information theory, in particular an appropriate notion of entropy. Entropy characterizes the minimum size to which data can be compressed such that it remains recoverable via a decoding operation. This decoder must be selected from a set of “physically allowed” operations. For instance, it must be completely positive for decoding quantum information. The analogue at the level of probabilities are convex maps of the form

$$\mathcal{D}_M : (P_E)_{E \in \mathcal{E}} \mapsto \left(\sum_E p_E^{(M_i)} P_E \right)_{M_i \in M}, \quad (3.1)$$

where the sum runs over finitely many elements of \mathcal{E} , and $p_E^{(M_i)} \geq 0$. The input to the decoder \mathcal{D}_M is compressed data in the form of a list of probabilities $P_E = \text{tr}(E\rho)$ stemming from a quantum state ρ . For a given measurement M , one wants the output of \mathcal{D}_M to

⁴This is equivalent to requiring that the inverse of the linear extension of the map $\mathbf{P}_{\mathcal{M}}$ (corresponding to the arrow labelled with “?” in Fig. 2) is continuous with respect to the norm on the probability representation induced by $\|\cdot\|_{\mathcal{M}}$ and the trace norm $\|\cdot\|_1$ on $\text{span}(\mathcal{D}(\mathcal{H}))$.

reproduce (up to a small error ε) the probability distribution $P_M(\rho)$ of the outcomes when measuring ρ . This leads to the following definition.

Definition 4 (Informal⁵). *Let M be a measurement and \mathcal{E} a set of POVM elements. We say that M can be ε -decoded from \mathcal{E} if there exist a decoding operation \mathcal{D}_M such that*

$$\forall \rho \in \mathcal{D}(\mathcal{H}) : \left\| \mathcal{D}_M\left(\left(\text{tr}(E\rho)\right)_{E \in \mathcal{E}}\right) - P_M(\rho) \right\|_1 < \varepsilon. \quad (3.2)$$

We now define the *entropy of a representation* $\mathbf{P}_{\mathcal{M}}$ by $H^\varepsilon := \log(|\mathcal{E}|)$, where $|\mathcal{E}|$ is the minimum input size required for \mathcal{D}_M to ε -decode for all $M \in \mathcal{M}$. For infinite-dimensional Hilbert spaces this quantity is infinite. In this case, we consider its scaling for restricted measurement sets $\mathcal{M}|_\Pi$, obtained by preceding each measurement in \mathcal{M} by an orthogonal finite-rank projector Π .

Definition 5. *Let $(\mathcal{E}_n)_{n \in \mathbb{N}}$ be a sequence of sets of POVM elements, $\{\Pi_{2^n}\}_{n \in \mathbb{N}}$ a nested family of projectors with $\text{rank}(\Pi_{2^n}) \geq 2^n$, and $(\varepsilon_n)_{n \in \mathbb{N}}$ a zero-sequence. We say the asymptotic entropy of \mathcal{M} is at most $(\log(|\mathcal{E}_n|))_{n \in \mathbb{N}}$ if all $M \in \mathcal{M}|_{\Pi_{2^n}}$ are ε_n -decodable from \mathcal{E}_n .*

Remark 6. *The asymptotic entropy of any \mathcal{M} is at most $(2^{n+\log(n)+3})_{n \in \mathbb{N}}$.*

Structure in the measurement set \mathcal{M} manifests itself in an entropy below the upper bound. Theorem 7, our main technical result, therefore shows that the probability representation $\mathbf{P}_{\mathcal{M}}$ cannot be robust when \mathcal{M} has non-negligible structure.

Theorem 7. *If \mathcal{M} has asymptotic entropy at most $(\varepsilon_n 2^n)_{n \in \mathbb{N}}$ for a zero-sequence $(\varepsilon_n)_{n \in \mathbb{N}}$, then the representation $\mathbf{P}_{\mathcal{M}}$ is not robust.*

Product measurements provide a canonical example of a measurement set with significant structure. A straightforward calculation shows that the asymptotic entropy of \mathcal{M}_\otimes scales as $(2^{n/2})_{n \in \mathbb{N}}$. The conclusion of our introductory example then follows as a corollary.⁶

Corollary 8. *The representation $\mathbf{P}_{\mathcal{M}_\otimes}$ is not robust.*

In the study of d -dimensional systems, one is often interested in fiducial representations $\mathbf{P}_{\mathcal{M}_d}$ that use a minimal measurement set \mathcal{M}_d [2, 3, 6, 10–14, 41]. SIC-POVMs are a prominent example [42]. Additionally, d is chosen to be the smallest Hilbert space dimension with which the system can be described. For example, if one uses an atom as qubit in a quantum computer, then one works with the corresponding 2-dimensional subspace rather than the high-dimensional Hilbert space of the atom.

While this minimization of the dimension is often implicit, it involves a non-trivial consistency assumption, which we adopt in the following: a dimensional restriction from a D -dimensional to a d -dimensional Hilbert space should not weaken the representation. Formally, using Definition 4 with $\varepsilon = 0$, we require that $\mathcal{M}_D|_{\Pi_d}$ is decodable from the POVM elements of \mathcal{M}_d , where Π_d is the projector onto the d -dimensional subspace.

To make an asymptotic statement, we consider the union $\mathcal{M} = \bigcup_d \mathcal{M}_d$ of the minimal measurement sets \mathcal{M}_d for all d . Because the state space for each d is $(d^2 - 1)$ -dimensional, and therefore polynomial in d , such measurement sets satisfy the following definition.

⁵See Definition B.2 for the formal definition, which also applies to continuous measurements.

⁶Alternatively, the statement can also be derived from well-known data hiding results [27–40].

	Structure preservation		
	Robust	Subsystems	Efficient
Density operator $\mathcal{D}(\mathcal{H})$	✓	✓	✓
Probability representations			
$\mathcal{P}_{\mathcal{M}_{\text{all}}}$	✓	✗	✗
$\mathcal{P}_{\mathcal{M}_{\otimes}}$	✗	✓	✗
$\mathcal{M}_{\text{efficient}}$	✗	depends on $\mathcal{M}_{\text{efficient}}$	✓

Table 1: **Density operator vs. probability representations.** The density operator representation of a quantum state is robust, in the sense that small deviations in the representation are physically insignificant. Furthermore, it respects the subsystem structure, and it is efficient, requiring only few real numbers. In contrast, probability representations that are robust cannot have any such structural properties.

Definition 9. We say that \mathcal{M} is efficient if there exists a nested family of rank- d projectors $\{\Pi_d\}_{d \in \mathbb{N}}$ and a sequence $(\mathcal{M}_d)_{d \in \mathbb{N}}$ of measurement sets such that $|\bigcup_{N \in \mathcal{M}_D} N| \leq \text{poly}(D)$ and, for all D , $\mathcal{M}|_{\Pi_D}$ can be decoded from the POVM elements of $\bigcup_{d=1}^D \mathcal{M}_d$.

This definition directly implies that the entropy of any efficient measurement set \mathcal{M} is at most $(\text{const } n)_{n \in \mathbb{N}}$, which yields another corollary to Theorem 7.

Corollary 10. If \mathcal{M} is efficient, the representation $\mathbf{P}_{\mathcal{M}}$ is not robust.

The results of this section show that the use of probability representations leads to a fundamental dilemma, which is summarized in Table 1.

4 Beyond Quantum

In quantum foundations, one often studies generalizations of quantum theory where states need not be representable by density operators. Probability representations are well suited for this task, as they allow one to directly modify the constraints that quantum theory imposes on the admissible lists of outcome probabilities. A widely used framework based on this idea is that of generalized probabilistic theories (GPTs) [3, 5, 6, 8, 9, 15, 16, 43–46], where each GPT is specified by the set of probability assignments corresponding to its valid states. A brief introduction to the formalism is given in Appendix C.

Since probability representations are fundamental to the GPT framework, the issues summarized in Table 1 also pose a challenge for GPTs. In fact, the situation is even more severe, as Proposition 2 does not generalize to GPTs beyond quantum theory. To state this result, we extend the trace distance to arbitrary GPTs by defining $\delta(\rho, \sigma) := \frac{1}{2} \sup_M \|P_M(\rho) - P_M(\sigma)\|_1$ where the supremum ranges over all measurements M . Note that, as in the quantum case, we allow for state spaces of unbounded dimension.

Theorem 11. There exists a GPT for which the topologies induced by $d_{\mathcal{M}_{\otimes}}$ and δ are different on state space, despite \mathcal{M}_{\otimes} being stable.

5 Conclusion

We conclude with a discussion of the implications of our results for various areas of research that use probability representations, starting with quantum foundations. Reconstruction programmes seek to derive quantum theory from postulates with a clear and direct physical meaning. A common postulate in this context is *local tomography*, which posits that the state of a bipartite system is uniquely determined by the statistics of local measurements, corresponding to a local representation $\mathbf{P}_{\mathcal{M}_{\otimes}}$ [2, 3, 9, 10, 47, 48]. Yet, for this to be physically grounded, $\mathbf{P}_{\mathcal{M}_{\otimes}}$ must be robust: infinitesimal statistical fluctuations must not imply wildly different states. Corollary 8 shows that this requirement fails for quantum systems of unbounded dimension.⁷ Consequently, even for prototypical physical systems—such as those composed of harmonic oscillators or single particles—local tomography is not a viable physical principle. This suggests that extending the current reconstruction programme to such systems is not a mere mathematical formality but a substantial conceptual challenge.⁸

Probability representations also play a central role in quantum interpretations. A prominent example is QBism, which regards a quantum state as a catalogue of an agent’s personal degrees of belief, corresponding to a probability representation $\mathbf{P}_{\mathcal{M}}$ [11, 17]. To formulate quantum theory—and specifically the state-update rule—entirely in probabilistic terms, QBism requires a representation that is not overcomplete, implemented, for instance, by SIC-POVMs [41]. However, Corollary 10 implies that, for systems of unbounded dimension, such probability representations fail to be robust. Our results thus point to a fundamental obstruction to extending the QBist programme beyond finite-dimensional systems.

In quantum information theory, probability representations are routinely employed to enable the application of classical information-theoretic tools to quantum systems. An operationally motivated approach to obtaining such a representation is to model the interaction between agents and the experimental setup as an abstract box. For example, to analyse bipartite entanglement, one may imagine two agents, Alice and Bob, who choose measurements α and β , and observe the respective results, X and Y .



The behaviour of this box is fully characterized by the conditional probability distribution $P_{XY|\alpha\beta}$, which is required to be non-signalling.⁹ This corresponds precisely to the probability representation $\mathbf{P}_{\mathcal{M}_{\otimes}}(\rho_{AB})$ of the state ρ_{AB} shared by Alice and Bob.

⁷Given that local tomography fails to be robust, one may wonder how the state of a composite quantum system can be determined in practice. This is achieved by imposing simplifying assumptions. For example, in quantum optics one often restricts attention to Gaussian states or to states with a bounded photon number.

⁸This contrasts with the expectation [10, 14] that generalizing such reconstructions to infinite dimensions may be “only a small conceptual (though possibly mathematically challenging) step.”

⁹The non-signalling property ensures that neither party can communicate through their choice of measurement. Technically, Alice’s marginal distribution $P_{X|\alpha\beta}$ is independent of β , and analogously for Bob’s.

Our results, notably Corollary 8, thus apply directly to this setting, implying that the box-based representation is not robust for systems of unbounded dimension. This failure is critical in device-independent quantum cryptography, for instance. There, devices are treated as adversarial, so that no bounds on their dimension can be assumed, yet robustness is essential (cf. the randomness-generation example in the introduction). While it has been proposed to establish cryptographic security directly at the level of boxes [43, 49], the non-robustness of $\mathbf{P}_{\mathcal{M}_{\otimes}}$ shows that this approach is not viable.

Quantum field theory (QFT) is another prominent domain in which probability representations are employed. Instead of wave functions, states are typically characterized by their n -point correlation functions.¹⁰ The injectivity of this representation follows from the Wightman reconstruction theorem [51]. Our results, however, suggest that such representations are not robust.

While our treatment assumes that states can be represented as density operators and thus is not directly applicable to general QFTs, theories satisfying the split property can be well approximated by discretized models in which degrees of freedom are localized on a lattice and the state space factorizes accordingly. In this regime, Corollary 8 shows that correlation functions fail to provide a robust state representation. This becomes particularly problematic when considering genuinely non-local observables. A notable example are the observables necessary to test for the athermality of Hawking radiation, which would manifest itself in complex non-local correlations.

One might assume that non-robustness occurs only in infinite-dimensional systems. In finite dimensions, all norms—and hence their induced topologies—are equivalent. However, non-robustness still appears through a dimension-dependent scaling factor between the distances $d_{\mathcal{M}}$ and δ . Our results can therefore be understood as the infinite-dimensional culmination of a scaling problem that is already present in finite dimensions [27–40].

In summary, we have argued against probability-based representations: although ubiquitous in physics, they face fundamental limitations, summarized by Table 1. This motivates the search for an alternative framework for representing states that (i) is topologically robust; (ii) preserves physically meaningful structure, such as the subsystem structure; and (iii) allows generalizations beyond quantum theory, in the spirit of GPTs. Developing such a framework is left for future work.

Acknowledgments

We thank Giulio Chiribella, Lucien Hardy, Lluís Masanes, Markus Müller, and Robert Spekkens for discussions. We acknowledge funding from the Swiss National Science Foundation via project No. 20QU-1.225171. We are also grateful for the support from the NCCR SwissMAP, the ETH Zurich Quantum Center, and the Simons Center for Geometry and Physics, where part of this work was carried out.

¹⁰See also [50] for another discussion of the differences between quantum states and correlation functions.

References

- [1] Michael E. Peskin. *An Introduction To Quantum Field Theory*. Andover, England, UK: Taylor & Francis, 1995. ISBN: 978-0-42950355-9. DOI: [10.1201/9780429503559](https://doi.org/10.1201/9780429503559).
- [2] William K. Wootters. “Quantum mechanics without probability amplitudes”. In: *Found. Phys.* 16.4 (1986), pp. 391–405. ISSN: 1572-9516. DOI: [10.1007/BF01882696](https://doi.org/10.1007/BF01882696).
- [3] Lucien Hardy. *Quantum theory from five reasonable axioms*. 2001. arXiv: [quant-ph/0101012](https://arxiv.org/abs/quant-ph/0101012) [quant-ph].
- [4] Piero G. L. Mana. *Why can states and measurement outcomes be represented as vectors?* 2004. arXiv: [quant-ph/0305117](https://arxiv.org/abs/quant-ph/0305117) [quant-ph].
- [5] Jonathan Barrett et al. “Nonlocal correlations as an information-theoretic resource”. In: *Phys. Rev. A* 71 (2 2005), p. 022101. DOI: [10.1103/PhysRevA.71.022101](https://doi.org/10.1103/PhysRevA.71.022101).
- [6] Jonathan Barrett. “Information processing in generalized probabilistic theories”. In: *Phys. Rev. A* 75 (3 2007), p. 032304. DOI: [10.1103/PhysRevA.75.032304](https://doi.org/10.1103/PhysRevA.75.032304).
- [7] Alexander Wilce. *Four and a half axioms for finite dimensional quantum mechanics*. 2009. arXiv: [0912.5530](https://arxiv.org/abs/0912.5530) [quant-ph].
- [8] Giulio Chiribella, Giacomo Mauro D’Ariano, and Paolo Perinotti. “Probabilistic theories with purification”. In: *Phys. Rev. A* 81.6 (2010), p. 062348. DOI: [10.1103/PhysRevA.81.062348](https://doi.org/10.1103/PhysRevA.81.062348).
- [9] Giulio Chiribella, Giacomo Mauro D’Ariano, and Paolo Perinotti. “Informational derivation of quantum theory”. In: *Phys. Rev. A* 84.1 (2011), p. 012311. DOI: [10.1103/PhysRevA.84.012311](https://doi.org/10.1103/PhysRevA.84.012311).
- [10] Lluís Masanes and Markus P Müller. “A derivation of quantum theory from physical requirements”. In: *New Journal of Physics* 13.6 (2011), p. 063001. DOI: [10.1088/1367-2630/13/6/063001](https://doi.org/10.1088/1367-2630/13/6/063001).
- [11] D. M. Appleby, Asa Ericsson, and Christopher A. Fuchs. *Properties of qbit state spaces*. 2011. arXiv: [0910.2750](https://arxiv.org/abs/0910.2750) [quant-ph].
- [12] Peter Janotta and Raymond Lal. “Generalized probabilistic theories without the no-restriction hypothesis”. In: *Phys. Rev. A* 87.5 (2013), p. 052131. DOI: [10.1103/PhysRevA.87.052131](https://doi.org/10.1103/PhysRevA.87.052131).
- [13] Lucien Hardy. “Reconstructing quantum theory”. In: *Quantum Theory: Informational Foundations and Foils*. Dordrecht, The Netherlands: Springer, 2015, pp. 223–248. ISBN: 978-94-017-7303-4. DOI: [10.1007/978-94-017-7303-4_7](https://doi.org/10.1007/978-94-017-7303-4_7).
- [14] Markus P. Müller and Lluís Masanes. “Information-theoretic postulates for quantum theory”. In: *Quantum Theory: Informational Foundations and Foils*. Ed. by Giulio Chiribella and Robert W. Spekkens. Dordrecht: Springer Netherlands, 2016, pp. 139–170. DOI: [10.1007/978-94-017-7303-4_5](https://doi.org/10.1007/978-94-017-7303-4_5).
- [15] Giacomo Mauro D’Ariano, Giulio Chiribella, and Paolo Perinotti. *Quantum Theory from First Principles: An Informational Approach*. Cambridge, England, UK: Cambridge University Press, 2017. ISBN: 978-1-10704342-8. DOI: [10.1017/9781107338340](https://doi.org/10.1017/9781107338340).

