entropy

MDPI

Article

Agents, Subsystems, and the Conservation of Information

Giulio Chiribella [1,2,3,4]

[1] Department of Computer Science, University of Oxford, Parks Road, Oxford OX1 3QD, UK; giulio.chiribella@cs.ox.ac.uk
[2] Canadian Institute for Advanced Research, CIFAR Program in Quantum Information Science, 661 University Ave, Toronto, ON M5G 1M1, Canada
[3] Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong, China
[4] HKU Shenzhen Institute of Research and Innovation, Yuexing 2nd Rd Nanshan, Shenzhen 518057, China

Received: 12 March 2018; Accepted: 5 May 2018; Published: 10 May 2018

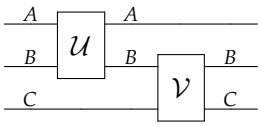
Abstract: Dividing the world into subsystems is an important component of the scientific method. The choice of subsystems, however, is not defined *a priori*. Typically, it is dictated by experimental capabilities, which may be different for different agents. Here, we propose a way to define subsystems in general physical theories, including theories beyond quantum and classical mechanics. Our construction associates every agent A with a subsystem S_A, equipped with its set of states and its set of transformations. In quantum theory, this construction accommodates the notion of subsystems as factors of a tensor product, as well as the notion of subsystems associated with a subalgebra of operators. Classical systems can be interpreted as subsystems of quantum systems in different ways, by applying our construction to agents who have access to different sets of operations, including multiphase covariant channels and certain sets of free operations arising in the resource theory of quantum coherence. After illustrating the basic definitions, we restrict our attention to closed systems, that is, systems where all physical transformations act invertibly and where all states can be generated from a fixed initial state. For closed systems, we show that all the states of all subsystems admit a canonical purification. This result extends the purification principle to a broader setting, in which coherent superpositions can be interpreted as purifications of incoherent mixtures.

Keywords: subsystem; agent; conservation of information; purification; group representations; commuting subalgebras

1. Introduction

The composition of systems and operations is a fundamental primitive in our modelling of the world. It has been investigated in depth in quantum information theory [1,2], and in the foundations of quantum mechanics, where composition has played a key role from the early days of Einstein–Podolski–Rosen [3] and Schroedinger [4]. At the level of frameworks, the most recent developments are the compositional frameworks of general probabilistic theories [5–15] and categorical quantum mechanics [16–20].

The mathematical structure underpinning most compositional approaches is the structure of monoidal category [18,21]. Informally, a monoidal category describes circuits, in which wires represent systems and boxes represent operations, as in the following diagram:



(1)

The composition of systems is described by a binary operation denoted by $\otimes$, and referred to as the "tensor product" (note that $\otimes$ is not necessarily a tensor product of vector spaces). The system $A \otimes B$ is interpreted as the composite system made of subsystems A and B. Larger systems are built in a bottom-up fashion, by combining subsystems together. For example, a quantum system of dimension $d = 2^n$ can arise from the composition of n single qubits.

In some situations, having a rigid decomposition into subsystems is neither the most convenient nor the most natural approach. For example, in algebraic quantum field theory [22], it is natural to start from a single system—the field—and then to identify subsystems, e.g., spatial or temporal modes. The construction of the subsystems is rather flexible, as there is no privileged decomposition of the field into modes. Another example of flexible decomposition into subsystems arises in quantum information, where it is crucial to identify degrees of freedom that can be treated as "qubits". Viola, Knill, and Laflamme [23] and Zanardi, Lidar, and Lloyd [24] proposed that the partition of a system into subsystems should depend on which operations are experimentally accessible. This flexible definition of subsystem has been exploited in quantum error correction, where decoherence free subsystems are used to construct logical qubits that are untouched by noise [25–30]. The logical qubits are described by "virtual subsystems" of the total Hilbert space [31], and in general such subsystems are spread over many physical qubits. In all these examples, the subsystems are constructed through an algebraic procedure, whereby the subsystems are associated with algebras of observables [32]. However, the notion of "algebra of observables" is less appealing in the context of general physical theories, because the multiplication of two observables may not be defined. For example, in the framework of general probabilistic theories [5–15], observables represent measurement procedures, and there is no notion of "multiplication of two measurement procedures".

In this paper, we propose a construction of subsystems that can be applied to general physical theories, even in scenarios where observables and measurements are not included in the framework. The core of our construction is to associate subsystems to sets of *operations*, rather than observables. To fix ideas, it is helpful to think that the operations can be performed by some *agent*. Given a set of operations, the construction extracts the degrees of freedom that are acted upon *only* by those operations, identifying a "private space" that only the agent can access. Such a private space then becomes the subsystem, equipped with its own set of states and its own set of operations. This construction is closely related to an approach proposed by Krämer and del Rio, in which the states of a subsystem are identified with equivalence classes of states of the global system [33]. In this paper, we extend the equivalence relation to transformations, providing a complete description of the subsystems. We illustrate the construction in a several examples, including

1. quantum subsystems associated with the tensor product of two Hilbert spaces,
2. subsystems associated with an subalgebra of self-adjoint operators on a given Hilbert space,
3. classical systems of quantum systems,
4. subsystems associated with the action of a group representation on a given Hilbert space.

The example of the classical systems has interesting implications for the resource theory of coherence [34–41]. Our construction implies that different types of agents, corresponding to different choices of free operations, are associated with the same subsystem, namely the largest classical subsystem of a given quantum system. Specifically, classical systems arise from strictly incoherent operations [41], physically incoherent operations [38,39], phase covariant operations [38–40], and multiphase covariant operations (to the best of our knowledge, multiphase covariant operations have not been considered so far in the resource theory of coherence). Notably, we do not obtain classical subsystems from the maximally incoherent operations [34] and from the incoherent operations [35,36],

which are the first two sets of free operations proposed in the resource theory of coherence. For these two types of operations, we find that the associated subsystem is the whole quantum system.