- [16] Martin Plávala. “General probabilistic theories: an introduction”. In: *Physics Reports* 1033 (2023), pp. 1–64. ISSN: 0370-1573. DOI: [10.1016/j.physrep.2023.09.001](https://doi.org/10.1016/j.physrep.2023.09.001).
- [17] Christopher A. Fuchs and Rüdiger Schack. “Quantum-bayesian coherence”. In: *Reviews of Modern Physics* 85.4 (2013), pp. 1693–1715. ISSN: 1539-0756. DOI: [10.1103/revmodphys.85.1693](https://doi.org/10.1103/revmodphys.85.1693).
- [18] Umesh Vazirani and Thomas Vidick. “Certifiable quantum dice: or, true random number generation secure against quantum adversaries”. In: *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*. STOC ’12. New York, New York, USA: Association for Computing Machinery, 2012, pp. 61–76. DOI: [10.1145/2213977.2213984](https://doi.org/10.1145/2213977.2213984).
- [19] Stefano Pironio and Serge Massar. “Security of practical private randomness generation”. In: *Phys. Rev. A* 87 (1 2013), p. 012336. DOI: [10.1103/PhysRevA.87.012336](https://doi.org/10.1103/PhysRevA.87.012336).
- [20] Daniela Frauchiger, Renato Renner, and Matthias Troyer. *True randomness from realistic quantum devices*. 2013. arXiv: [1311.4547](https://arxiv.org/abs/1311.4547) [quant-ph].
- [21] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge, England, UK: Cambridge University Press, 2010. ISBN: 978-0-51197666-7. DOI: [10.1017/CB09780511976667](https://doi.org/10.1017/CB09780511976667).
- [22] Carla Ferradini et al. *Defining security in quantum key distribution*. 2025. arXiv: [2509.13405](https://arxiv.org/abs/2509.13405) [quant-ph].
- [23] Matthias Christandl et al. “One-and-a-half quantum de Finetti theorems”. In: *Communications in Mathematical Physics* 273.2 (2007), pp. 473–498. ISSN: 1432-0916. DOI: [10.1007/s00220-007-0189-3](https://doi.org/10.1007/s00220-007-0189-3).
- [24] Ueli Maurer and Renato Renner. “Abstract cryptography”. In: *Innovations in Computer Science — Proceedings of the ICS 2011*. Beijing, China: Tsinghua University Press, 2011, pp. 1–21. URL: <https://conference.iis.tsinghua.edu.cn/ICS2011/content/papers/14.html>.
- [25] Lev Vaidman. “Instantaneous measurement of nonlocal variables”. In: *Phys. Rev. Lett.* 90.1 (2003), p. 010402. DOI: [10.1103/PhysRevLett.90.010402](https://doi.org/10.1103/PhysRevLett.90.010402).
- [26] Carlton M. Caves, Christopher A. Fuchs, and Rüdiger Schack. “Unknown quantum states: the quantum de Finetti representation”. In: *Journal of Mathematical Physics* 43.9 (2002), pp. 4537–4559. ISSN: 1089-7658. DOI: [10.1063/1.1494475](https://doi.org/10.1063/1.1494475).
- [27] Barbara M. Terhal, David P. DiVincenzo, and Debbie W. Leung. “Hiding bits in Bell states”. In: *Phys. Rev. Lett.* 86 (25 2001), pp. 5807–5810. DOI: [10.1103/PhysRevLett.86.5807](https://doi.org/10.1103/PhysRevLett.86.5807).
- [28] David P. DiVincenzo et al. “Locking classical correlations in quantum states”. In: *Phys. Rev. Lett.* 92.6 (2004), p. 067902. DOI: [10.1103/PhysRevLett.92.067902](https://doi.org/10.1103/PhysRevLett.92.067902).
- [29] T. Eggeling and R. F. Werner. “Hiding classical data in multipartite quantum states”. In: *Phys. Rev. Lett.* 89 (9 2002), p. 097905. DOI: [10.1103/PhysRevLett.89.097905](https://doi.org/10.1103/PhysRevLett.89.097905).
- [30] Patrick Hayden et al. “Randomizing quantum states: constructions and applications”. In: *Communications in Mathematical Physics* 250.2 (2004), pp. 371–391. ISSN: 1432-0916. DOI: [10.1007/s00220-004-1087-6](https://doi.org/10.1007/s00220-004-1087-6).

- [31] Robert König et al. “Small accessible quantum information does not imply security”. In: *Phys. Rev. Lett.* 98.14 (2007), p. 140502. DOI: [10.1103/PhysRevLett.98.140502](https://doi.org/10.1103/PhysRevLett.98.140502).
- [32] William Matthews and Andreas Winter. “On the chernoff distance for asymptotic locc discrimination of bipartite quantum states”. In: *Commun. Math. Phys.* 285.1 (2009), pp. 161–174. ISSN: 1432-0916. DOI: [10.1007/s00220-008-0582-6](https://doi.org/10.1007/s00220-008-0582-6).
- [33] Cécilia Lancien and Andreas Winter. “Distinguishing multi-partite states by local measurements”. In: *Communications in Mathematical Physics* 323.2 (2013), pp. 555–573. ISSN: 1432-0916. DOI: [10.1007/s00220-013-1779-x](https://doi.org/10.1007/s00220-013-1779-x).
- [34] Eric Chitambar and Min-Hsiu Hsieh. “Asymptotic state discrimination and a strict hierarchy in distinguishability norms”. In: *J. Math. Phys.* 55.11 (2014), p. 112204. ISSN: 0022-2488. DOI: [10.1063/1.4902027](https://doi.org/10.1063/1.4902027).
- [35] Guillaume Aubrun and Cecilia Lancien. “Locally restricted measurements on a multipartite quantum system: data hiding is generic”. In: *Quantum Inf. Comput.* (2015), pp. 513–540. DOI: [10.26421/QIC15.5-6](https://doi.org/10.26421/QIC15.5-6).
- [36] Ludovico Lami. “Quantum data hiding with continuous-variable systems”. In: *Phys. Rev. A* 104.5 (2021), p. 052428. DOI: [10.1103/PhysRevA.104.052428](https://doi.org/10.1103/PhysRevA.104.052428).
- [37] Willian H. G. Corrêa, Ludovico Lami, and Carlos Palazuelos. “Maximal gap between local and global distinguishability of bipartite quantum states”. In: *IEEE Trans. Inf. Theory* 68.11 (2022), pp. 7306–7314. DOI: [10.1109/TIT.2022.3186428](https://doi.org/10.1109/TIT.2022.3186428).
- [38] Hao-Chung Cheng, Andreas Winter, and Nengkun Yu. “Discrimination of quantum states under locality constraints in the many-copy setting”. In: *Communications in Mathematical Physics* 404.1 (2023), pp. 151–183. ISSN: 1432-0916. DOI: [10.1007/s00220-023-04836-0](https://doi.org/10.1007/s00220-023-04836-0).
- [39] Francesco Anna Mele and Ludovico Lami. *Optimising quantum data hiding*. 2025. arXiv: [2510.03538](https://arxiv.org/abs/2510.03538) [quant-ph].
- [40] Donghoon Ha and Jeong San Kim. “Quantum data-hiding scheme using orthogonal separable states”. In: *Phys. Rev. A* 111 (5 2025), p. 052405. DOI: [10.1103/PhysRevA.111.052405](https://doi.org/10.1103/PhysRevA.111.052405).
- [41] Christopher A. Fuchs and Rüdiger Schack. “A quantum-bayesian route to quantum-state space”. In: *Foundations of Physics* 41.3 (2010), pp. 345–356. ISSN: 1572-9516. DOI: [10.1007/s10701-009-9404-8](https://doi.org/10.1007/s10701-009-9404-8).
- [42] Joseph M. Renes et al. “Symmetric informationally complete quantum measurements”. In: *Journal of Mathematical Physics* 45.6 (June 2004), pp. 2171–2180. ISSN: 1089-7658. DOI: [10.1063/1.1737053](https://doi.org/10.1063/1.1737053).
- [43] Jonathan Barrett, Lucien Hardy, and Adrian Kent. “No signaling and quantum key distribution”. In: *Physical Review Letters* 95.1 (2005). ISSN: 1079-7114. DOI: [10.1103/physrevlett.95.010503](https://doi.org/10.1103/physrevlett.95.010503).
- [44] R. W. Spekkens. “Contextuality for preparations, transformations, and unsharp measurements”. In: *Phys. Rev. A* 71 (5 2005), p. 052108. DOI: [10.1103/PhysRevA.71.052108](https://doi.org/10.1103/PhysRevA.71.052108).

- [45] Lucien Hardy. *Reformulating and reconstructing quantum theory*. 2011. arXiv: [1104.2066 \[quant-ph\]](#).
- [46] Peter Janotta and Haye Hinrichsen. “Generalized probability theories: what determines the structure of quantum theory?” In: *Journal of Physics A: Mathematical and Theoretical* 47.32 (2014), p. 323001. ISSN: 1751-8121. DOI: [10.1088/1751-8113/47/32/323001](#).
- [47] William K Wootters. “Local accessibility of quantum states”. In: *Complexity, entropy and the physics of information* 8 (1990), pp. 39–46.
- [48] Howard Barnum and Alexander Wilce. “Local tomography and the jordan structure of quantum theory”. In: *Foundations of Physics* 44.2 (2014), pp. 192–212. DOI: [10.1007/s10701-014-9777-1](#).
- [49] Lluís Masanes et al. “Full security of quantum key distribution from no-signaling constraints”. In: *IEEE Transactions on Information Theory* 60.8 (2014), pp. 4973–4986. ISSN: 1557-9654. DOI: [10.1109/tit.2014.2329417](#).
- [50] Nima Arkani-Hamed, Ross Glew, and Francisco Vazão. *Correlators are simpler than wavefunctions*. 2025. arXiv: [2512.23795 \[hep-th\]](#).
- [51] A. S. Wightman. “Quantum field theory in terms of vacuum expectation values”. In: *Phys. Rev.* 101 (2 1956), pp. 860–866. DOI: [10.1103/PhysRev.101.860](#).
- [52] Mark M. Wilde. “Tools of quantum Shannon theory”. In: *Quantum Information Theory*. Cambridge University Press, 2017, pp. 227–228. DOI: [10.1017/9781316809976](#).
- [53] Gerard J. Murphy. “Chapter 4 - von Neumann algebras”. In: *Algebras and Operator Theory*. San Diego: Academic Press, 1990, pp. 112–139. ISBN: 978-0-08-092496-0. DOI: [10.1016/B978-0-08-092496-0.50008-9](#).
- [54] Michael Reed and Barry Simon. “III - Banach spaces”. In: *Methods of Modern Mathematical Physics*. Academic Press, 1972, pp. 67–89. ISBN: 978-0-12-585001-8. DOI: [10.1016/B978-0-12-585001-8.50009-X](#).
- [55] Walter Rudin. *Functional Analysis*. Maidenhead, England, UK: McGraw-Hill, 1991. ISBN: 978-0-07054236-5.
- [56] Frédéric Dupuis et al. “One-shot decoupling”. In: *Communications in Mathematical Physics* 328.1 (2014), pp. 251–284. ISSN: 1432-0916. DOI: [10.1007/s00220-014-1990-4](#).
- [57] Rajendra Bhatia. *Matrix Analysis*. New York, NY, USA: Springer, 1997. ISBN: 978-1-4612-0653-8. DOI: [10.1007/978-1-4612-0653-8](#).
- [58] Elizabeth S. Meckes. *The Random Matrix Theory of the Classical Compact Groups*. Cambridge, England, UK: Cambridge University Press, 2019. ISBN: 978-1-10830345-3. DOI: [10.1017/9781108303453](#).
- [59] John Watrous. *The Theory of Quantum Information*. Cambridge, England, UK: Cambridge University Press, 2018. ISBN: 978-1-31684814-2. DOI: [10.1017/9781316848142](#).

A Topological properties

Definition A.1. A set \mathcal{M} of measurements is *stable* if for every POVM element E with finite-dimensional support the topologies induced by $d_{\mathcal{M}}$ and $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$ are identical.

Remark A.2. Let \mathcal{N} be the set of POVM elements that appear in a measurement set \mathcal{M} . Then \mathcal{M} is stable if any possible POVM element with finite support is in the closure of $\text{span}(\mathcal{N})$ with respect to $\|\cdot\|_{\infty}$. This is, in particular, the case for \mathcal{M}_{\otimes} .

Proof. Let E be a POVM element with finite support and $(\rho_n)_{n \in \mathbb{N}}$ a sequence converging to ρ with respect to $d_{\mathcal{M}}$. We first show that, under the assumption made in the remark, the sequence also converges with respect to $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$.

To see this, take a sequence of POVM elements $(E_n)_{n \in \mathbb{N}}$ in the span of the POVM element of \mathcal{M} that converges to E with respect to $\|\cdot\|_{\infty}$. For every $\varepsilon > 0$ there exists an $E_m = \sum_i a_i^m N_i^m$ with $N_i^m \in \mathcal{N}$ such that $\|E_m - E\|_{\infty} \leq \varepsilon$. So we find

$$\begin{aligned} \lim_{n \rightarrow \infty} |\text{tr}(E(\rho_n - \rho))| &\leq \lim_{n \rightarrow \infty} \sum_i |a_i^m| \cdot |\text{tr}(N_i(\rho_n - \rho))| + |\text{tr}((E_m - E)(\rho_n - \rho))| \\ &\leq \lim_{n \rightarrow \infty} \sum_i |a_i^k| \cdot \|\rho_n - \rho\|_{\mathcal{M}} + 2\varepsilon \\ &= 2\varepsilon. \end{aligned} \tag{A.1}$$

As this holds for every $\varepsilon > 0$, we have $\lim_{n \rightarrow \infty} |\text{tr}(E(\rho_n - \rho))| = 0$. This implies that the sequence $(\rho_n)_{n \in \mathbb{N}}$ converges to ρ also with respect to $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$.

We have thus established that every sequence $(\rho_n)_{n \in \mathbb{N}}$ that converges with respect to $d_{\mathcal{M}}$ also converges with respect to $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$. Because, conversely, $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$ dominates $d_{\mathcal{M}}$, the topology induced by $d_{\mathcal{M}}$ is equal to the topology induced by $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$. The stability condition thus holds.

Because product POVM elements with finite support linearly span POVM elements with finite support, the condition is met for \mathcal{M}_{\otimes} . \square

Proposition 2. The topologies induced by $d_{\mathcal{M}}$ and δ are identical on the space of density matrices $\mathcal{D}(\mathcal{H})$, except when \mathcal{M} is not stable.

Proof. We first show that, if the topologies induced by $d_{\mathcal{M}}$ and δ are identical, then \mathcal{M} is stable. If these two topologies are identical, then the topology of $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$ is finer than the topology of δ . Furthermore, because $d_{\mathcal{N}} \leq \delta$ holds for arbitrary measurement sets \mathcal{N} , the topology induced by $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$ is coarser than that of δ . Consequently, the topologies induced by $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$ and δ are identical.

We now show that the stability of \mathcal{M} implies that the topologies induced by $d_{\mathcal{M}}$ and δ are identical. Stability means that, for any POVM element E with finite support, the topologies induced by $d_{\mathcal{M} \cup \{E, \mathbb{1}-E\}}$ and $d_{\mathcal{M}}$ are identical. Let $\{|n\rangle\}_{n \in \mathbb{N}}$ be an orthonormal basis of \mathcal{H} and $P_N = \sum_{i=0}^N |i\rangle\langle i|$ projectors. For any measurements set \mathcal{M} satisfying the conditions of the proposition and $N \in \mathbb{N}$, the map $P_N : \rho \mapsto P_N \rho P_N$, where ρ is a state, is continuous with respect to $\|\cdot\|_{\mathcal{M}}$. To see this, let $(\rho_n)_{n \in \mathbb{N}}$ be a sequence that converges to ρ with respect to $\|\cdot\|_{\mathcal{M}}$ and let $\mathcal{E} = \{E_1, \dots, E_{N^2}\}$ be a tomographically complete POVM

on the support of P_N . We define the norm $\|\rho\|_{\mathcal{E}} := \sup_{E \in \mathcal{E}} |\text{tr}(EA)|$ on the image of P_N . Since the topology induced by $d_{\mathcal{M} \cup \{E, \mathbb{1} - E\}}$ is identical to that of $d_{\mathcal{M}}$ it follows that

$$\begin{aligned} \forall E \in \mathcal{E} : \lim_{n \rightarrow \infty} |\text{tr}(EP_N(\rho_n - \rho)P_N)| &= \lim_{n \rightarrow \infty} |\text{tr}(E(\rho_n - \rho))| \\ &\leq \lim_{n \rightarrow \infty} d_{\mathcal{M} \cup \{E, \mathbb{1} - E\}}(\rho_n, \rho) = 0. \end{aligned} \quad (\text{A.2})$$

As $|\mathcal{E}| < \infty$, we find that $P_N(\rho_n)$ converges to $P_N(\rho)$ with respect to $\|\cdot\|_{\mathcal{E}}$, and because the image of P_N is finite-dimensional also with respect to $\|\cdot\|_{\mathcal{M}}$. As this holds for any converging sequence, we have established that the map P_N is continuous with respect to $\|\cdot\|_{\mathcal{M}}$.

Let $(\rho^{(n)})_{n \in \mathbb{N}}$ be a sequence of states such that $\lim_{n \rightarrow \infty} d_{\mathcal{M}}(\rho^{(n)}, \rho) = 0$. Then

$$\begin{aligned} 0 &= \lim_{n \rightarrow \infty} 2d_{\mathcal{M}}(\rho^{(n)}, \rho) \\ &= \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \|\rho^{(n)} - \rho\|_{\mathcal{M}} + \|\rho - P_N \rho P_N\|_{\mathcal{M}} \\ &\geq \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \|\rho^{(n)} - P_N \rho P_N\|_{\mathcal{M}} \\ &= \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \|\rho^{(n)} - P_N \rho P_N\|_{\mathcal{M}} + \|P_N \rho^{(n)} P_N - P_N \rho P_N\|_{\mathcal{M}} \\ &\geq \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \|\rho^{(n)} - P_N \rho^{(n)} P_N\|_{\mathcal{M}} \\ &\geq \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \sum_{E_i \in M} |\text{tr}(E_i(P_N \rho^{(n)} P_N - \rho^{(n)}))| \\ &\geq \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} |1 - \text{tr}(P_N \rho^{(n)} P_N)| \end{aligned} \quad (\text{A.3})$$

where $M \in \mathcal{M}$ is a measurement with POVM elements $\{E_i\}_i$, and we used both the continuity of P_N with respect to $\|\cdot\|_{\mathcal{M}}$ and that $\lim_{N \rightarrow \infty} \delta(P_N \rho P_N, \rho) = 0$. Using this result, we can calculate the limit with respect to $\|\cdot\|_1$,

$$\begin{aligned} \lim_{n \rightarrow \infty} \|\rho^{(n)} - \rho\|_1 &= \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \|\rho^{(n)} - \rho\|_1 - \|P_N \rho P_N - \rho\|_1 \\ &\leq \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \|\rho^{(n)} - P_N \rho P_N\|_1 \\ &= \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \|\rho^{(n)} - P_N \rho P_N\|_1 - \|P_N \rho P_N - P_N \rho^{(n)} P_N\|_1 \\ &\leq \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} \|\rho^{(n)} - P_N \rho^{(n)} P_N\|_1 \\ &\leq \lim_{N \rightarrow \infty} \lim_{n \rightarrow \infty} 2\sqrt{1 - \text{tr}(P_N \rho^{(n)} P_N)} = 0 \end{aligned} \quad (\text{A.4})$$

where in the last inequality we used the gentle measurement lemma [52, Lemma 9.4.2]. We have thus shown that, if a sequence $(\rho_n)_{n \in \mathbb{N}}$ converges with respect to $\|\cdot\|_{\mathcal{M}}$ then it also converges with respect to $\|\cdot\|_1$. This, together with the fact that $\|\cdot\|_1$ dominates $\|\cdot\|_{\mathcal{M}}$, proves that the topologies induced by δ and $d_{\mathcal{M}}$ are equal. \square

Remark A.3. *There exists a tomographically complete measurement set \mathcal{M} such that the topologies induced by $d_{\mathcal{M}}$ and δ are not the same on $\mathcal{D}(\mathcal{H})$.*

Proof. Let $\{|n\rangle\}_{n \in \mathbb{N}}$ be a basis and $P = \sum_n e^{-n} |n\rangle\langle n|$. We define

$$\mathcal{M} = \{\{PEP, \mathbb{1} - PEP\} \mid \langle 0|E|0\rangle = 0, 0 \leq E \leq \mathbb{1}\} \cup \{\{\mathbb{1}\}\}. \quad (\text{A.5})$$

It can be readily verified that \mathcal{M} is tomographically complete. To show that the topology induced by $d_{\mathcal{M}}$ is different from the topology induced by δ , we consider the sequence $(|n\rangle\langle n|)_{n \in \mathbb{N}}$. This sequence obviously does not converge with respect to δ . However, it converges with respect to $d_{\mathcal{M}}$. To see the latter, note first that the POVM element $\mathbb{1}$ cannot be used to distinguish $|0\rangle\langle 0|$ from $|n\rangle\langle n|$. Furthermore, for any POVM element E with $\langle 0|E|0\rangle = 0$, it holds that $\text{tr}(PEP(|n\rangle\langle n| - |0\rangle\langle 0|)) = e^{-2n} \langle n|E|n\rangle \leq e^{-2n}$. \square

Before proceeding with the proof of our next main statements, we need a technical lemma. The lemma refers to norms that are defined on the space $\text{span}(\mathcal{D}(\mathcal{H}))$, which contains all Hermitian trace-class operators on \mathcal{H} . We also remark that any such operator A can be written as a sum of a positive part A_+ and a negative part A_- .

Lemma A.4. *If the norms $\|\cdot\|_1$ and $\|\cdot\|_{\mathcal{M}}$ do not induce the same topology then there exists a sequence $(A^{(n)})_{n \in \mathbb{N}}$ of Hermitian trace-class operators from the set¹¹*

$$\mathcal{O}_{\text{diff}} := \{A : \text{tr}(A) = 0 \wedge \text{tr}(A_+) \leq \frac{1}{11}\}, \quad (\text{A.6})$$

such that

$$\lim_{n \rightarrow \infty} \|A^{(n)}\|_{\mathcal{M}} = 0, \quad (\text{A.7})$$

whereas there exists $\mu > 0$ such that

$$\forall n \in \mathbb{N} : \quad \|A^{(n)}\|_1 \geq \mu. \quad (\text{A.8})$$

Proof. The Hilbert space \mathcal{H} is infinite-dimensional, as the norms $\|\cdot\|_1$ and $\|\cdot\|_{\mathcal{M}}$, do not induce the same topology. Furthermore, because $\|\cdot\|_1$ dominates $\|\cdot\|_{\mathcal{M}}$, the inequivalence of norms implies that there exists a sequence $(A^{(n)})_{n \in \mathbb{N}}$ of trace-class operators satisfying (A.7), while $\lim_{n \rightarrow \infty} \|A^{(n)}\|_1 \neq 0$. By restricting to a suitable subsequence, we can also ensure that (A.8) holds.

In the remainder of the proof, we will show that, by appropriately modifying this sequence, we can ensure that its elements lie in $\mathcal{O}_{\text{diff}}$.

We first take care of the condition $\text{tr}(A_+) \leq \frac{1}{11}$. For this, consider the sequence $(B^{(n)})_{n \in \mathbb{N}}$ defined by

$$B^{(n)} := \frac{1}{\max(11\|A^{(n)}\|_1, 1)} A^{(n)}. \quad (\text{A.9})$$

As $\forall n \in \mathbb{N} : \|B^{(n)}\|_{\mathcal{M}} \leq \|A^{(n)}\|_{\mathcal{M}}$, the sequence $(B^{(n)})_{n \in \mathbb{N}}$ still converges with respect to $\|\cdot\|_{\mathcal{M}}$. Furthermore, for all n it holds that $\|B^{(n)}\|_1 \geq \frac{\mu}{11}$. As $\|\cdot\|_1$ is compatible with data processing, it follows that $(B^{(n)})_{n \in \mathbb{N}}$ has the desired property

$$\frac{1}{11} \geq \|B^{(n)}\|_1 \geq |\text{tr}(\Pi_{\pm} B^{(n)} \Pi_{\pm})| = |\text{tr}(B_{\pm}^{(n)})| \quad (\text{A.10})$$

where Π_{\pm} is the projector on the positive (negative) part of $B^{(n)}$. This shows that we can, without loss of generality, assume that $\text{tr}(A_+) \leq \frac{1}{11}$.

¹¹The choice of $\frac{1}{11}$ is due to a preference for prime numbers of at least one of the authors.

Next, we turn to the property $\text{tr}(A^{(n)}) = 0$. Let $|e_0\rangle$ be an eigenvector of $A^{(n)}$ such that the corresponding eigenvalue λ_0 satisfies $0 \leq \lambda_0 \leq \frac{1}{n}$. Such an eigenvector exists as $\text{tr}(A_+^{(n)}) \leq 1$ and the Hilbert space \mathcal{H} is infinite dimensional. Note that the sequence $(B^{(n)})_{n \in \mathbb{N}}$ defined by $B^{(n)} = A^{(n)} - \text{tr}(A^{(n)}) |e_0\rangle\langle e_0|$ does not converge with respect to $\|\cdot\|_1$ because, for all $n \in \mathbb{N}$,

$$\|B^{(n)}\|_1 = \text{tr}(A_+^{(n)}) - \text{tr}(A_-^{(n)}) - \lambda_0 + |\lambda_0 - \text{tr}(A^{(n)})| \geq \mu - \frac{1}{n}. \quad (\text{A.11})$$

However, it still converges with respect to $\|\cdot\|_{\mathcal{M}}$ as

$$\|B^{(n)}\|_{\mathcal{M}} \leq \|A^{(n)}\|_{\mathcal{M}} + |\text{tr}(A^{(n)})| \leq 2\|A^{(n)}\|_{\mathcal{M}} \quad (\text{A.12})$$

where we used that $|\text{tr}(A)| \leq \|A\|_{\mathcal{M}}$ in the last inequality. □

Proposition 3. *The following statements are equivalent:*

- (1) *The representation $\mathbf{P}_{\mathcal{M}}$ is robust.*
- (2) *The topologies induced by $\|\cdot\|_{\mathcal{M}}$ and $\|\cdot\|_1$ are identical on $\text{span}(\mathcal{D}(\mathcal{H}))$.¹²*
- (3) *$\text{span}(\mathcal{D}(\mathcal{H}))$ is complete with respect to $\|\cdot\|_{\mathcal{M}}$.*

Proof. (2) \implies (1): Let Σ be a subset of the state space and $(\rho^{(n)})_{n \in \mathbb{N}}$ a sequence such that $\lim_{n \rightarrow \infty} d_{\mathcal{M}}(\rho^{(n)}, \Sigma) = 0$. Then there exists a sequence $(\sigma^{(n)})_{n \in \mathbb{N}} \subset \Sigma$ such that $\lim_{n \rightarrow \infty} d_{\mathcal{M}}(\rho^{(n)}, \sigma^{(n)}) = \lim_{n \rightarrow \infty} \|\rho^{(n)} - \sigma^{(n)}\|_{\mathcal{M}} = 0$. As the norms induce the same topology, it follows that $\lim_{n \rightarrow \infty} \|\rho^{(n)} - \sigma^{(n)}\|_1 = 0$, which implies $\lim_{n \rightarrow \infty} \delta(\rho^{(n)}, \Sigma) = 0$.

(1) \implies (2): Assume by contradiction that (2) does not hold. Then the underlying Hilbert space must be infinite-dimensional, because all norms on a finite-dimensional vector space are equivalent. Let $\{|n\rangle\}_{n \in \mathbb{N}}$ be an orthonormal basis of this Hilbert space and $(A^{(n)})_{n \in \mathbb{N}}$ the sequence of operators in $\mathcal{O}_{\text{diff}}$ as defined by Lemma A.4. From this, we can build sequences $(\rho^{(n)})_{n \in \mathbb{N}}$ and $(\sigma^{(n)})_{n \in \mathbb{N}}$ of states by

$$\rho^{(n)} := |n\rangle\langle n| \left(1 - \text{tr}(A_+^{(n)})\right) + A_+^{(n)}, \quad \sigma^{(n)} := |n\rangle\langle n| \left(1 + \text{tr}(A_-^{(n)})\right) - A_-^{(n)}. \quad (\text{A.13})$$

Note that, because all operators from $\mathcal{O}_{\text{diff}}$ satisfy $\text{tr}(A_+) \leq 1$, these are valid states.