After examining the above examples, we explore the general features of our construction. An interesting feature is that certain properties, such as the impossibility of instantaneous signalling between two distinct subsystems, arise *by fiat*, rather then being postulated as physical requirements. This fact is potentially useful for the project of finding new axiomatizations of quantum theory [42–48] because it suggests that some of the axioms assumed in the usual (compositional) framework may turn out to be consequences of the very definition of subsystem. Leveraging on this fact, one could hope to find axiomatizations with a smaller number of axioms that pinpoint exactly the distinctive features of quantum theory. In addition, our construction suggests a *desideratum* that every truly fundamental axiom should arguably satisfy: *an axiom for quantum theory should hold for all possible subsystems of quantum systems*. We call this requirement *Consistency Across Subsystems*. If one accepts our broad definition of subsystems, then Consistency Across Subsystems is a very non-trivial requirement, which is not easily satisfied. For example, the Subspace Axiom [5], stating that all systems with the same number of distinguishable states are equivalent, does not satisfy Consistency Across Subsystems because classical subsystems are not equivalent to the corresponding quantum systems, even if they have the same number of distinguishable states.

In general, proving that Consistence Across Subsystems is satisfied may require great effort. Rather than inspecting the existing axioms and checking whether or not they are consistent across subsystems, one can try to formulate the axioms in a way that guarantees the validity of this property. We illustrate this idea in the case of the Purification Principle [8,12,13,15,49–51], which is the key ingredient in the quantum axiomatization of Refs. [13,15,42] and plays a central role in the axiomatic foundation of quantum thermodynamics [52–54] and quantum information protocols [8,15,55–57]. Specifically, we show that the Purification Principle holds for *closed systems*, defined as systems where all transformations are invertible, and where every state can be generated from a fixed initial state by the action of a suitable transformation. Closed systems satisfy the Conservation of Information [58], i.e., the requirement that physical dynamics should send distinct states to distinct states. Moreover, the states of the closed systems can be interpreted as "pure". In this setting, the general notion of subsystem captures the idea of purification, and extends it to a broader setting, allowing us to regard coherent superpositions as the "purifications" of classical probability distributions.

The paper is structured as follows. In Section 2, we outline related works. In Section 3, we present the main framework and the construction of subsystems. The framework is illustrated with five concrete examples in Section 4. In Section 5, we discuss the key structures arising from our construction, such as the notion of partial trace and the validity of the no-signalling property. In Section 6, we identify two requirements, concerning the existence of agents with non-overlapping sets of operations, and the ability to generate all states from a given initial state. We also highlight the relation between the second requirement and the notion of causality. We then move to systems satisfying the Conservation of Information (Section 7) and we formalize an abstract notion of closed systems (Section 8). For such systems, we provide a dynamical notion of pure states, and we prove that every subsystem satisfies the Purification Principle (Section 9). A macro-example, dealing with group representations in quantum theory is provided in Section 10. Finally, the conclusions are drawn in Section 11.

2. Related Works

In quantum theory, the canonical route to the definition of subsystems is to consider commuting algebras of observables, associated with independent subsystems. The idea of defining independence in terms of commutation has a long tradition in quantum field theory and, more recently, quantum information theory. In algebraic quantum field theory [22], the local subsystems associated with causally disconnected regions of spacetime are described by commuting C*-algebras. A closely related approach is to associate quantum systems to von Neumann algebras, which can be characterized as double commutants [59]. In quantum error correction, decoherence free subsystems are associated

with the commutant of the noise operators [28,29,31]. In this context, Viola, Knill, and Laflamme [23] and Zanardi, Lidar, and Lloyd [24] made the point that subsystems should be defined operationally, in terms of the experimentally accessible operations. The canonical approach of associating subsystems to subalgebras was further generalized by Barnum, Knill, Ortiz, and Viola [60,61], who proposed the notion of generalized entanglement, i.e., entanglement relative to a subspace of operators. Later, Barnum, Ortiz, Somma, and Viola explored this notion in the context of general probabilistic theories [62].

The above works provided a concrete model of subsystems that inspired the present work. An important difference, however, is that here we will not use the notions of observable and expectation value. In fact, we will not use any probabilistic notion, making our construction usable also in frameworks where no notion of measurement is present. This makes the construction appealingly simple, although the flip side is that more work will have to be done in order to recover the probabilistic features that are built-in in other frameworks.

More recently, del Rio, Krämer, and Renner [63] proposed a general framework for representing the knowledge of agents in general theories (see also the Ph.D. theses of del Rio [64] and Krämer [65]). Krämer and del Rio further developed the framework to address a number of questions related to locality, associating agents to monoids of operations, and introducing a relation, called *convergence through a monoid*, among states of a global system [33]. Here, we will extend this relation to transformations, and we will propose a general definition of subsystem, equipped with its set of states and its set of transformations.

Another related work is the work of Brassard and Raymond-Robichaud on no-signalling and local realism [66]. There, the authors adopt an equivalence relation on transformations, stating that two transformations are equivalent iff they can be transformed into one another through composition with a local reversible transformation. Such a relation is related to the equivalence relation on transformations considered in this paper, in the case of systems satisfying the Conservation of Information. It is interesting to observe that, notwithstanding the different scopes of Ref. [66] and this paper, the Conservation of Information plays an important role in both. Ref. [66], along with discussions with Gilles Brassard during QIP 2017 in Seattle, provided inspiration for the present paper.

3. Constructing Subsystems

Here, we outline the basic definitions and the construction of subsystems.