We calculate the distance between any two states of the two sequences. For $n \neq m$, we have

$$\begin{aligned} 2\delta(\rho^{(n)}, \sigma^{(m)}) &= \|\rho^{(n)} - \sigma^{(m)}\|_1 \\ &= \left\| |n\rangle\langle n| \left(1 - \text{tr}(A_+^{(n)})\right) + A_+^{(n)} - |m\rangle\langle m| \left(1 + \text{tr}(A_-^{(m)})\right) + A_-^{(m)} \right\|_1 \\ &\geq \left| 1 - \text{tr}(A_+^{(n)}) + \langle n| A_+^{(n)} |n\rangle + \langle n| A_-^{(m)} |n\rangle \right| \\ &\geq 1 - \text{tr}(A_+^{(n)}) + \text{tr}(A_-^{(m)}) \\ &\geq 1 - \frac{2}{11} \end{aligned} \quad (\text{A.14})$$

¹²This is equivalent to requiring that the inverse of the linear extension of the map $\mathbf{P}_{\mathcal{M}}$ (corresponding to the arrow labelled with “?” in Fig. 2) is continuous with respect to the norm on the probability representation induced by $\|\cdot\|_{\mathcal{M}}$ and the trace norm $\|\cdot\|_1$ on $\text{span}(\mathcal{D}(\mathcal{H}))$.

where, in the first inequality, we used that the 1-norm is non-increasing under any trace non-increasing completely positive map. For $n = m$, we have $\rho^{(n)} - \sigma^{(n)} = A^{(n)}$. Therefore, $\forall n \in \mathbb{N} : \delta(\rho^{(n)}, \sigma^{(n)}) \geq \mu$. Define the set $\Sigma = \{\sigma^{(n)} | n \in \mathbb{N}\}$. By definition, $\lim_{n \rightarrow \infty} d_{\mathcal{M}}(\rho^{(n)}, \Sigma) \leq \lim_{n \rightarrow \infty} d_{\mathcal{M}}(\rho^{(n)}, \sigma^{(n)}) = 0$. Furthermore, for all $n \in \mathbb{N}$, the bound $\delta(\rho^{(n)}, \Sigma) \geq \min(1 - \frac{2}{11}, \mu)$ holds. Therefore, $\mathbf{P}_{\mathcal{M}}$ is not robust.

(2) \implies (3): Assume that the topologies induced by $\|\cdot\|_{\mathcal{M}}$ and $\|\cdot\|_1$ are identical. Then there exists a constant $C > 0$ such that $C\|\cdot\|_1 \leq \|\cdot\|_{\mathcal{M}} \leq \|\cdot\|_1$. Therefore, a sequence is Cauchy or converges with respect to $\|\cdot\|_{\mathcal{M}}$ if and only if it is Cauchy or converges with respect to $\|\cdot\|_1$. The space $\text{span}(\mathcal{D}(\mathcal{H}))$ is the set of Hermitian trace-class operators, which is complete with respect to $\|\cdot\|_1$ [53, 4.2.2. Corollary] and, thus, also with respect to $\|\cdot\|_{\mathcal{M}}$.

(3) \implies (2): Assume the space $\text{span}(\mathcal{D}(\mathcal{H}))$ with the topology induced by $\|\cdot\|_{\mathcal{M}}$ is complete and, thus, a Banach space. Consider the identity map $(\text{span}(\mathcal{D}(\mathcal{H})), \|\cdot\|_1) \rightarrow (\text{span}(\mathcal{D}(\mathcal{H})), \|\cdot\|_{\mathcal{M}})$. This map is continuous as $\|\cdot\|_{\mathcal{M}} \leq \|\cdot\|_1$. By the open mapping theorem for continuous linear functions on Banach spaces [54, Theorem III.11], the inverse of this map is also continuous. Thus, the topologies induced by $\|\cdot\|_{\mathcal{M}}$ and $\|\cdot\|_1$ are identical. \square

Remark A.5. *The representation $\mathbf{P}_{\mathcal{M}}$ being robust is also equivalent to $\text{span}(\mathcal{D}(\mathcal{H}))$ not being meagre¹³ with respect to the topology induced by $\|\cdot\|_{\mathcal{M}}$.*

Proof. If the topologies induced by $\|\cdot\|_{\mathcal{M}}$ and $\|\cdot\|_1$ are identical then, by Proposition 3, $\text{span}(\mathcal{D}(\mathcal{H}))$ equipped with $\|\cdot\|_{\mathcal{M}}$ is a Banach space. It follows directly from the Baire category theorem [54, Theorem III.8] that a Banach space is not meagre.

Conversely, assume the space $\text{span}(\mathcal{D}(\mathcal{H}))$ with the topology induced by $\|\cdot\|_{\mathcal{M}}$ is not meagre. Consider the family of functionals $\mathcal{F} := \{A \in \text{span}(\mathcal{D}(\mathcal{H})) \mapsto \text{tr}(EA) | 0 \leq E \leq \mathbb{1}\}$. This family of functionals is pointwise bounded on $\text{span}(\mathcal{D}(\mathcal{H}))$:

$$\forall A \in \text{span}(\mathcal{D}(\mathcal{H})) : \sup_{0 \leq E \leq \mathbb{1}} \text{tr}(EA) = \|A\|_1 < \infty. \quad (\text{A.15})$$

As $\text{span}(\mathcal{D}(\mathcal{H}))$ is not meagre with respect to the topology induced by $\|\cdot\|_{\mathcal{M}}$, we can apply Banach-Steinhaus [55, Theorem 2.5], which implies that the family of functionals \mathcal{F} is pointwise equicontinuous with respect to $\|\cdot\|_{\mathcal{M}}$. Therefore, for every $\varepsilon > 0$, there is a $\delta > 0$ such that $\|A\|_{\mathcal{M}} \leq \delta \implies \|A\|_1 \leq \varepsilon$. Thus, any sequence that converges with respect to $\|\cdot\|_{\mathcal{M}}$ also converges with respect to $\|\cdot\|_1$. The reverse is also true as $\|\cdot\|_{\mathcal{M}} \leq \|\cdot\|_1$. Thus, the topologies induced by $\|\cdot\|_{\mathcal{M}}$ and $\|\cdot\|_1$ are identical. \square

B Asymptotic entropy

Here we give the formal version of Definition 4. First, we define the allowed decoding operations.

Definition B.1. *Let \mathcal{E} be a collection of POVM elements and M a POVM on a measurable space (\mathcal{O}, Σ_M) . A decoding operation \mathcal{D}_M for M maps lists of probabilities $(P_E)_{E \in \mathcal{E}}$ to a*

¹³A topological space X is meagre if it is the countable union of nowhere dense sets, i.e., sets whose closures have an empty interior.

function

$$\mathcal{D}_M((P_E)_{E \in \mathcal{E}}) : F \in \mathcal{S} \mapsto \sum_E p_E(F) P_E \in \mathbb{R} \quad (\text{B.1})$$

where the sum runs over finitely many elements of \mathcal{E} , $\{p_E\}_{E \in \mathcal{E}} \subset \mathbb{R}_+$, and \mathcal{S} is a semi-algebra that generates Σ_M and is closed under finite disjoint unions.

To define ε -decoding, we use the following norm on functions $P : \mathcal{S} \rightarrow \mathbb{R}$:

$$\|P\| := \sup_{F \in \mathcal{S}} |P(F)|. \quad (\text{B.2})$$

Definition B.2. Let \mathcal{E} be a collection of POVM elements. We say that \mathcal{M} can be ε -decoded from \mathcal{E} if for every $M \in \mathcal{M}$ there exists a sequence of decoding operations $(\mathcal{D}_M^{(n)})_{n \in \mathbb{N}}$ such that

$$\forall \rho \in \mathcal{D}(\mathcal{H}) : \limsup_{n \rightarrow \infty} \sup_{M \in \mathcal{M}} \left\| \mathcal{D}_M^{(n)}((\text{tr}(E\rho))_{E \in \mathcal{E}}) - P_M(\rho) \right\| < \varepsilon. \quad (\text{B.3})$$

Lemma B.3. Let \mathcal{M} be ε -decodable from a set of POVM elements \mathcal{E} and let ρ and σ be states. Then for every $M \in \mathcal{M}$ there exists a semi-algebra \mathcal{S}_M generating Σ_M such that for every $F \in \mathcal{S}_M$ there exists an operator N_F^M in the positive span of \mathcal{E} satisfying

$$\text{tr}(N_F^M \rho) \leq 1 + \varepsilon, \quad \text{tr}(N_F^M \sigma) \leq 1 + \varepsilon, \quad (\text{B.4})$$

$$||\text{tr}(M(F)(\rho - \sigma))| - |\text{tr}(N_F^M(\rho - \sigma))|| \leq 2\varepsilon. \quad (\text{B.5})$$

Proof. Let $(\mathcal{D}_M^{(n)})_{n \in \mathbb{N}, M \in \mathcal{M}}$ be the decoding operations that exist because \mathcal{M} can be ε -decoded from \mathcal{E} , and let $k \in \mathbb{N}$ be such that

$$\sup_{M \in \mathcal{M}} \left\| \mathcal{D}_M^{(k)}((\text{tr}(E\rho))_{E \in \mathcal{E}}) - P_M(\rho) \right\| \leq \varepsilon \text{ and } \sup_{M \in \mathcal{M}} \left\| \mathcal{D}_M^{(k)}((\text{tr}(E\sigma))_{E \in \mathcal{E}}) - P_M(\sigma) \right\| \leq \varepsilon. \quad (\text{B.6})$$

Then, for every $M \in \mathcal{M}$, consider the decoding operation $\mathcal{D}_M^{(k)}$. Let \mathcal{S}_M be the semi-algebra specified by the decoding operation $\mathcal{D}_M^{(k)}$, and let $N_F^M = \sum_{E \in \mathcal{E}} p_E^M(F) E$, where $p_E^M(F)$ is also specified by the decoding operation. Then, by Definition B.2, it follows that for all $M \in \mathcal{M}$ and $F \in \mathcal{S}_M$

$$\begin{aligned} ||\text{tr}(P_M(F)(\rho - \sigma))| - |\text{tr}(N_F^M(\rho - \sigma))|| &\leq |\text{tr}(P_M(F)(\rho - \sigma)) - \text{tr}(N_F^M(\rho - \sigma))| \\ &\leq |\text{tr}(P_M(F)\rho) - \text{tr}(N_F^M\rho)| \\ &\quad + |\text{tr}(P_M(F)\sigma) - \text{tr}(N_F^M\sigma)| \\ &\leq 2\varepsilon. \end{aligned} \quad (\text{B.7})$$

Furthermore, (B.3) ensures that for all $M \in \mathcal{M}$ and $F \in \mathcal{S}_M$

$$\text{tr}(N_F^M \rho) \leq \text{tr}(P_M(F)\rho) + \varepsilon \leq 1 + \varepsilon. \quad (\text{B.8})$$

The same argument also applies to σ . \square

B.1 Proof of Theorem 7

Let \mathcal{H} be a d -dimensional Hilbert space, $|\psi\rangle \in \mathcal{H}$ and $\rho \in \mathcal{D}(\mathcal{H})$. For the proof of Theorem 7, the following function is useful

$$D_{|\psi\rangle}^\rho : U(\mathcal{H}) \rightarrow \mathbb{R}$$

$$U \mapsto \left| \langle \psi | U \rho U^\dagger | \psi \rangle - \frac{1}{d} \right|. \quad (\text{B.9})$$

Let us now prove some properties of this function.

Lemma B.4. *For every $|\psi\rangle \in \mathcal{H}$, the function $D_{|\psi\rangle}^\rho$ is $2^{-H_{\min}(\rho) + \frac{3}{2}}$ -Lipschitz with respect to the 2-norm on the group $U(\mathcal{H})$ of unitaries on \mathcal{H} .*

Proof. First note that it suffices to show for every $|\psi\rangle$ that

$$|D_{|\psi\rangle}^\rho(U) - D_{|\psi\rangle}^\rho(\mathbb{1})| \leq 2^{-H_{\min}(\rho) + \frac{3}{2}} \|U - \mathbb{1}\|_2, \quad (\text{B.10})$$

as then the lemma follows from

$$|D_{|\psi\rangle}^\rho(U) - D_{|\psi\rangle}^\rho(U')| = |D_{(U')^\dagger |\psi\rangle}^\rho((U')^\dagger U) - D_{(U')^\dagger |\psi\rangle}^\rho(\mathbb{1})|, \quad (\text{B.11})$$

and the fact that, for all $X \in \text{Herm}(L)$ and $U \in U(L)$ it holds that $\|UX\|_2 = \|X\|_2$.

We define $\theta \in [0, \pi)$ by

$$\cos(\theta) = |\langle \psi | U | \psi \rangle| \quad (\text{B.12})$$

and a state $|\bar{\psi}\rangle$ such that $\langle \bar{\psi} | \psi \rangle = 0$, as well as

$$U | \psi \rangle = e^{i\varphi} (\cos(\theta) | \psi \rangle + \sin(\theta) | \bar{\psi} \rangle). \quad (\text{B.13})$$

Then, we find that

$$\begin{aligned} |D_{|\psi\rangle}^\rho(U) - D_{|\psi\rangle}^\rho(\mathbb{1})| &\leq |\langle \psi | \rho | \psi \rangle - \langle \psi | U \rho U^\dagger | \psi \rangle| \\ &= |(1 - \cos(\theta)^2) \langle \psi | \rho | \psi \rangle - \sin(\theta)^2 \langle \bar{\psi} | \rho | \bar{\psi} \rangle - 2 \sin(\theta) \cos(\theta) \text{Re}(\langle \bar{\psi} | \rho | \psi \rangle)| \\ &\leq \sin(\theta)^2 (\langle \psi | \rho | \psi \rangle + \langle \bar{\psi} | \rho | \bar{\psi} \rangle) + |2 \sin(\theta) \cos(\theta)| |\text{Re}(\langle \bar{\psi} | \rho | \psi \rangle)| \end{aligned} \quad (\text{B.14})$$

We estimate $\langle \psi | \rho | \psi \rangle$, $\langle \bar{\psi} | \rho | \bar{\psi} \rangle$ and $|\text{Re}(\langle \bar{\psi} | \rho | \psi \rangle)|$. By definition of the min-entropy, it holds that $\rho \leq 2^{-H_{\min}(\rho)} \mathbb{1}$. Thus, we find that $\langle \psi | \rho | \psi \rangle \leq 2^{-H_{\min}(\rho)}$ and $\langle \bar{\psi} | \rho | \bar{\psi} \rangle \leq 2^{-H_{\min}(\rho)}$. To bound $|\text{Re}(\langle \bar{\psi} | \rho | \psi \rangle)|$, we observe that

$$\begin{aligned} |\text{Re}(\langle \bar{\psi} | \rho | \psi \rangle)|^2 &\leq |\langle \bar{\psi} | \rho | \psi \rangle|^2 \\ &= \langle \bar{\psi} | \rho | \psi \rangle \langle \psi | \rho | \bar{\psi} \rangle \\ &\leq \langle \bar{\psi} | \rho^2 | \bar{\psi} \rangle \\ &\leq 2^{-2H_{\min}(\rho)}. \end{aligned} \quad (\text{B.15})$$

Thus, also $|\operatorname{Re}(\langle \bar{\psi} | \rho | \psi \rangle)| \leq 2^{-H_{\min}(\rho)}$. Plugging this result into the previous calculation, we find that

$$\begin{aligned}
|D_{|\psi\rangle}^{\rho}(U) - D_{|\psi\rangle}^{\rho}(\mathbb{1})| &\leq 2^{-H_{\min}(\rho)+1} \left(\sin(\theta)^2 + |\cos(\theta) \sin(\theta)| \right) \\
&= 2^{-H_{\min}(\rho)+1} \sqrt{\sin(\theta)^4 + \cos(\theta)^2 \sin(\theta)^2 + 2 \sin(\theta)^2 |\cos(\theta) \sin(\theta)|} \\
&\leq 2^{-H_{\min}(\rho)+1} \sqrt{\sin(\theta)^4 + \cos(\theta)^2 \sin(\theta)^2 + \sin(\theta)^2} \\
&= 2^{-H_{\min}(\rho)+\frac{3}{2}} \sqrt{\sin(\theta)^2} = 2^{-H_{\min}(\rho)+\frac{3}{2}} \sqrt{1 - \cos(\theta)^2}
\end{aligned} \tag{B.16}$$

Let us now relate this result to the 2-norm. First, we observe that

$$\begin{aligned}
\| |\psi\rangle - U |\psi\rangle \|^2 &= 2 - 2 \operatorname{Re}(\langle \psi | U | \psi \rangle) \\
&= 2 - 2 \cos(\varphi) \cos(\theta) - (1 - \cos(\theta)^2) + (1 - \cos(\theta)^2) \\
&\geq \cos(\varphi)^2 - 2 \cos(\varphi) \cos(\theta) + \cos(\theta)^2 + (1 - \cos(\theta)^2) \\
&= (\cos(\varphi) - \cos(\theta))^2 + (1 - \cos(\theta)^2) \\
&\geq 1 - \cos(\theta)^2.
\end{aligned} \tag{B.17}$$

Furthermore, $\| |\psi\rangle - U |\psi\rangle \|^2$ can be bounded by $\|\mathbb{1} - U\|_2^2$

$$\begin{aligned}
\| |\psi\rangle - U |\psi\rangle \|^2 &= 2 - 2 \operatorname{Re}(\langle \psi | U | \psi \rangle) \\
&= \operatorname{tr} \left(|\psi\rangle \langle \psi| (2\mathbb{1} - U - U^\dagger) \right) \\
&= \operatorname{tr} \left(|\psi\rangle \langle \psi| (\mathbb{1} - U)^\dagger (\mathbb{1} - U) \right) \\
&\leq \operatorname{tr} \left((\mathbb{1} - U)^\dagger (\mathbb{1} - U) \right) = \|\mathbb{1} - U\|_2^2
\end{aligned} \tag{B.18}$$

where in the last inequality we used that $(\mathbb{1} - U)^\dagger (\mathbb{1} - U)$ is a positive operator. Thus,

$$|D_{|\psi\rangle}^{\rho}(U) - D_{|\psi\rangle}^{\rho}(\mathbb{1})| \leq 2^{-H_{\min}(\rho)+\frac{3}{2}} \| |\psi\rangle - U |\psi\rangle \| \leq 2^{-H_{\min}(\rho)+\frac{3}{2}} \|\mathbb{1} - U\|_2^2. \tag{B.19}$$

□

Lemma B.5. *The average of $D_{|\psi\rangle}^{\rho}(U)$ over U chosen according to the Haar measure satisfies*

$$\langle D_{|\psi\rangle}^{\rho} \rangle = \int D_{|\psi\rangle}^{\rho}(U) dU \leq 2^{-\log(d) - \frac{1}{2} H_{\min}(\rho)}. \tag{B.20}$$

Proof. To calculate this average, we use [56, Theorem 3.3], from which it follows that

$$\int \left| \langle \psi | U \rho U^\dagger | \psi \rangle - \frac{1}{d} \right| dU \leq 2^{-\frac{1}{2}(H_2(\rho) + H_2(\tau))} \tag{B.21}$$

where $H_2(\rho) := -\log(\operatorname{tr}(\rho^2)) \leq H_{\min}(\rho)$ and $\tau = \frac{1}{d} |\psi\rangle \langle \psi|$. Thus, we find

$$\int \left| \langle \psi | U \rho U^\dagger | \psi \rangle - \frac{1}{d} \right| dU \leq 2^{-\log(d) - \frac{1}{2} H_{\min}(\rho)}. \tag{B.22}$$

□

Lemma B.6. Let \mathcal{H} be an infinite-dimensional Hilbert space, $\{|n\rangle\}_{n \in \mathbb{N}}$ an orthonormal basis of \mathcal{H} , and $(\rho^{(m)})_{m \in \mathbb{N}}, (\sigma^{(n)})_{n \in \mathbb{N}}$ two sequences of states defined by

$$\rho^{(m)} := \frac{1}{m} \sum_{k=0}^{m-1} |k\rangle\langle k|, \quad \sigma^{(n)} = \sum_{k=0}^{n-1} \frac{2(n-k)}{n(n+1)} |k\rangle\langle k|, \quad (\text{B.23})$$

then there is an $N \in \mathbb{N}$ such for all $\forall m \in \mathbb{N}, n \geq N : \|\text{spec}(\sigma^{(n)}) - \text{spec}(\rho^{(m)})\|_1 \geq \frac{2}{11}$.

Proof. We distinguish different cases.

Case $m \geq n - 1$: In this case, we can write

$$\|\text{spec}(\sigma^{(n)}) - \text{spec}(\rho^{(m)})\|_1 = \left(\sum_{k=0}^{n-1} \left| \frac{2(n-k)}{n(n+1)} - \frac{1}{m} \right| + \left| 0 - (m-n) \frac{1}{m} \right| \right). \quad (\text{B.24})$$

The sum can be divided into two parts of equal magnitude: the part where the terms in the absolute value are positive and one where they are negative. The former is the case when $k \in \{0, \dots, k_{\max}\}$ with $k_{\max} := n - \frac{n(n+1)}{2m}$. Therefore, we find by a straightforward but tedious calculation¹⁴

$$\begin{aligned} \frac{1}{2} \|\text{spec}(\sigma^{(n)}) - \text{spec}(\rho^{(m)})\|_1 &= \sum_{k=0}^{k_{\max}} \left| \frac{2(n-k)}{n(n+1)} - \frac{1}{m} \right| + \left| 0 - (m-n) \frac{1}{m} \right| \\ &\geq \frac{1}{4} + O\left(\frac{1}{n}\right). \end{aligned} \quad (\text{B.25})$$

Case $m < n - 1$: In this case, we can write

$$\|\text{spec}(\sigma^{(n)}) - \text{spec}(\rho^{(m)})\|_1 = \frac{1}{2} \sum_{k=0}^m \left| \frac{2(n-k)}{n(n+1)} - \frac{1}{m} \right| + \frac{1}{2} \sum_{k=m+1}^{n-1} \left| \frac{2(n-k)}{n(n+1)} - 0 \right|. \quad (\text{B.26})$$

We consider two subcases.

Case $k_{\max} \geq 0$: In this case $n - \frac{n(n+1)}{2m} \geq 0 \iff m \geq \frac{n+1}{2}$. As before, we divide the sum into two parts of equal magnitude: the part where the terms in the absolute value are positive and where they are negative. The latter is the case if $m \geq k \geq k_{\max}$. Thus, we find by a straightforward but tedious calculation:

$$\begin{aligned} \frac{1}{2} \|\text{spec}(\sigma^{(n)}) - \text{spec}(\rho^{(m)})\|_1 &= \sum_{k=k_{\max}}^m \left| \frac{2(n-k)}{n(n+1)} - \frac{1}{m} \right| \\ &\geq \left(1 - \frac{m}{n}\right)^2 + \left(1 - \frac{n}{2m}\right)^2 + O\left(\frac{1}{n}\right). \end{aligned} \quad (\text{B.27})$$

Consider the function $f(x) := (1 - \frac{1}{x})^2 + (1 - \frac{x}{2})^2$. To find the minimum of this function, we set its derivative to zero

$$2 \frac{1}{x^2} \left(1 - \frac{1}{x}\right) - \left(1 - \frac{x}{2}\right) = 0. \quad (\text{B.28})$$

This equation is solved by $x = \sqrt{2}$. Therefore, the minimum of this function is $f(\sqrt{2}) = 2(1 - \frac{1}{\sqrt{2}})^2 \approx 0.17 > \frac{1}{11}$, which puts a lower bound on (B.27).

¹⁴To see the tedious calculations in this proof, download the source code and enable the option “showcalc”.

Case $k_{\max} < 0$: In this case $n - \frac{n(n+1)}{2m} < 0 \iff m < \frac{n+1}{2}$ and we find by another tedious calculation

$$\begin{aligned} \frac{1}{2} \|\text{spec}(\sigma^{(n)}) - \text{spec}(\rho^{(m)})\|_1 &= \sum_{k=0}^m \left| \frac{2(n-k)}{n(n+1)} - \frac{1}{m} \right| \\ &\geq \frac{1}{4} + O\left(\frac{1}{n}\right) \end{aligned} \quad (\text{B.29})$$

□

Theorem 7. *If \mathcal{M} has asymptotic entropy at most $(\varepsilon_n 2^n)_{n \in \mathbb{N}}$ for a zero-sequence $(\varepsilon_n)_{n \in \mathbb{N}}$, then the representation $\mathbf{P}_{\mathcal{M}}$ is not robust.*

Proof. Let $\{\Pi_{2^n}\}_{n \in \mathbb{N}}$ be the family of projectors, $\{\mathcal{E}_n\}_{n \in \mathbb{N}}$ the sequence of sets of POVM elements, and $(\eta_n)_{n \in \mathbb{N}}$ the zero-sequence that yield the asymptotic entropy at most $(\varepsilon_n 2^n)_{n \in \mathbb{N}}$. The family of projectors $\{\Pi_{2^n}\}_{n \in \mathbb{N}}$ commutes. Therefore, there exists a basis $\{|n\rangle\}_{n \in \mathbb{N}}$ such that the span of the first 2^n basis elements is contained in the support of Π_{2^n} . Using this basis we define the projectors $P_n = \sum_{i=0}^{2^n-1} |i\rangle\langle i|$, the sequence

$$\sigma^{(n)} := \sum_{k=0}^{2^n-1} \frac{2(2^n - k)}{2^n(2^n + 1)} |k\rangle\langle k|, \quad (\text{B.30})$$

and the set

$$\Sigma := \bigcup_{n=0}^{\infty} \mathcal{B}^{\frac{1}{13}}\left(\frac{P_n}{n}\right), \quad (\text{B.31})$$

where $\mathcal{B}^\varepsilon(\rho) := \{\sigma \in \mathcal{D}(\mathcal{H}) \mid \delta(\sigma, \rho) < \varepsilon\}$. Furthermore, we denote by \mathcal{H}_n the Hilbert space spanned by $\{|0\rangle, \dots, |n\rangle\}$.

Next we show, that there is an $N \in \mathbb{N}$ such that for all $n > N$ and unitaries U on \mathcal{H}_{2^n} it holds that $U\sigma^{(n)}U^\dagger \notin \Sigma$. To show this, we use [57, Lemma IV.3.1]

$$\forall \rho, \sigma : \|\rho - \sigma\|_1 \geq \|\text{spec}(\sigma) - \text{spec}(\rho)\|_1 \quad (\text{B.32})$$

where $\text{spec}(\rho)$ is the probability distribution defined by the ordered list of eigenvalues of ρ . As the spectrum of an operator is invariant under unitary operations, it follows from Lemma B.6 that there is an $N \in \mathbb{N}$ such that $\forall U \in U(\mathcal{H}_{2^n}), n > N : \delta(U\sigma^{(n)}U^\dagger, \Sigma) \geq \frac{1}{11}$. Therefore, $\forall U \in U(\mathcal{H}_{2^n}) : \lim_{n \rightarrow \infty} \delta(U\sigma^{(n)}U^\dagger, \Sigma) \neq 0$.

Our goal is now to show that there exists a sequence of unitaries $\{U^{(n)}\}_{n \in \mathbb{N}}$ such that $U^{(n)}$ has support on \mathcal{H}_{2^n} and $\lim_{n \rightarrow \infty} d_{\mathcal{M}}(U^{(n)}\sigma^{(n)}(U^{(n)})^\dagger, 2^{-n}P_{2^n}) = 0$. If such a sequence of unitaries exists, this implies immediately that $\lim_{n \rightarrow \infty} d_{\mathcal{M}}(U^{(n)}\sigma^{(n)}(U^{(n)})^\dagger, \Sigma) = 0$ and, by the above result about δ , the representation $\mathbf{P}_{\mathcal{M}}$ is not robust.

Because the support of P_{2^n} and $\sigma^{(n)}$ is contained in the support of Π_{2^n} , for any measurement $M \in \mathcal{M}$ and unitary $U \in U(\mathcal{H}_{2^n})$ it holds that

$$\|P_M(U\sigma^{(n)}U^\dagger) - P_M(2^{-n}P_{2^n})\|_1 = \|P_{M|_{\Pi_{2^n}}}(U\sigma^{(n)}U^\dagger) - P_{M|_{\Pi_{2^n}}}(2^{-n}P_{2^n})\|_1. \quad (\text{B.33})$$

Therefore, it suffices to consider measurements in $\mathcal{M}|_{\Pi_{2^n}}$, which, by assumption of the theorem, can be η_n -decoded from \mathcal{E}_n . Therefore, we can apply Lemma B.3 to the

states $U\sigma^{(n)}U^\dagger$ and $2^{-n}P_{2^n}$. Let \mathcal{S}_M be the semi-algebra and let N_F^M be the operator from Lemma B.3 associated to $M \in \mathcal{M}$ and $F \in \mathcal{S}_M$, then

$$\begin{aligned}
d_{\mathcal{M}}(U\sigma^{(n)}U^\dagger, 2^{-n}P_{2^n}) &= \sup_{M \in \mathcal{M}} \sup_{F \in \mathcal{S}_M} |\text{tr}(M(F)(2^{-n}P_{2^n} - U\sigma^{(n)}U^\dagger))| \\
&\leq 2\eta_n + \sup_{M \in \mathcal{M}} \sup_{F \in \mathcal{S}_M} |\text{tr}(N_F^M(2^{-n}P_{2^n} - U\sigma^{(n)}U^\dagger))| \\
&= 2\eta_n + \sup_{M \in \mathcal{M}} \sup_{F \in \mathcal{S}_M} |\text{tr}(P_{2^n}N_F^MP_{2^n}(2^{-n}P_{2^n} - U\sigma^{(n)}U^\dagger))| \\
&\leq 2\eta_n + \sup_{M \in \mathcal{M}} \sup_{F \in \mathcal{S}_M} \sum_{E \in \mathcal{E}} p_E^M(F) |\text{tr}(P_{2^n}EP_{2^n}(2^{-n}P_{2^n} - U\sigma^{(n)}U^\dagger))|, \quad (\text{B.34})
\end{aligned}$$

where the sum over E goes over finitely many $p_E^M(F) > 0$. For every $\bar{E} = \sum_j p_j |\psi_j\rangle\langle\psi_j| \in P_{2^n}\mathcal{E}_n P_{2^n}$ we define a function

$$D_{\bar{E}} : U \rightarrow \sum_j p_j D_{|\psi_j\rangle}^{\sigma^{(n)}}(U) \quad (\text{B.35})$$

where $D_{|\psi_j\rangle}^{\sigma^{(n)}}(U)$ is given by (B.9). Diagonalizing $P_{2^n}EP_{2^n}$ and applying the triangle inequality for the absolute value yields

$$d_{\mathcal{M}}(U\sigma^{(n)}U^\dagger, 2^{-n}P_{2^n}) \leq 2\eta_n + \sup_{M \in \mathcal{M}} \sup_{F \in \mathcal{S}_M} \sum_{E \in \mathcal{E}} p_E^M(F) D_{P_{2^n}EP_{2^n}}(U). \quad (\text{B.36})$$

We now turn to finding upper bounds on $D_{\bar{E}}(U)$. To do so, the following two observations are useful. The function $D_{\bar{E}}$ is $2^{-n+\frac{5}{2}} \text{tr}(\bar{E})$ -Lipschitz continuous with respect to the 2-norm on $U(\mathcal{H}_{2^n})$, as

$$\begin{aligned}
|D_{\bar{E}}(U) - D_{\bar{E}}(U')| &\leq \sum_j p_j |D_{|\psi_j\rangle}^{\sigma^{(n)}}(U) - D_{|\psi_j\rangle}^{\sigma^{(n)}}(U')| \\
&\leq \sum_j p_j \frac{4\sqrt{2}}{2^n + 1} \|U - U'\|_2 \\
&\leq 2^{-n+\frac{5}{2}} \text{tr}(\bar{E}) \|U - U'\|_2
\end{aligned} \quad (\text{B.37})$$

where for the second inequality we used Lemma B.4 and that $H_{\min}(\sigma^{(n)}) = -\log\left(\frac{2}{2^n+1}\right)$. Furthermore, from Lemma B.5, it follows that for a unitary U chosen according to the Haar measure $\langle D_{\bar{E}}(U) \rangle \leq 2^{-\frac{3}{2}n+\frac{1}{2}} \text{tr}(\bar{E})$.