3.1. A Pre-Operational Framework

Our starting point is to consider a single system S, with a given set of states and a given set of transformations. One could think S to be the whole universe, or, more modestly, our "universe of discourse", representing the fragment of the world of which we have made a mathematical model. We denote by $\mathsf{St}(S)$ the set of states of the system (sometimes called the "state space"), and by $\mathsf{Transf}(S)$ be the set of transformations the system can undergo. We assume that $\mathsf{Transf}(S)$ is equipped with a composition operation $\circ$, which maps a pair of transformations $\mathcal{A}$ and $\mathcal{B}$ into the transformation $\mathcal{B} \circ \mathcal{A}$. The transformation $\mathcal{B} \circ \mathcal{A}$ is interpreted as the transformation occurring when $\mathcal{B}$ happens right before $\mathcal{A}$. We also assume that there exists an identity operation $\mathcal{I}_S$, satisfying the condition $\mathcal{A} \circ \mathcal{I}_S = \mathcal{I}_S \circ \mathcal{A} = \mathcal{A}$ for every transformation $\mathcal{A} \in \mathsf{Transf}(A)$. In short, we assume that the physical transformations form a *monoid*.

We do not assume any structure on the state space $\mathsf{St}(S)$: in particular, we do not assume that $\mathsf{St}(S)$ is convex. We do assume, however, is that there is an action of the monoid $\mathsf{Transf}(S)$ on the set $\mathsf{St}(S)$: given an input state $\psi \in \mathsf{St}(S)$ and a transformation $\mathcal{T} \in \mathsf{Transf}(S)$, the action of the transformation produces the output state $\mathcal{T}\psi \in \mathsf{St}(S)$.

Example 1 (Closed quantum systems)**.** *Let us illustrate the basic framework with a textbook example, involving a closed quantum system evolving under unitary dynamics. Here, S is a quantum system of dimension*

d, and the state space $\mathsf{St}(S)$ *is the set of pure quantum states, represented as rays on the complex vector space* $\mathbb{C}^d$*, or equivalently, as rank-one projectors. With this choice, we have*

$$\mathsf{St}(S) = \left\{ |\psi\rangle\langle\psi| \ : \quad |\psi\rangle \in \mathbb{C}^d \,, \quad \langle\psi|\psi\rangle = 1 \right\}. \tag{2}$$

The physical transformations are represented by unitary channels, i.e., by maps of the form $|\psi\rangle\langle\psi| \mapsto U|\psi\rangle\langle\psi|U^\dagger$*, where* $U \in M_d(\mathbb{C})$ *is a unitary d-by-d matrix over the complex field. In short, we have*

$$\mathsf{Transf}(S) = \left\{ U \cdot U^\dagger \ : \quad U \in M_d(\mathbb{C}) \,, \quad U^\dagger U = U U^\dagger = I \right\}, \tag{3}$$

where I is the d-by-d identity matrix. The physical transformations form a monoid, with the composition operation induced by the matrix multiplication $(U \cdot U^\dagger) \circ (V \cdot V^\dagger) := (UV) \cdot (UV)^\dagger$*.*

Example 2 (Open quantum systems)**.** *Generally, a quantum system can be in a mixed state and can undergo an irreversible evolution. To account for this scenario, we must take the state space* $\mathsf{St}(S)$ *to be the set of all density matrices. For a system of dimension d, this means that the state space is*

$$\mathsf{St}(S) = \left\{ \rho \in M_d(\mathbb{C}) \ : \quad \rho \geq 0 \quad \mathrm{Tr}[\rho] = 1 \right\}, \tag{4}$$

where $\mathrm{Tr}[\rho] = \sum_{n=1}^{d} \langle n|\rho|n\rangle$ *denotes the matrix trace, and* $\rho \geq 0$ *means that the matrix* ρ *is positive semidefinite.* $\mathsf{Transf}(S)$ *is the set of all quantum channels [67], i.e., the set of all linear, completely positive, and trace-preserving maps from* $M_d(\mathbb{C})$ *to itself. The action of the quantum channel* $\mathcal{T}$ *on a generic state* ρ *can be specified through the Kraus representation [68]*

$$\mathcal{T}(\rho) = \sum_{i=1}^{r} T_i \rho T_i^\dagger \,, \tag{5}$$

where $\{T_i\}_{i=1}^r \subseteq M_d(\mathbb{C})$ *is a set of matrices satisfying the condition* $\sum_{i=1}^r T_i^\dagger T_i = I$*. The composition of two transformations* $\mathcal{T}$ *and S is given by the composition of the corresponding linear maps.*

Note that, at this stage, there is no notion of measurement in the framework. The sets $\mathsf{St}(S)$ and $\mathsf{Transf}(S)$ are meant as a model of system S irrespectively of anybody's ability to measure it, or even to operate on it. For this reason, we call this layer of the framework *pre-operational*. One can think of the pre-operational framework as the arena in which agents will act. Of course, the physical description of such an arena might have been suggested by experiments done earlier on by other agents, but this fact is inessential for the scope of our paper.

3.2. Agents

Let us introduce agents into the picture. In our framework, an agent A is identified a set of transformations, denoted as $\mathsf{Act}(A;S)$ and interpreted as the possible actions of A on S. Since the actions must be allowed physical processes, the inclusion $\mathsf{Act}(A;S) \subseteq \mathsf{Transf}(S)$ must hold. It is natural, but not strictly necessary, to assume that the concatenation of two actions is a valid action, and that the identity transformation is a valid action. When these assumptions are made, $\mathsf{Act}(A;S)$ is a monoid. Still, the construction presented in the following will hold not only for monoids, but also for generic sets $\mathsf{Act}(A;S)$. Hence, we adopt the following minimal definition:

Definition 1 (Agents)**.** *An agent A is identified by a subset* $\mathsf{Act}(A;S) \subseteq \mathsf{Transf}(S)$*.*

Note that this definition captures only one aspect of agency. Other aspects—such as the ability to gather information, make decisions, and interact with other agents—are important too, but not necessary for the scope of this paper.

We also stress that the interpretation of the subset $\mathsf{Act}(A;S) \subseteq \mathsf{Transf}(S)$ as the set of *actions of an agent* is not strictly necessary for the validity of our results. Nevertheless, the notion of "agent" here is useful because it helps explaining the rationale of our construction. The role of the agent is somehow similar to the role of a "probe charge" in classical electromagnetism. The probe charge need not exist in reality, but helps—as a conceptual tool—to give operational meaning to the magnitude and direction of the electric field.