These two observations about $D_{\bar{E}}(U)$ allow us to apply [58, Theorem 5.16 and Theorem 5.9], which states that, for any d -dimensional Hilbert space \mathcal{H} , for any function $f : U(\mathcal{H}) \rightarrow \mathbb{R}$ that is κ -Lipschitz with respect to the 2-norm, and for a unitary U chosen according to the Haar measure we have

$$\Pr(f(U) \geq \langle f \rangle + \varepsilon) \leq e^{-\frac{\varepsilon^2 d}{24\kappa^2}}. \quad (\text{B.38})$$

Applying this theorem yields

$$\Pr(D_{\bar{E}}(U) \geq \Delta(\bar{E})) \leq e^{-\frac{\delta_n^2 2^n}{24(4\sqrt{2})^2}} \quad (\text{B.39})$$

where $\Delta(\bar{E}) := 2^{-n} \text{tr}(\bar{E}) \left(2^{-\frac{n}{2} + \frac{1}{2}} + \delta_n \right)$ and $\delta_n^2 := \frac{24(4\sqrt{2})^2}{2^n} (1 + \ln(|\mathcal{E}_n|))$. Combined with the union bound this yields

$$\Pr(\exists \bar{E} \in P_{2^n} \mathcal{E}_n P_{2^n} : D_{\bar{E}}(U) \geq \Delta(\bar{E})) \leq |P_{2^n} \mathcal{E}_n P_{2^n}| e^{-\frac{\delta_n^2 2^n}{24(4\sqrt{2})^2}} \leq |\mathcal{E}_n| e^{-\frac{\delta_n^2 2^n}{24(4\sqrt{2})^2}}. \quad (\text{B.40})$$

As, $|\mathcal{E}_n| \exp(-\frac{\delta_n^2 2^n}{24(4\sqrt{2})^2}) = e^{-1} < 1$, we have that

$$\Pr(\forall \bar{E} \in P_{2^n} \mathcal{E}_n P_{2^n} : D_{\bar{E}}(U) \leq \Delta(\bar{E})) > 0 \quad (\text{B.41})$$

and, thus, there exists a unitary such that $\forall \bar{E} \in P_{2^n} \mathcal{E}_n P_{2^n} : D_{\bar{E}}(U) \leq \Delta(\bar{E})$. We now define $U^{(n)}$ to be a unitary with this property. From this definition and (B.36), we find

$$\begin{aligned} d_{\mathcal{M}}(U^{(n)} \sigma^{(n)} (U^{(n)})^\dagger, 2^{-n} P_{2^n}) &\leq 2\eta_n + \sup_{M \in \mathcal{M}} \sup_{F \in \mathcal{S}_M} \sum_{E \in \mathcal{E}} p_E^M(F) \Delta(P_{2^n} E P_{2^n}) \\ &\leq 2\eta_n + \left(\sqrt{2} \times 2^{-\frac{n}{2}} + \delta_n \right) \sup_{M \in \mathcal{M}} \sup_{F \in \mathcal{S}_M} \text{tr}(2^{-n} P_{2^n} N_F^M) \\ &\leq 3\eta_n + \left(\sqrt{2} \times 2^{-\frac{n}{2}} + \delta_n \right) \end{aligned} \quad (\text{B.42})$$

By assumption of the theorem, we know that $\lim_{n \rightarrow \infty} \frac{\ln(|\mathcal{E}_n|)}{2^n} = \ln(2) \lim_{n \rightarrow \infty} \varepsilon_n = 0$, which implies that $\lim_{n \rightarrow \infty} \delta_n = 0$. Therefore, $\lim_{n \rightarrow \infty} d_{\mathcal{M}}(U^{(n)} \sigma^{(n)} (U^{(n)})^\dagger, 2^{-n} P_{2^n}) = 0$, which was what remained to prove the theorem. \square

B.2 Proof of Remark 6

Before proving Theorem 7, we recall the definition of ε -nets and one of their properties.

Definition B.7 (ε -net of states). *Let \mathcal{H} be a Hilbert space. Then we call a set of states $\mathcal{N} \subset \mathcal{H}$ an ε -net if*

$$\forall |\varphi\rangle \in \mathcal{H} \exists |\bar{\varphi}\rangle \in \mathcal{N} : \| |\varphi\rangle - |\bar{\varphi}\rangle \| \leq \varepsilon. \quad (\text{B.43})$$

Lemma B.8 (Size of ε -Net). *Let \mathcal{H} be a d -dimensional Hilbert space, then there exists a ε -net \mathcal{N} on \mathcal{H} such that*

$$|\mathcal{N}| \leq \left(1 + \frac{2}{\varepsilon} \right)^{2d}. \quad (\text{B.44})$$

Proof. [59, Theorem 1.8] \square

Lemma B.9. *Let \mathcal{H} be a Hilbert space, then for any two pure states $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ it holds that*

$$\| |\phi\rangle\langle\phi| - |\psi\rangle\langle\psi| \|_1 \leq 2 \| |\phi\rangle - |\psi\rangle \|. \quad (\text{B.45})$$

Proof. First note that

$$\begin{aligned}
\| |\psi\rangle - |\phi\rangle \|^2 &= 2 - 2\text{Re}(\langle\psi|\phi\rangle) \\
&= 2 - 2\text{Re}(\langle\psi|\phi\rangle) - 1 + |\langle\psi|\phi\rangle|^2 + (1 - |\langle\psi|\phi\rangle|^2) \\
&\geq 2 - 2\sqrt{\text{Re}(\langle\psi|\phi\rangle)^2 + \text{Im}(\langle\psi|\phi\rangle)^2} - 1 + |\langle\psi|\phi\rangle|^2 + (1 - |\langle\psi|\phi\rangle|^2) \\
&\geq 1 - 2|\langle\psi|\phi\rangle| + |\langle\psi|\phi\rangle|^2 + (1 - |\langle\psi|\phi\rangle|^2) \\
&= (1 - |\langle\psi|\phi\rangle|)^2 + (1 - |\langle\psi|\phi\rangle|^2) \\
&\geq 1 - |\langle\psi|\phi\rangle|^2 \\
&= \frac{1}{2} \| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|^2_2.
\end{aligned} \tag{B.46}$$

Note that $|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|$ is a Hermitian rank-2 operator, thus there exist states $|e_1\rangle, |e_2\rangle$ such that

$$|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| = a_1 |e_1\rangle\langle e_1| + a_2 |e_2\rangle\langle e_2| \tag{B.47}$$

and, we find that

$$\begin{aligned}
\| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_1 &= |a_1| + |a_2| \\
&= \langle (1, 1), (|a_1|, |a_2|) \rangle \\
&\leq \sqrt{2}(|a_1|^2 + |a_2|^2)^{1/2} \\
&= \sqrt{2} \| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_2.
\end{aligned} \tag{B.48}$$

Combining this result with the above, we find

$$\| |\phi\rangle\langle\phi| - |\psi\rangle\langle\psi| \|_1 \leq 2 \| |\phi\rangle - |\psi\rangle \|. \tag{B.49}$$

□

Lemma B.10. *The set of all measurements has asymptotic entropy at most $(2^{n+\log(n)+3})_{n \in \mathbb{N}}$.*

Proof. Let $\{|n\rangle\}_{n \in \mathcal{N}}$ be a basis, \mathcal{H}_{2^n} the span of the first 2^n basis elements, $\Pi_{2^n} = \sum_{n=0}^{2^n-1} |n\rangle\langle n|$, M a measurement, $M|_{\Pi_{2^n}}$ the restriction of M to the support of Π_{2^n} , and \mathcal{N}_n a (2^{-2^n}) -net on \mathcal{H}_{2^n} .

For any measurable set $F \in \Sigma_M$, consider $M|_{\Pi_{2^n}}(F)$, which has support only on \mathcal{H}_{2^n} . We decompose $M|_{\Pi_{2^n}}(F)$ into its eigenbasis $M|_{\Pi_{2^n}}(F) = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Let $|\phi_i\rangle \in \mathcal{N}_n$ be such that $\| |\phi_i\rangle - |\psi_i\rangle \| \leq 2^{-2^n}$ and define $E_F^M = \sum_i p_i |\phi_i\rangle\langle\phi_i|$. The corresponding decoding operation \mathcal{D}_M is defined in the obvious way. We find

$$\begin{aligned}
|\text{tr}((M|_{\Pi_{2^n}}(F) - E_F^M)\rho)| &\leq \|M|_{\Pi_{2^n}}(F) - E_F^M\|_1 \\
&\leq \sum_i p_i \| |\psi_i\rangle\langle\psi_i| - |\phi_i\rangle\langle\phi_i| \|_1 \\
&\leq 2^{-2n+1} \text{tr}(M|_{\Pi_{2^n}}(F)) \leq 2^{-n+1}
\end{aligned} \tag{B.50}$$

where we used Lemma B.9 in the second to last inequality.

The same argument can be applied for every measurement M and every $F \in \Sigma_M$. Thus, $\mathcal{M}_{\text{all}}|_{\Pi_{2^n}}$ can be 2^{-n+2} -decoded from \mathcal{N}_n , where one understands the elements of

\mathcal{N}_n as the corresponding rank-1 projectors. From Lemma B.8 it follows that there is a 2^{-2n} -net \mathcal{N}_n such that

$$\log(|\mathcal{N}_n|) = 2^{n+1} \log(1 + 2^{2n+1}) \leq (2n + 2)2^{n+1} = 2^{n+\log(n)+3}. \quad (\text{B.51})$$

Therefore, the asymptotic entropy of \mathcal{M}_{all} is at most $(2^{n+\log(n)+3})_{n \in \mathbb{N}}$. \square

Remark 6. *The asymptotic entropy of any \mathcal{M} is at most $(2^{n+\log(n)+3})_{n \in \mathbb{N}}$.*

Proof. We observe that the asymptotic entropy is monotonic under set inclusion: if the asymptotic entropy of \mathcal{M}' is at most $(H_n)_{n \in \mathbb{N}}$ and $\mathcal{M} \subseteq \mathcal{M}'$ then the asymptotic entropy of \mathcal{M} is also at most $(H_n)_{n \in \mathbb{N}}$. The remark then follows from applying this observation to the result of Lemma B.10. \square

B.3 Proof of Corollary 8

Corollary 8. *The representation $\mathbf{P}_{\mathcal{M}_{\otimes}}$ is not robust.*

Proof. Denote the two subsystems relative to which \mathcal{M}_{\otimes} is product to by A and B . Furthermore, let $\{|n\rangle_A\}_{n \in \mathbb{N}}, \{|n\rangle_B\}_{n \in \mathbb{N}}$ be orthonormal bases of \mathcal{H}_A and \mathcal{H}_B respectively. We denote by $\mathcal{H}_{N,A}$ the span of the first N basis vectors and by $\Pi_{N,A}$ the projector onto $\mathcal{H}_{N,A}$, and analogously for $\mathcal{H}_{N,B}$ and $\Pi_{N,B}$. On the joint system AB , we define the family of projectors $\{\Pi_{2^n}\}_{n \in \mathbb{N}}$ as $\Pi_{2^n} = \Pi_{(2^{n/2}),A} \otimes \Pi_{(2^{n/2}),B}$ if n is even and $\Pi_{2^n} = \Pi_{2^{(n+1)/2},A} \otimes \Pi_{2^{(n-1)/2},B}$ if n is odd. Let $\mathcal{N}_A^{(n)}$ and $\mathcal{N}_B^{(n)}$ be 2^{-2n} -nets on the supports of the corresponding subspaces. Using these nets, we define the set of POVM elements

$$\mathcal{E}_n := \{|\psi\rangle\langle\psi|_A \otimes |\phi\rangle\langle\phi|_A \mid |\psi\rangle_A \in \mathcal{N}_A^{(n)}, |\phi\rangle_B \in \mathcal{N}_B^{(n)}\}. \quad (\text{B.52})$$

For any measurement $M = M_A \otimes M_B \in \mathcal{M}_{\otimes}$, the associated σ -algebra, $\Sigma_{M_A \otimes M_B}$, is the product σ -algebra of the σ -algebras associated to the measurements M_A and M_B , i.e., $\Sigma_{M_A \otimes M_B} = \Sigma_{M_A} \otimes \Sigma_{M_B}$. A product σ -algebra admits a semi-algebra of rectangles $\mathcal{S}_{AB} := \{A \times B \mid A \in \Sigma_{M_A}, B \in \Sigma_{M_B}\}$. Denote by \mathcal{S}_{AB}^* the semi-algebra which corresponds to the closure of \mathcal{S}_{AB} under finite disjoint unions. Any $F \in \mathcal{S}_{AB}^*$ is the finite disjoint union of rectangles, i.e., $F = \bigsqcup_{i=1}^k A_i \times B_i$. Therefore, the POVM element $M|_{\Pi_{2^n}}(F)$ can be written as

$$M|_{\Pi_{2^n}}(F) = \sum_{k=1}^{\ell} E_{A,k} \otimes E_{B,k}, \quad (\text{B.53})$$

with $E_{A,k}$ and $E_{B,k}$ POVM elements, such that the support of $E_{A,k} \otimes E_{B,k}$ is contained in the support of Π_{2^n} . Based on their diagonalization $E_{A,k} \otimes E_{B,k} = \sum_i p_{i,k} |\psi_i\rangle\langle\psi_i|_{A,k} \otimes \sum_j q_{j,k} |\phi_j\rangle\langle\phi_j|_{B,k}$, with $p_{i,k}, q_{j,k} \geq 0$, we define

$$N_F^M = \sum_{k=1}^{\ell} \sum_i p_{i,k} |\bar{\psi}_i\rangle\langle\bar{\psi}_i|_{A,k} \otimes \sum_j q_{j,k} |\bar{\phi}_j\rangle\langle\bar{\phi}_j|_{B,k} \quad (\text{B.54})$$

where $|\bar{\psi}_i\rangle\langle\bar{\psi}_i|_{A,k} \in \mathcal{N}_A^{(n)}$ and $|\bar{\phi}_j\rangle\langle\bar{\phi}_j|_{B,k} \in \mathcal{N}_B^{(n)}$ such that $\| |\bar{\psi}_i\rangle_{A,k} - |\psi_i\rangle \| \leq 2^{-2n}$ and analogously for $|\bar{\phi}_j\rangle_{B,k}$. The collection of operators $\{N_F^M\}_{F \in \mathcal{S}_{AB}^*}$ defines a decoding operation

$\mathcal{D}_M((P_E)_{E \in \mathcal{E}_n})$ in the obvious way. Then we find that for all $F \in \mathcal{S}_{AB}^*$

$$\begin{aligned}
|\text{tr}((M|_{\Pi_{2^n}}(F) - N_F^M)\rho)| &\leq \|M|_{\Pi_{2^n}}(F) - N_F^M\|_1 \\
&\leq \sum_{i,j,k} p_{i,k} q_{j,k} \| |\psi_i\rangle\langle\psi_i|_{A,k} \otimes |\phi_i\rangle\langle\phi_i|_{B,k} - |\bar{\psi}_i\rangle\langle\bar{\psi}_i|_{A,k} \otimes |\bar{\phi}_i\rangle\langle\bar{\phi}_i|_{A,k} \|_1 \\
&\leq \sum_{i,j,k} p_{i,k} q_{j,k} (\| |\psi_i\rangle\langle\psi_i|_{A,k} \otimes (|\phi_j\rangle\langle\phi_j|_{B,k} - |\bar{\phi}_j\rangle\langle\bar{\phi}_j|_{B,k}) \|_1 \\
&\quad + \| (|\psi_i\rangle\langle\psi_i|_{A,k} - |\bar{\psi}_i\rangle\langle\bar{\psi}_i|_{A,k}) \otimes |\bar{\phi}_j\rangle\langle\bar{\phi}_j|_{B,k} \|_1) \\
&\leq 2^{-2n+2} \text{tr}(M|_{\Pi_{2^n}}(F)) \leq 2^{-n+2}.
\end{aligned} \tag{B.55}$$

As $M \in \mathcal{M}_{\otimes}$ was arbitrary, $\mathcal{M}_{\otimes}|_{\Pi_{2^n}}$ can be 2^{-n+3} -decoded from \mathcal{E}_n .