In general, the set of actions available to agent A may be smaller than the set of all physical transformations on S. In addition, there may be other agents that act on system S independently of agent A. We define the independence of actions in the following way:

Definition 2. *Agents A and B* act independently *if the order in which they act is irrelevant, namely*

$$\mathcal{A} \circ \mathcal{B} = \mathcal{B} \circ \mathcal{A}\,, \qquad \forall \mathcal{A} \in \mathsf{Act}(A;S)\,, \mathcal{B} \in \mathsf{Act}(B;S)\,. \tag{6}$$

In a very primitive sense, the above relation expresses the fact that A and B act on "different degrees of freedom" of the system.

Remark 1 (Commutation of transformations vs. commutation of observables)**.** *Commutation conditions similar to Equation (6) are of fundamental importance in quantum field theory, where they are known under the names of "Einstein causality" [69] and "Microcausality" [70]. However, the similarity should not mislead the reader. The field theoretic conditions are expressed in terms of operator algebras. The condition is that the operators associated with independent systems commute. For example, a system localized in a certain region could be associated with the operator algebra* A*, and another system localized in another region could be associated with the operator algebra* B*. In this situation, the commutation condition reads*

$$CD = DC \qquad \forall C \in \mathsf{A}, \quad \forall D \in \mathsf{B}\,. \tag{7}$$

In contrast, Equation (6) is a condition on the transformations*, and not on the observables, which are not even described by our framework. In quantum theory, Equation (6) is a condition on the completely positive maps, and not to the elements of the algebras* A *and* B*. In Section 4, we will bridge the gap between our framework and the usual algebraic framework, focussing on the scenario where* A *and* B *are finite dimensional von Neumann algebras.*

3.3. Adversaries and Degradation

From the point of view of agent A, it is important to identify the degrees of freedom that no other agent B can affect. In an adversarial setting, agent B can be viewed as an adversary that tries to control as much of the system as possible.

Definition 3 (Adversary)**.** *Let A be an agent and let* $\mathsf{Act}(A;S)$ *be her set of operations. An* adversary *of A is an agent B that acts independently of A, i.e., an agent B whose set of actions satisfies*

$$\mathsf{Act}(B;S) \subseteq \mathsf{Act}(A;S)' := \Big\{ \mathcal{B} \in \mathsf{Transf}(S) \;:\quad \mathcal{B} \circ \mathcal{A} = \mathcal{A} \circ \mathcal{B}\,, \forall \mathcal{A} \in \mathsf{Act}(A;S) \Big\}\,. \tag{8}$$

Like the agent, the adversary is a conceptual tool, which will be used to illustrate our notion of subsystem. The adversary need not be a real physical entity, localized outside the agent's laboratory, and trying to counteract the agent's actions. Mathematically, the adversary is just a subset of the commutant of $\mathsf{Act}(A;S)$. The interpretation of B as an "adversary" is a way to "give life to to the mathematics", and to illustrate the rationale of our construction.

When B is interpreted as an adversary, we can think of his actions as a "degradation", which compromises states and transformations. We denote the degradation relation as $\succeq_B$, and write

$$\phi \succeq_B \psi \qquad \text{iff} \qquad \exists \mathcal{B} \in \mathsf{Act}(B;S) : \psi = \mathcal{B}\,\phi\,, \tag{9}$$

$$\mathcal{S} \succeq_B \mathcal{T} \qquad \text{iff} \qquad \exists \mathcal{B}_1, \mathcal{B}_2 \in \mathsf{Act}(B;S) : \mathcal{T} = \mathcal{B}_1 \circ \mathcal{S} \circ \mathcal{B}_2 \tag{10}$$

for $\phi, \psi \in \mathsf{St}(S)$ or $\mathcal{S}, \mathcal{T} \in \mathsf{Transf}(S)$.

The states that can be obtained by degrading ψ will be denoted as

$$\mathsf{Deg}_B(\psi) := \Big\{ \mathcal{B}\psi \; : \quad \mathcal{B} \in \mathsf{Act}(B;S) \Big\}\,. \tag{11}$$

The transformations that can be obtained by degrading $\mathcal{T}$ will be denoted as

$$\mathsf{Deg}_B(\mathcal{T}) := \Big\{ \mathcal{B}_1 \circ \mathcal{T} \circ \mathcal{B}_2 \; : \quad \mathcal{B}_1, \mathcal{B}_2 \in \mathsf{Act}(B;S) \Big\}. \tag{12}$$

The more operations B can perform, the more powerful B will be as an adversary. The most powerful adversary compatible with the independence condition (6) is the adversary that can implement all transformations in the commutant of $\mathsf{Act}(A;S)$:

Definition 4. *The* maximal adversary *of agent A is the agent A' that can perform the actions* $\mathsf{Act}\big(A';S\big) := \mathsf{Act}(A;S)'$.

Note that the actions of the maximal adversary are automatically a monoid, even if the set $\mathsf{Act}(A;S)$ is not. Indeed,

- the identity map $\mathcal{I}_S$ commutes with all operations in $\mathsf{Act}(A;S)$, and
- if $\mathcal{B}$ and $\mathcal{B}'$ commute with every operation in $\mathsf{Act}(A;S)$, then also their composition $\mathcal{B} \circ \mathcal{B}'$ will commute with all the operations in $\mathsf{Act}(A;S)$.

In the following, we will use the maximal adversary to define the subsystem associated with agent A.

3.4. The States of the Subsystem

Given an agent A, we think of the subsystem S_A to be the collection of all degrees of freedom that are unaffected by the action of the maximal adversary A'. Consistently with this intuitive picture, we partition the states of S into disjoint subsets, with the interpretation that two states are in the same subset if and only if they correspond to the same state of subsystem S_A.

We denote by Λ_ψ the subset of $\mathsf{St}(S)$ containing the state ψ. To construct the state space of the subsystem, we adopt the following rule:

Rule 1. *If the state ψ is obtained from the state ϕ through degradation, i.e., if $\psi \in \mathsf{Deg}_{A'}(\phi)$, then ψ and ϕ must correspond to the same state of subsystem S_A, i.e., one must have $\Lambda_\psi = \Lambda_\phi$.*

Rule 1 imposes that all states in the set $\mathsf{Deg}_{A'}(\psi)$ must be contained in the set Λ_ψ. Furthermore, we have the following fact:

Proposition 1. *If the sets $\mathsf{Deg}_{A'}(\phi)$ and $\mathsf{Deg}_{A'}(\psi)$ have non-trivial intersection, then $\Lambda_\phi = \Lambda_\psi$.*

Proof. By Rule 1, every element of $\mathsf{Deg}_{A'}(\phi)$ is contained in Λ_ϕ. Similarly, every element of $\mathsf{Deg}_{A'}(\psi)$ is contained in Λ_ψ. Hence, if $\mathsf{Deg}_{A'}(\phi)$ and $\mathsf{Deg}_{A'}(\psi)$ have non-trivial intersection, then also Λ_ϕ and Λ_ψ have non-trivial intersection. Since the sets Λ_ϕ and Λ_ψ belong to a disjoint partition, we conclude that $\Lambda_\phi = \Lambda_\psi$. □

Generalizing the above argument, it is clear that two states ϕ and ψ must be in the same subset $\Lambda_\phi = \Lambda_\psi$ if there exists a finite sequence $(\psi_1, \psi_2, \dots, \psi_n) \subseteq \mathsf{St}(S)$ such that

$$\psi_1 = \phi\,, \qquad \psi_n = \psi\,, \qquad \text{and} \qquad \mathsf{Deg}_{A'}(\psi_i) \cap \mathsf{Deg}_{A'}(\psi_{i+1}) \neq \emptyset \quad \forall i \in \{1, 2, \dots, n-1\}\,. \tag{13}$$

When this is the case, we write $\phi \simeq_A \psi$. Note that the relation $\phi \simeq_A \psi$ is an equivalence relation. When the relation $\phi \simeq_A \psi$ holds, we say that ϕ and ψ are *equivalent for agent* A. We denote the equivalence class of the state ψ by $[\psi]_A$.

By Rule 1, the whole equivalence class $[\psi]_A$ must be contained in the set Λ_ψ, meaning that all states in the equivalence class must correspond to the same state of subsystem S_A. Since we are not constrained by any other condition, we make the minimal choice

$$\Lambda_\psi := [\psi]_A\,. \tag{14}$$

In summary, the state space of system S_A is

$$\mathsf{St}(S_A) := \Big\{ [\psi]_A : \ \psi \in \mathsf{St}(S) \Big\}\,. \tag{15}$$

3.5. The Transformations of a Subsystem

The transformations of system S_A can also be constructed through equivalence classes. Before taking equivalence classes, however, we need a candidate set of transformations that can be interpreted as acting exclusively on subsystem S_A. The largest candidate set is the set of all transformations that commute with the actions of the maximal adversary A', namely

$$\mathsf{Act}(A'; S)' = \mathsf{Act}(A; S)''\,. \tag{16}$$

In general, $\mathsf{Act}(A; S)''$ could be larger than $\mathsf{Act}(A; S)$, in agreement with the fact the set of physical transformations of system S_A could be larger than the set of operations that agent A can perform. For example, agent A could have access only to noisy operations, while another, more technologically advanced agent could perform more accurate operations on the same subsystem.

For two transformations $\mathcal{S}$ and $\mathcal{T}$ in $\mathsf{Act}(A; S)''$, the degradation relation $\succeq_{A'}$ takes the simple form

$$\mathcal{S} \succeq_{A'} \mathcal{T} \qquad \text{iff} \qquad \mathcal{T} = \mathcal{B} \circ \mathcal{S} \quad \text{for some } \mathcal{B} \in \mathsf{Act}(A'; S)\,. \tag{17}$$

As we did for the set of states, we now partition the set $\mathsf{Act}(A; S)''$ into disjoint subsets, with the interpretation that two transformations act in the same way on the subsystem S_A if and only if they belong to the same subset.

Let us denote by $\Theta_{\mathcal{A}}$ the subset containing the transformation $\mathcal{A}$. To find the appropriate partition of $\mathsf{Act}(A; S)''$ into disjoint subsets, we adopt the following rule:

Rule 2. *If the transformation $\mathcal{T} \in \mathsf{Act}(A; S)''$ is obtained from the transformation $\mathcal{S} \in \mathsf{Act}(A; S)''$ through degradation, i.e., if $\mathcal{T} \in \mathsf{Deg}_{A'}(\mathcal{S})$, then $\mathcal{T}$ and $\mathcal{S}$ must act in the same way on the subsystem S_A, i.e., they must satisfy $\Theta_{\mathcal{T}} = \Theta_{\mathcal{S}}$.*

Intuitively, the motivation for the above rule is that system S_A is *defined* as the system that is not affected by the action of the adversary.

Rule 2 implies that all transformations in $\mathsf{Deg}_{A'}(\mathcal{T})$ must be contained in $\Theta_{\mathcal{T}}$. Moreover, we have the following:

Proposition 2. *If the sets $\mathsf{Deg}_{A'}(\mathcal{S})$ and $\mathsf{Deg}_{A'}(\mathcal{T})$ have non-trivial intersection, then $\Theta_{\mathcal{S}} = \Theta_{\mathcal{T}}$.*

Proof. By Rule 2, every element of $\mathsf{Deg}_{A'}(\mathcal{S})$ is contained in $\Theta_{\mathcal{S}}$. Similarly, every element of $\mathsf{Deg}_{A'}(\mathcal{T})$ is contained in $\Theta_{\mathcal{T}}$. Hence, if $\mathsf{Deg}_{A'}(\mathcal{S})$ and $\mathsf{Deg}_{A'}(\mathcal{T})$ have non-trivial intersection, then also $\Theta_{\mathcal{S}}$ and $\Theta_{\mathcal{T}}$ have non-trivial intersection. Since the sets $\Lambda_{\mathcal{S}}$ and $\Lambda_{\mathcal{T}}$ belong to a disjoint partition, we conclude that $\Lambda_{\mathcal{S}} = \Lambda_{\mathcal{T}}$. □