By Lemma B.8 there exist nets $\mathcal{N}_A^{(n)}, \mathcal{N}_B^{(n)}$ such that

$$\log(|\mathcal{E}_n|) \leq (2n+2)2^{\frac{n+1}{2}+2} = \left((2n+2)2^{-\frac{n-1}{2}+2}\right)2^n. \tag{B.56}$$

This implies that the asymptotic entropy of \mathcal{M}_{\otimes} is at most $((2n+2)2^{-\frac{n-1}{2}+2})2^n_{n \in \mathbb{N}}$. Thus, by Theorem 7, the representation $\mathbf{P}_{\mathcal{M}_{\otimes}}$ is not robust. \square

Remark B.11. *Note that an analogous proof also shows that the set \mathcal{M}_{sep} of measurements whose POVM elements are separable does not lead to a robust representation.*

B.4 Related results

Theorem 7 characterized the robustness of a set of measurement \mathcal{M} by how compressible the representation $\mathbf{P}_{\mathcal{M}}$ is. Using [35, Theorem 1] one can find a characterization that is based on the asymptotic number of measurements.

Definition B.12. *Let $\{\Pi_{2^n}\}_{n \in \mathbb{N}}$ be a nested family of projectors with $\text{rank}(\Pi_{2^n}) \geq 2^n$, then the asymptotic size of \mathcal{M} is at most $(\log(|\mathcal{M}|_{\Pi_{2^n}}))_{n \in \mathbb{N}}$.*

Theorem B.13. *If there exists a zero-sequence $(\varepsilon_n)_{n \in \mathbb{N}}$ such that \mathcal{M} has asymptotic size at most $(\varepsilon_n 2^{2n})_{n \in \mathbb{N}}$, then $\mathbf{P}_{\mathcal{M}}$ is not robust.*

Proof. If $\log(|\mathcal{M}|_{\Pi_{2^n}}) \leq \varepsilon_n 2^{2n}$, then $|\mathcal{M}|_{\Pi_{2^n}} \leq e^{\ln(2)\varepsilon_n 2^{2n}}$. From [35, Theorem 1] it follows that there are constants $C, c > 0$ such that there exists a Hermitian trace-class operator $A^{(n)}$ with $\|A^{(n)}\|_{\mathcal{M}} \leq \Delta_n \|A^{(n)}\|_1$ where $\Delta_n = \max(\frac{\sqrt{\ln(2)c\varepsilon_n}}{C} 2^{-\frac{n}{2}})$. Therefore, the norms $\|\cdot\|_{\mathcal{M}}$ and $\|\cdot\|_1$ are not equivalent. By Proposition 3, it follows that $\mathbf{P}_{\mathcal{M}}$ is not robust. \square

Combined with Remark 6, this theorem shows that a robust representation $\mathbf{P}_{\mathcal{M}}$ is highly compressible: the number of measurements in $\mathcal{M}|_{\Pi_{2^n}}$, and thus also the number of entries in $\mathbf{P}_{\mathcal{M}}$, needs to scale at least as $2^{2^{2n}}$, but there exists an encoding into a set \mathcal{E} with only of the order of 2^{n2^n} POVM elements.

C Proof of Theorem 11

Before we go on to prove Theorem 11, we review the necessary aspects of GPTs for this paper.

C.1 GPTs

States and measurements. Operationally, a state of a GPT system is understood as a particular preparation procedure. Consequently, the state space is the set of all preparation procedures. It is assumed that the state space is convex. The convex mixture $p\rho + (1-p)\sigma$ of two states ρ, σ is operationally understood as the procedure that prepares ρ with probability p and σ with probability $(1-p)$.¹⁵ Furthermore, two preparation procedures that lead to the same probability distributions for all measurements that can be performed on this system, are treated as the same state. This motivates the following definitions.

Definition C.1. *The state space of a system A is a convex subset $\mathcal{S}_A \subset V_A$ of an \mathbb{R} -vector space V_A ¹⁶ such that there exists a linear function $\mathbf{1}_A : V_A \rightarrow \mathbb{R}$ with the property $\mathbf{1}_A(\mathcal{S}_A) = 1$.*

The set of effects \mathcal{E}_A of system A are a subset of the dual space $\mathcal{E}_A \subseteq V_A^$ such that $\forall E \in \mathcal{E}_A : E(\mathcal{S}_A) \subseteq [0, 1]$ and*

$$\forall \omega_1, \omega_2 \in \mathcal{S}_A : (\forall E \in \mathcal{E}_A : E(\omega_1) = E(\omega_2)) \implies \omega_1 = \omega_2 \quad (\text{C.1})$$

as well as

$$\forall E_1, E_2 \in \mathcal{E}_A : (\forall \omega \in \mathcal{S}_A : E_1(\omega) = E_2(\omega)) \implies E_1 = E_2. \quad (\text{C.2})$$

We call a set of effects $\{E_i\}_{i=1}^N \subseteq \mathcal{E}_A$ a measurement if

$$\sum_{i=1}^N E_i = \mathbf{1}_A. \quad (\text{C.3})$$

As in quantum theory, we define a tomographically complete set of measurements.

Definition C.2. *A set of measurements \mathcal{M} is tomographically complete if the map*

$$v \in \mathcal{S}_A \mapsto (P_M(v))_{M \in \mathcal{M}} \quad (\text{C.4})$$

is injective, where $P_M(\rho)$ is the probability distribution of the measurement \mathcal{M} .

System composition. There is no single rule how the state spaces of two systems A and B compose that applies to any GPT. The only requirement is that states can be independently composed. Technically, this means that for any two systems A, B there exists a bilinear map

$$\begin{aligned} \iota : V_A \times V_B &\rightarrow V_{AB}, \\ (\omega_A, \omega_B) &\mapsto \omega_A \omega_B, \end{aligned} \quad (\text{C.5})$$

such that $\text{Im}(\iota|_{\mathcal{S}_A \times \mathcal{S}_B}) \subset \mathcal{S}_{AB}$ and for any two effects $E_A \in \mathcal{E}_A, E_B \in \mathcal{E}_B$ there is an effect $E_A E_B \in \mathcal{E}_{AB}$ such that

$$(E_A E_B)(\omega_A \omega_B) = E_A(\omega_A) E_B(\omega_B). \quad (\text{C.6})$$

Often one additionally requires that the composition rule satisfies the so-called *local tomography* assumption.

¹⁵An important assumption here is that the randomness that determines whether σ or ρ is prepared is independent of any randomness that is used in the preparation procedure of ρ or σ .

¹⁶The dimension of this vector space may be unbounded.

Definition C.3. A GPT satisfies the local tomography assumption if, for any two systems A and B , the set of product measurements \mathcal{M}_\otimes is tomographically complete.

Metric. In most treatments of GPTs there is no explicit metric defined on the state space. Motivated by the trace distance, we use a metric defined in analogy to the trace distance. A similar metric was already introduced in [8, 9, 15] for operational probabilistic theories, a close relative to GPTs.

Definition C.4. The trace distance δ on the state space \mathcal{S}_A is defined by

$$\delta(\rho, \sigma) := \frac{1}{2} \sup_{M \in \mathcal{M}_A} \|P_M(\rho) - P_M(\sigma)\|_1. \quad (\text{C.7})$$

This metric δ satisfies the composability criterion (1.8) if the system A has the property that for all systems B

$$\forall \rho_B \in \mathcal{S}_B, M \in \mathcal{M}_{AB} : M(\cdot \otimes \rho_B) \in \mathcal{M}_A. \quad (\text{C.8})$$

As we did in quantum theory, we can also define a metric associated to a tomographically complete measurement set \mathcal{M} .

Definition C.5. For any tomographically complete set of measurements \mathcal{M} we define the metric

$$d_{\mathcal{M}}(\rho, \sigma) := \frac{1}{2} \sup_{M \in \mathcal{M}} \|P_M(\rho) - P_M(\sigma)\|_1. \quad (\text{C.9})$$

As in quantum theory, we define the notion of a stable measurement set \mathcal{M} .

Definition C.6. A measurement set \mathcal{M} on a system A , is called stable if for all effects $M \in \mathcal{E}_A$ the topologies induced by $d_{\mathcal{M}}$ and $d_{\mathcal{M} \cup \{(E, \mathbf{1}_A - E)\}}$ are identical.

C.2 Constructing the GPT for Theorem 11

We now construct the GPT that proves Theorem 11. This GPT has two elementary types of systems: keys and locks. All other types of systems are obtained by composing key and lock systems. We start by introducing the elementary systems.

Lock systems. Before we give the formal definition, we give the intuition behind a lock system: A lock system acts like a lock that takes a bit string as input and opens if this bit string matches an internally stored one. More technically, we model a lock as a system where for every¹⁷ bit string $s \in \{0, 1\}^*$, corresponding to the input to the lock, there is a measurement consisting of two effects $E_L^{s \rightarrow \checkmark}$ and $E_L^{s \rightarrow \times}$, corresponding to the outcome that the lock opens or stays closed, respectively. Furthermore, for every bit string k there is a state of the lock $\sigma_L^{(k)}$ where the lock opens upon the input k . Graphically, we depict a

¹⁷We denote by $\{0, 1\}^*$ the set of all bit strings, including the empty bit string.

measurement with input s on this state by

$$E_L^{s \rightarrow \checkmark}(\sigma_L^{(k)}) = \begin{array}{c} s \\ \downarrow \\ \boxed{\begin{array}{c} L \quad k \end{array}} \\ \downarrow \\ \checkmark \end{array} = 1. \quad (\text{C.10})$$

To fully specify the state $\sigma_L^{(k)}$, we also need to define the behaviour of the lock when the input s is different from k . If the input bit string s is longer than k , the lock opens if the first $|k|$ bits of s match with those of k — the lock simply ignores the superfluous input. If s is shorter than k , then the lock just randomly generates more bits, appends them to s , and checks if this new bit string agrees with k . In summary,

$$E_L^{s \rightarrow \checkmark}(\sigma_L^{(k)}) = \begin{array}{c} s \\ \downarrow \\ \boxed{\begin{array}{c} L \quad k \end{array}} \\ \downarrow \\ \checkmark \end{array} = \begin{cases} \delta_{s,k} & \text{if } |s| \geq |k|, \\ \frac{\delta_{s,k}}{2^{|k|-|s|}} & \text{else} \end{cases} \quad (\text{C.11})$$

where $|\cdot|$ denotes the length of a bit string and $\delta_{s,k} = 1$ if deleting the trailing bits of the longer bit string results in two identical bit strings, and $\delta_{s,k} = 0$ otherwise. Sometimes locks can be stubborn, and they do not open no matter what you do.¹⁸ We model this behaviour by a state $\sigma_L^{(\perp)}$ that does not open for any input, i.e.,

$$\forall s \in \{0,1\}^* : E_L^{s \rightarrow \checkmark}(\sigma_L^{(\perp)}) = \begin{array}{c} s \\ \downarrow \\ \boxed{\begin{array}{c} L \quad \perp \end{array}} \\ \downarrow \\ \checkmark \end{array} = 0. \quad (\text{C.12})$$

The state space of a lock system is then the convex hull of $\{\sigma_L^{(k)}\}_{k \in \{0,1\}^* \cup \{\perp\}}$.

Before we state the formal definition, we must introduce some notation. We denote by χ_I is the characteristic function of the set I . For a bit string $s \in \{0,1\}^n$, we define the interval $I_s = [0.s, 0.s + 2^{-n}]$ where $0.s$ understood as the rational number r with $0.s$ as its binary expansion.

Definition C.7. *The state space is of a lock system is*

$$\mathcal{S}_L = \{(f, 1) | f \in \text{conv}(\{\chi_{I_s} | s \in \{0,1\}^*\} \cup \{0\})\} \subset V_L \quad (\text{C.13})$$

with $V_L = L^1([0,1]) \oplus \mathbb{R}$ and the $\mathbf{1}_L$ -effect is given by $\mathbf{1}_L(f, c) = c$.

For every $s \in \{0,1\}^*$ and $r \in \{\checkmark, \times\}$ there is an effect $E_L^{s \rightarrow r}$. The set of effects \mathcal{E}_L is given by all convex combination of these effects. The action of the effect $E_L^{s \rightarrow r}$ on an element of V_L is

$$E_L^{s \rightarrow \checkmark}(f, c) = \frac{1}{|I_s|} \int_{I_s} f(r) dr \quad (\text{C.14})$$

$$E_L^{s \rightarrow \times} = \mathbf{1}_L - E_L^{s \rightarrow \checkmark} \quad (\text{C.15})$$

¹⁸Maybe an angle grinder would open it, but we do not want to harm our object of study.

It is easy to see that this combination of states and effects satisfies Definition C.1. The states $\sigma_L^{(k)}$ and $\sigma_L^{(\perp)}$ we intuitively introduced before, are formally given by

$$\sigma_L^{(k)} := (\chi_{I_k}, 1) \quad (\text{C.16})$$

$$\sigma_L^{(\perp)} := (0, 1). \quad (\text{C.17})$$

Indeed, these states have the desired behaviour when measured, as

$$E_L^{s \rightarrow \checkmark}(\sigma_L^{(\perp)}) = 0 \quad (\text{C.18})$$

$$E_L^{s \rightarrow \checkmark}(\sigma_K^{(k)}) = \frac{1}{|I_s|} \int_{I_s} \chi_k dx = \frac{|I_s \cap I_k|}{|I_s|} = \begin{cases} \delta_{s,k} & \text{if } |s| \geq |k| \\ \frac{\delta_{s,k}}{2^{|k|-|s|}} & \text{else} \end{cases}. \quad (\text{C.19})$$

Key systems. Intuitively, a key system is a system that has an internally stored bit string, the key. The system can be queried to output the first n bits of the key, where n is any natural number (including 0). More technically speaking, there is a measurement consisting of 2^n effects $\{E_K^{n \rightarrow s}\}_{s \in \{0,1\}^n}$, corresponding to the 2^n possibilities for the first n bits of the key. For every bit string $k \in \{0,1\}^*$, there is a state of the key $\sigma_K^{(k)}$, such that if the first n bits of the key are measured, the output is the first n bits of k . In particular, if $n = |k|$, we have

$$E_K^{|k| \rightarrow k}(\sigma_K^{(k)}) = \boxed{\begin{array}{c} \downarrow |k| \\ K \quad k \\ \downarrow k \end{array}} = 1. \quad (\text{C.20})$$

If $n > |k|$, the key system randomly generates bits and appends them to k until the resulting bit string has length n . In particular, if a key system has no key stored, i.e., it is in state $\sigma_K^{(\emptyset)}$, measuring the first n bits of the key yields a uniform distribution over all n -bit strings. We summarize the behaviour of these states

$$E_K^{n \rightarrow s}(\sigma_K^{(k)}) = \boxed{\begin{array}{c} \downarrow n \\ K \quad k \\ \downarrow s \end{array}} = \begin{cases} \delta_{s,k} & \text{if } |k| \geq n \\ \frac{\delta_{s,k}}{2^{n-|k|}} & \text{else} \end{cases}. \quad (\text{C.21})$$

The state space of a key system is then defined as the convex hull of $\{\sigma_K^{(k)}\}_{k \in \{0,1\}^*}$. To make this a valid state space, we need to ensure that states which cannot be distinguished by two measurements are identical. The following formal definition takes care of this.