Using the above proposition, we obtain that the equality $\Theta_{\mathcal{T}} = \Theta_{\mathcal{S}}$ holds whenever there exists a finite sequence $(\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n) \subseteq \mathsf{Act}(A;S)''$ such that

$$\mathcal{A}_1 = \mathcal{S}\,, \qquad \mathcal{A}_n = \mathcal{T}\,, \qquad \text{and} \qquad \mathsf{Deg}_{A'}(\mathcal{A}_i) \cap \mathsf{Deg}_{A'}(\mathcal{A}_{i+1}) \neq \emptyset \quad \forall i \in \{1, 2, \dots, n-1\}\,. \tag{18}$$

When the above relation is satisfied, we write $\mathcal{S} \simeq_A \mathcal{T}$ and we say that $\mathcal{S}$ *and* $\mathcal{T}$ *are equivalent for agent* A. It is immediate to check that $\simeq_A$ is an equivalence relation. We denote the equivalence class of the transformation $\mathcal{T} \in \mathsf{Act}(A;S)''$ as $[\mathcal{T}]_A$.

By Rule 2, all the elements of $[\mathcal{T}]_A$ must be contained in the set $\Theta_{\mathcal{T}}$, i.e., they should correspond to the same transformation on S_A. Again, we make the minimal choice: we stipulate that the set $\Theta_{\mathcal{T}}$ coincides exactly with the equivalence class $[\mathcal{T}]_A$. Hence, the transformations of subsystem S_A are

$$\mathsf{Transf}(S_A) := \Big\{ [\mathcal{T}]_A : \ \mathcal{T} \in \mathsf{Act}(A;S)'' \Big\}\,. \tag{19}$$

The composition of two transformations $[\mathcal{T}_1]_A$ and $[\mathcal{T}_2]_A$ is defined in the obvious way, namely

$$[\mathcal{T}_1]_A \circ [\mathcal{T}_2]_A := [\mathcal{T}_1 \circ \mathcal{T}_2]_A\,. \tag{20}$$

Similarly, the action of the transformations on the states is defined as

$$[\mathcal{T}]_A\, [\psi]_A := [\mathcal{T}\, \psi]_A\,. \tag{21}$$

In Appendix A, we show that definitions (20) and (21) are well-posed, in the sense that their right-hand sides are independent of the choice of representatives within the equivalence classes.

Remark 1. *It is important not to confuse the transformation* $\mathcal{T} \in \mathsf{Act}(A;S)''$ *with the equivalence class* $[\mathcal{T}]_A$*: the former is a transformation* on the whole system S*, while the latter is a transformation only on subsystem* S_A*. To keep track of the distinction, we define the* restriction *of the transformation* $\mathcal{T} \in \mathsf{Act}(A;S)''$ *to the subsystem* S_A *via the map*

$$\pi_A(\mathcal{T}) := [\mathcal{T}]_A\,. \tag{22}$$

Proposition 3. *The restriction map* $\pi_A : \mathsf{Act}(A;S)'' \to \mathsf{Transf}(S_A)$ *is a monoid homomorphism, namely* $\pi_A(\mathcal{I}_S) = \mathcal{I}_{S_A}$ *and* $\pi_A(\mathcal{S} \circ \mathcal{T}) = \pi_A(\mathcal{S}) \circ \pi_A(\mathcal{T})$ *for every pair of transformations* $\mathcal{S}, \mathcal{T} \in \mathsf{Act}(A;S)''$.

Proof. Immediate from the definition (20). □

4. Examples of Agents, Adversaries, and Subsystems

In this section, we illustrate the construction of subsystems in five concrete examples.

4.1. Tensor Product of Two Quantum Systems

Let us start from the obvious example, which will serve as a sanity check for the soundness of our construction. Let S be a quantum system with Hilbert space $\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B$. The states of S are all the density operators on the Hilbert space $\mathcal{H}_S$. The space of all linear operators from $\mathcal{H}_S$ to itself will be denoted as $\mathsf{Lin}(\mathcal{H}_S)$, so that

$$\mathsf{St}(S) = \left\{ \rho \in \mathsf{Lin}(\mathcal{H}_S) \ : \quad \rho \geq 0, \quad \mathrm{Tr}[\rho] = 1 \right\}. \tag{23}$$

The transformations are all the quantum channels (linear, completely positive, and trace-preserving linear maps) from $\mathsf{Lin}(\mathcal{H}_S)$ to itself. We will denote the set of all channels on system S as $\mathsf{Chan}(S)$. Similarly, we will use the notation $\mathsf{Lin}(\mathcal{H}_A)$ [$\mathsf{Lin}(\mathcal{H}_B)$] for the spaces of linear operators from $\mathcal{H}_A$ [$\mathcal{H}_B$] to itself, and the notation $\mathsf{Chan}(A)$ [$\mathsf{Chan}(B)$] for the quantum channels from $\mathsf{Lin}(\mathcal{H}_A)$ [$\mathsf{Lin}(\mathcal{H}_B)$] to itself.

We can now define an agent A whose actions are all quantum channels acting locally on system A, namely

$$\mathsf{Act}(A;S) := \left\{ \mathcal{A} \otimes \mathcal{I}_B \ : \quad \mathcal{A} \in \mathsf{Chan}(A) \right\}, \tag{24}$$

where $\mathcal{I}_B$ denotes the identity map on $\mathsf{Lin}(\mathcal{H}_B)$. It is relatively easy to see that the commutant of $\mathsf{Act}(A;S)$ is

$$\mathsf{Act}(A;S)' = \left\{ \mathcal{I}_A \otimes \mathcal{B} \ : \quad \mathcal{B} \in \mathsf{Chan}(B) \right\} \tag{25}$$

(see Appendix B for the proof). Hence, the maximal adversary of agent A is the adversary $A' = B$ that has full control on the Hilbert space $\mathcal{H}_B$. Note also that one has $\mathsf{Act}(A;S)'' = \mathsf{Act}(A;S)$.

Now, the following fact holds:

Proposition 4. *Two states $\rho, \sigma \in \mathsf{St}(S)$ are equivalent for agent A if and only if $\mathrm{Tr}_B[\rho] = \mathrm{Tr}_B[\sigma]$, where Tr_B denotes the partial trace over the Hilbert space $\mathcal{H}_B$.*

Proof. Suppose that the equivalence $\rho \simeq_A \sigma$ holds. By definition, this means that there exists a finite sequence $(\rho_1, \rho_2, \dots, \rho_n)$ such that

$$\rho_1 = \rho\,, \qquad \rho_n = \sigma\,, \qquad \text{and} \qquad \mathsf{Deg}_B(\rho_i) \cap \mathsf{Deg}_B(\rho_{i+1}) \neq \emptyset \quad \forall i \in \{1, 2, \dots, n-1\}\,. \tag{26}$$

In turn, the condition of non-trivial intersection implies that, for every $i \in \{1, 2, \dots, n-1\}$, one has

$$(\mathcal{I}_A \otimes \mathcal{B}_i)(\rho_i) = (\mathcal{I}_A \otimes \widetilde{\mathcal{B}}_i)(\rho_{i+1})\,, \tag{27}$$

where $\mathcal{B}_i$ and $\widetilde{\mathcal{B}}_i$ are two quantum channels in $\mathsf{Chan}(B)$. Since $\mathcal{B}_i$ and $\widetilde{\mathcal{B}}_i$ are trace-preserving, Equation (27) implies $\mathrm{Tr}_B[\rho_i] = \mathrm{Tr}_B[\rho_{i+1}]$, as one can see by taking the partial trace on $\mathcal{H}_B$ on both sides. In conclusion, we obtained the equality $\mathrm{Tr}_B[\rho] \equiv \mathrm{Tr}_B[\rho_1] = \mathrm{Tr}_B[\rho_2] = \cdots = \mathrm{Tr}_B[\rho_n] \equiv \mathrm{Tr}_B[\sigma]$.

Conversely, suppose that the condition $\mathrm{Tr}_B[\rho] = \mathrm{Tr}_B[\sigma]$ holds. Then, one has

$$(\mathcal{I}_A \otimes \mathcal{B}_0)(\rho) = (\mathcal{I}_A \otimes \mathcal{B}_0)(\sigma)\,, \tag{28}$$

where $\mathcal{B}_0 \in \mathsf{Chan}(B)$ is the erasure channel defined as $\mathcal{B}_0(\cdot) = \beta_0\ \mathrm{Tr}_B[\cdot]$, β_0 being a fixed (but otherwise arbitrary) density matrix in $\mathsf{Lin}(\mathcal{H}_B)$. Since $\mathcal{I}_A \otimes \mathcal{B}_0$ is an element of $\mathsf{Act}(B;S)$, Equation (28) shows that the intersection between $\mathsf{Deg}_B(\rho)$ and $\mathsf{Deg}_B(\sigma)$ is non-empty. Hence, ρ and σ correspond to the same state of system S_A. □

We have seen that two global states $\rho, \sigma \in \mathsf{St}(S)$ are equivalent for agent A if and only if they have the same partial trace over B. Hence, the state space of the subsystem S_A is

$$\mathsf{St}(S_A) = \left\{ \mathrm{Tr}_B[\rho] \ : \qquad \rho \in \mathsf{St}(S) \right\}, \tag{29}$$

consistently with the standard prescription of quantum mechanics.

Now, let us consider the transformations. It is not hard to show that two transformations $\mathcal{T}, \mathcal{S} \in \mathsf{Act}(A;S)''$ are equivalent if and only if $\mathrm{Tr}_B \circ \mathcal{T} = \mathrm{Tr}_B \circ \mathcal{S}$ (see Appendix B for the details). Recalling that the transformations in $\mathsf{Act}(A;S)''$ are of the form $\mathcal{A} \otimes \mathcal{I}_B$, for some $\mathcal{A} \in \mathsf{Chan}(A)$, we obtain that the set of transformations of S_A is

$$\mathsf{Transf}(S_A) = \mathsf{Chan}(A)\,. \tag{30}$$

In summary, our construction correctly identifies the quantum subsystem associated with the Hilbert space $\mathcal{H}_A$, with the right set of states and the right set of physical transformations.

4.2. Subsystems Associated with Finite Dimensional Von Neumann algebras

In this example, we show that our notion of subsystem encompasses the traditional notion of subsystem based on an algebra of observables. For simplicity, we restrict our attention to a quantum system S with finite dimensional Hilbert space $\mathcal{H}_S \simeq \mathbb{C}^d$, $d < \infty$. With this choice, the state space $\mathsf{St}(S)$ is the set of all density matrices in $M_d(\mathbb{C})$ and the transformation monoid $\mathsf{Transf}(S)$ is the set of all quantum channels (linear, completely positive, trace-preserving maps) from $M_d(\mathbb{C})$ to itself.

We now define an agent A associated with a von Neumann algebra $\mathsf{A} \subseteq \mathsf{M_d}(\mathbb{C})$. In the finite dimensional setting, a von Neumann algebra is just a matrix algebra that contains the identity operator and is closed under the matrix adjoint. Every such algebra can be decomposed in a block diagonal form. Explicitly, one can decompose the Hilbert space $\mathcal{H}_S$ as

$$\mathcal{H}_S = \bigoplus_k \left(\mathcal{H}_{A_k} \otimes \mathcal{H}_{B_k}\right)\,, \tag{31}$$

for appropriate Hilbert spaces $\mathcal{H}_{A_k}$ and $\mathcal{H}_{B_k}$. Relative to this decomposition, the elements of the algebra A are characterized as

$$C \in \mathsf{A} \qquad \Longleftrightarrow \qquad C = \bigoplus_k \left(C_k \otimes I_{B_k}\right)\,, \tag{32}$$

where C_k is an operator in $\mathsf{Lin}(\mathcal{H}_{A_k})$, and I_{B_k} is the identity on $\mathcal{H}_{B_k}$. The elements of the commutant algebra A' are characterized as

$$D \in \mathsf{A}' \qquad \Longleftrightarrow \qquad D = \bigoplus_k \left(I_{A_k} \otimes D_k\right)\,, \tag{33}$$

where I_{A_k} is the identity on $\mathcal{H}_{A_k}$ and D_k is an operator in $\mathsf{Lin}(\mathcal{H}_{B_k})$.