Definition C.8 (Key systems K). *The state space \mathcal{S}_K is*

$$\mathcal{S}_K = \text{conv} \left(\left\{ \frac{\chi_{I_s}}{|I_s|} \mid s \in \{0,1\}^* \right\} \right) \subset L^1([0,1]) \quad (\text{C.22})$$

The unit effect $\mathbf{1}_K$ is $\mathbf{1}_K(f) = \int_{[0,1]} f(x) dx$. The set of effects \mathcal{E}_K is the convex hull of effects of the form $\sum_{s \in R \subset \{0,1\}^n} E_K^{n \rightarrow s}$. The action of an effect $E_K^{n \rightarrow s}$ on $f \in L^1([0,1])$ is

$$E_K^{n \rightarrow s}(f) = \int_{I_s} f(x) dx. \quad (\text{C.23})$$

It is easy to see that, Definition C.1 is satisfied by this state space and set of effects. The states $\sigma_K^{(k)}$ and $\sigma_K^{(\emptyset)}$ we have intuitively introduced are formally given by

$$\sigma_K^{(k)} := \frac{1}{|I_k|} \chi_{I_k} \quad (\text{C.24})$$

where for $k = \emptyset, I_k = [0, 1]$. These states indeed have the desired behaviour when measured

$$E_K^{n \rightarrow s}(\sigma_K^{(k)}) = \int_{I_s} \chi_{I_k}(x) dx = \frac{|I_s \cap I_k|}{|I_k|} = \begin{cases} \delta_{s,k} & \text{if } |k| \geq n \\ \frac{\delta_{s,k}}{2^{n-|k|}} & \text{else.} \end{cases} \quad (\text{C.25})$$

Composition of keys and locks. To define the composition of key and lock systems, we consider the smallest possible composed state space that still satisfies the requirements of the GPT framework. This means that we only allow for mixtures of product states. On the measurement side, we allow only product measurements and measurements that can be implemented by first measuring one system and then determine the measurement on the next system based on this outcome.

Definition C.9 (Composition rule). *When composing a key and a lock system the function \imath is the tensor product $\otimes : V_K \times V_L \rightarrow V_K \otimes V_L$. The state space of the composed system is defined as the convex hull of $\mathcal{S}_{KL} := \text{conv}(\mathcal{S}_K \otimes \mathcal{S}_L)$. The identity effect is $\mathbf{1}_{KL} := \mathbf{1}_K \otimes \mathbf{1}_L$. The set of effects \mathcal{E}_{KL} are all linear functionals E such that $E(\mathcal{S}_{KL}) \subseteq [0, 1]$ and*

$$\begin{aligned} \exists n \in \mathbb{N}, \{p_i\}_{i \in \{1, \dots, n\}} \in \mathbb{R}_+, \{E_{K,i}\}_{i \in \{1, \dots, n\}} \subset \mathcal{E}_K, \{E_{L,i}\}_{i \in \{1, \dots, n\}} \subset \mathcal{E}_L : \\ E = \sum_{i=1}^n p_i E_{K,i} \otimes E_{L,i} \\ \text{or } E = \mathbf{1}_{KL} - \sum_{i=1}^n p_i E_{K,i} \otimes E_{L,i} \end{aligned} \quad (\text{C.26})$$

The composition of multiple keys and of multiple lock systems is defined analogously.

One important measurement of a key-lock system is the measurement that uses the output of a measurement on the K system to determine the input on the L system. It essentially measures whether the input that opens the lock is the key that is stored in the key system. Mathematically, this measurement is given by the effects

$$\begin{aligned} E_{KL}^{n \rightarrow \checkmark} &:= \sum_{s \in \{0,1\}^n} E_K^{n \rightarrow s} \otimes E_L^{s \rightarrow \checkmark} \\ E_{KL}^{n \rightarrow \times} &:= \mathbf{1}_{KL} - E_{KL}^{n \rightarrow \checkmark}. \end{aligned} \quad (\text{C.27})$$

On a state $\sigma_K^{(k)} \otimes \sigma_L^{(k')}$ with $k, k' \in \{0, 1\}^n$ this measurement acts as

$$E_{KL}^{n \rightarrow \checkmark}(\sigma_K^{(k)} \otimes \sigma_L^{(k')}) = \begin{array}{c} \begin{array}{|c|} \hline K \\ \hline \end{array} \begin{array}{|c|} \hline k \\ \hline \end{array} \otimes \begin{array}{|c|} \hline L \\ \hline \end{array} \begin{array}{|c|} \hline k' \\ \hline \end{array} \\ \downarrow \quad \quad \quad \downarrow \checkmark \end{array} = \delta_{k,k'}. \quad (\text{C.28})$$

Remark C.10. The metric δ satisfies the composability property of (1.8). This follows from (C.8) because any measurement is a sum of product effects with positive coefficients.

The following lemma shows that this GPT satisfies local tomography.

Lemma C.11. Consider a GPT where for every bipartite system AB the joint state space is given by linear combinations of product states, i.e.,

$$S_{AB} \subset \text{span}(\iota(\mathcal{S}_A, \mathcal{S}_B)), \quad (\text{C.29})$$

then this GPT satisfies local tomography.

Proof. For every system A the linear map

$$M_A : v \in \text{span}(\mathcal{S}_A) \mapsto (E(v))_{E \in \mathcal{E}_A} \quad (\text{C.30})$$

is invertible. We define the map $M_A M_B$ on the joint state space by

$$M_A M_B \iota(\sigma_A, \sigma_B) = (E_A(\sigma_A) E_B(\sigma_B))_{E_A \in \mathcal{E}_A, E_B \in \mathcal{E}_B} \quad (\text{C.31})$$

and demanding linearity. Note that the vector space spanned by $(E_A(\sigma_A) E_B(\sigma_B))_{E_A \in \mathcal{E}_A, E_B \in \mathcal{E}_B}$ is isomorphic to the vector space spanned by $(E_A(\sigma_A))_{E_A \in \mathcal{E}_A} \otimes (E_B(\sigma_B))_{E_B \in \mathcal{E}_B}$. Let us denote the isomorphism by Φ . We then find that

$$M_A^{-1} \otimes M_B^{-1} \circ \Phi \circ M_A M_B \iota(\sigma_A, \sigma_B) = \sigma_A \otimes \sigma_B. \quad (\text{C.32})$$

By definition of the tensor product there exists a linear map h such that $h(\sigma_A \otimes \sigma_B) = \iota(\sigma_A, \sigma_B)$. Thus, as all maps are linear, $h \circ M_A^{-1} \otimes M_B^{-1} \circ \Phi$ is the inverse of $M_A M_B$. Hence, a state of the system AB is uniquely determined by the statistics of local measurements. As the systems AB were generic, the theory is locally tomographic. \square

The topology of keys and locks. We are now ready to show that for this GPT the topology induced by $d_{\mathcal{M}_{\otimes}}$ on the state space is different from the topology induced by δ . The intuition behind this proof is to consider the sequence of states $(\rho_{KL}^{(n)})_{n \in \mathbb{N}}$ given by

$$\rho_{KL}^{(n)} := \sum_{k \in \{0,1\}^n} \begin{array}{c} \Downarrow \\ \boxed{K \quad k} \\ \Downarrow \end{array} \otimes \begin{array}{c} \Downarrow \\ \boxed{L \quad k} \\ \Downarrow \end{array}. \quad (\text{C.33})$$

Using only product measurements this state is close to the state $\sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}$. Intuitively, to distinguish these two states, one tries to provoke an opening of the lock. Using only product measurements, one needs to guess the input that opens the lock. This guess is correct only with probability 2^{-n} . Therefore, the distance between $\rho_{KL}^{(n)}$ and $\sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}$ measured by $d_{\mathcal{M}_{\otimes}}$ vanishes as $n \rightarrow \infty$. However, if any measurement can be used, then the measurement that reads out the first n bits of the key and uses this as an input to the lock opens the lock with certainty. Therefore, for any n the distance between $\rho_{KL}^{(n)}$ and $\sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}$ measured by δ is 1. We have thus constructed a sequence that converges with respect to $d_{\mathcal{M}_{\otimes}}$, but not with respect to δ . This immediately implies that these two metrics induce different topologies. We formalize this intuitive argument by the following proposition. Theorem 11 then follows from Proposition C.12 and Lemma C.13.

Proposition C.12. *The metrics $d_{\mathcal{M}_{\otimes}}$ and δ do not induce the same topology on \mathcal{S}_{KL} .*

Proof. Consider the sequence of states $(\rho_{KL}^{(n)})_{n \in \mathbb{N}}$ given by

$$\rho_{KL}^{(n)} := \frac{1}{2^n} \sum_{k \in \{0,1\}^n} \sigma_K^{(k)} \otimes \sigma_L^{(k)}. \quad (\text{C.34})$$

First note that, $\forall n \in \mathbb{N} : \delta(\rho_{KL}^{(n)}, \sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}) = 1$. To see this, consider the measurement given by $\{E_{KL}^{n \rightarrow \checkmark}, \mathbf{1}_{KL} - E_{KL}^{n \rightarrow \checkmark}\}$; see (C.27). For this measurement, we find that

$$\begin{aligned} E_{KL}^{n \rightarrow \checkmark}(\rho_{KL}^{(n)}) &= \frac{1}{2^n} \sum_{k,s \in \{0,1\}^n} E_K^{n \rightarrow s}(\sigma_K^{(k)}) E_L^{s \rightarrow \checkmark}(\sigma_L^{(k)}) \\ &= \frac{1}{2^n} \sum_{k,s \in \{0,1\}^n} \delta_{s,k} E_L^{s \rightarrow \checkmark}(\sigma_L^{(k)}) = 1 \end{aligned} \quad (\text{C.35})$$

whereas

$$E_{KL}^{n \rightarrow \checkmark}(\sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}) = \sum_{s \in \{0,1\}^n} E_K^{n \rightarrow s}(\sigma_K^{(\emptyset)}) E_L^{s \rightarrow \checkmark}(\sigma_L^{(\perp)}) = 0. \quad (\text{C.36})$$

Thus, $\delta(\rho_{KL}^{(n)}, \sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}) = 1$.

Let us now show that with respect to $d_{\mathcal{M}_{\otimes}}$ the sequence $\rho_{KL}^{(n)}$ converges to $\sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}$. Product measurements of key and lock systems are convex mixtures of measurements of the form $M_K \otimes M_L = \{\sum_{\ell \in J_i \subset \{0,1\}^n} E_K^{n \rightarrow \ell} \otimes E_L^{s \rightarrow r}\}_{i,r}$ where $\cup_i J_i = \{0,1\}^n$ and $s \in \{0,1\}^*$. Therefore, it suffices to consider these measurements to calculate $d_{\mathcal{M}_{\otimes}}(\rho_{KL}^{(n)}, \sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)})$. Furthermore, note that when $|s| < n$, the measurement $\{\sum_{\ell \in I_j \subset \{0,1\}^n} E_K^{n \rightarrow \ell} \otimes E_L^{s \rightarrow r}\}_{j,r}$ is a convex mixture of measurements with $|s| = n$. Moreover, when a measurement is applied to the states $\rho_{KL}^{(n)}, \sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}$ and $|s| > n$, the resulting probability distribution is the same as when s is replaced by the bit string s' given by the first n bits of s . Therefore, we only need to consider bit strings s of length n . It is also useful to note that

$$|E_K^{n \rightarrow s} \otimes \mathbf{1}_L(\rho_{KL}^{(n)} - \sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)})| = |2^{-n} \sum_{k \in \{0,1\}^n} E_K^{n \rightarrow s}(\sigma_K^{(k)} - \sigma_K^{(\emptyset)})| = 0. \quad (\text{C.37})$$

Thus, for any such measurement $M_K \otimes M_L$

$$\begin{aligned} &\|P_{M_K \otimes M_L}(\rho_{KL}^{(n)}) - P_{M_K \otimes M_L}(\sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)})\|_1 \\ &\leq \sum_{\ell \in \{0,1\}^n} \sum_{r \in \{\checkmark, \times\}} |E_K^{n \rightarrow \ell} \otimes E_L^{s \rightarrow r}(\rho_{KL}^{(n)} - \sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)})| \\ &= 2 \sum_{\ell \in \{0,1\}^n} E_K^{n \rightarrow \ell} \otimes E_L^{s \rightarrow \checkmark}(\rho_{KL}^{(n)}) \\ &\leq 2^{-n+1} \sum_{\ell \in \{0,1\}^n, k \in \{0,1\}^n} E_K^{n \rightarrow \ell} \otimes E_L^{s \rightarrow \checkmark}(\sigma_K^{(k)} \otimes \sigma_L^{(k)}) \\ &= 2^{-n+1} \sum_{\ell \in \{0,1\}^n} E_K^{n \rightarrow \ell}(\sigma_K^{(s)}) = 2^{-n+1} \end{aligned} \quad (\text{C.38})$$

where in the first equality we used (C.37), $E_L^{s \rightarrow \times} = \mathbf{1}_L - E_L^{s \rightarrow \checkmark}$ and $E_L^{s \rightarrow \checkmark}(\sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}) = 0$. Thus, $\lim_{n \rightarrow \infty} d_{\mathcal{M}_{\otimes}}(\rho_{KL}^{(n)}, \sigma_K^{(\emptyset)} \otimes \sigma_L^{(\perp)}) = 0$.

In summary, we have found a sequence $(\rho_{KL}^{(n)})_{n \in \mathbb{N}}$ of states that converges with respect to $d_{\mathcal{M}_{\otimes}}$, but not with respect to δ . So, the topologies induced by these two metrics are not identical on the state space. \square

Lemma C.13. *The measurement set \mathcal{M}_{\otimes} is stable.*

Proof. For any effect $E \in \mathcal{E}_{SK}$ there exists an $n \in \mathbb{N}$ such that $E = \sum_{i=1}^m p_i E_{K,i} \otimes E_{L,i}$. Let $(\rho_n)_{n \in \mathbb{N}}$ be a sequence that converges to ρ with respect to $d_{\mathcal{M}_{\otimes}}$. Then this sequence also converges with respect to $d_{\mathcal{M}_{\otimes} \cup \{E, \mathbf{1}_{SK} - E\}}$, as

$$\begin{aligned} \lim_{n \rightarrow \infty} d_{\mathcal{M}_{\otimes} \cup \{E, \mathbf{1}_{SK} - E\}}(\rho_n, \rho) &\leq \lim_{n \rightarrow \infty} d_{\mathcal{M}_{\otimes}}(\rho_n, \rho) + \lim_{n \rightarrow \infty} |E(\rho_n - \rho)| \\ &\leq \lim_{n \rightarrow \infty} \sum_{i=1}^m p_i (E_{K,i} \otimes E_{L,i})(\rho_n) \\ &\leq \sum_{i=1}^m p_i \lim_{n \rightarrow \infty} d_{\mathcal{M}_{\otimes}}(\rho_n, \rho) = 0, \end{aligned} \tag{C.39}$$

where we used in the last inequality that for any product effect $E_K \otimes E_L$ the measurement $M = \{E_K \otimes E_L, (\mathbf{1}_K - E_K) \otimes E_L, E_K \otimes (\mathbf{1}_L - E_L), (\mathbf{1}_K - E_K) \otimes (\mathbf{1}_L - E_L)\}$ is a product measurement. \square