We grant agent A the ability to implement all quantum channels with Kraus operators in the algebra A, i.e., all quantum channels in the set

$$\mathsf{Chan}(\mathsf{A}) := \left\{\mathcal{C} \in \mathsf{Chan}(S) \;:\quad \mathcal{C}(\cdot) = \sum_{i=1}^{r} C_i \cdot C_i^\dagger\,,\quad C_i \in \mathsf{A}\ \forall \mathsf{i} \in \{1,\dots,\mathsf{r}\}\right\}. \tag{34}$$

The maximal adversary of agent A is the agent B who can implement all the quantum channels that commute with the channels in $\mathsf{Chan}(\mathsf{A})$, namely

$$\mathsf{Act}(B;S) = \mathsf{Chan}(\mathsf{A})'\,. \tag{35}$$

In Appendix C, we prove that $\mathsf{Chan}(\mathsf{A})'$ coincides with the set of quantum channels with Kraus operators in the commutant of the algebra A: in formula,

$$\mathsf{Chan}(\mathsf{A})' = \mathsf{Chan}(\mathsf{A}')\,. \tag{36}$$

As in the previous example, the states of subsystem S_A can be characterized as "partial traces" of the states in S, provided that one adopts the right definition of "partial trace". Denoting the commutant of the algebra A by $\mathsf{B} := \mathsf{A}'$, one can define the "partial trace over the algebra B" as the channel $\mathrm{Tr}_{\mathsf{B}} : \mathsf{Lin}(\mathcal{H}_S) \to \bigoplus_k \mathsf{Lin}(\mathcal{H}_{A_k})$ specified by the relation

$$\mathrm{Tr}_{\mathsf{B}}(\rho) := \bigoplus_k \mathrm{Tr}_{B_k}\left[\Pi_k \rho \Pi_k\right], \tag{37}$$

where Π_k is the projector on the subspace $\mathcal{H}_{A_k} \otimes \mathcal{H}_{B_k} \subseteq \mathcal{H}_S$, and Tr_{B_k} denotes the partial trace over the space $\mathcal{H}_{B_k}$. With definition (37), is not hard to see that two states are equivalent for A if and only if they have the same partial trace over B:

Proposition 5. *Two states ρ, $\sigma \in \mathsf{St}(S)$ are equivalent for A if and only if $\mathrm{Tr}_{\mathsf{B}}[\rho] = \mathrm{Tr}_{\mathsf{B}}[\sigma]$.*

The proof is provided in Appendix C. In summary, the states of system $\mathsf{St}(S_A)$ are obtained from the states of S via partial trace over B, namely

$$\mathsf{St}(S_A) = \left\{ \mathrm{Tr}_{\mathsf{B}}(\rho) \ : \quad \rho \in \mathsf{St}(S) \right\}. \tag{38}$$

Our construction is consistent with the standard algebraic construction, where the states of system S_A are defined as restrictions of the global states to the subalgebra A: indeed, for every element $C \in \mathsf{A}$, we have the relation

$$\begin{aligned} \mathrm{Tr}[C\,\rho] &= \mathrm{Tr}\left[\left(\bigoplus_k C_k \otimes I_{B_k}\right)\rho\right] \\ &= \sum_k \mathrm{Tr}[(C_k \otimes I_{B_k})\,\Pi_k \rho \Pi_k] \\ &= \sum_k \mathrm{Tr}\left\{C_k\ \mathrm{Tr}_{B_k}[\Pi_k \rho \Pi_k]\right\} \\ &= \mathrm{Tr}\left\{\check{C}\,\mathrm{Tr}_{\mathsf{B}}[\rho]\right\}, \qquad \check{C} := \bigoplus_k C_k\,, \end{aligned} \tag{39}$$

meaning that the restriction of the state ρ to the subalgebra A is in one-to-one correspondence with the state $\mathrm{Tr}_{\mathsf{B}}[\rho]$.

Alternatively, the states of subsystem S_A can be characterized as density matrices of the block diagonal form

$$\sigma = \bigoplus_k p_k\,\sigma_k\,, \tag{40}$$

where (p_k) is a probability distribution, and each σ_k is a density matrix in $\mathsf{Lin}(\mathcal{H}_{A_k})$. In Appendix C, we characterize the transformations of the subsystem S_A as quantum channels $\mathcal{A}$ of the form

$$\mathcal{A} = \bigoplus_k \mathcal{A}_k\,, \tag{41}$$

where $\mathcal{A}_k : \mathsf{Lin}(\mathcal{H}_{A_k}) \to \mathsf{Lin}(\mathcal{H}_{A_k})$ is a linear, completely positive, and trace-preserving map. In summary, the subsystem S_A is a direct sum of quantum systems.

4.3. Coherent Superpositions vs. Incoherent Mixtures in Closed-System Quantum Theory

We now analyze an example involving only pure states and reversible transformations. Let S be a single quantum system with Hilbert space $\mathcal{H}_S = \mathbb{C}^d, d < \infty$, equipped with a distinguished orthonormal basis $\{|n\rangle\}_{n=1}^d$. As the state space, we consider the set of pure quantum states: in formula,

$$\mathsf{St}(S) = \Big\{ |\psi\rangle\langle\psi| \ : \quad |\psi\rangle \in \mathbb{C}^d \,, \quad \langle\psi|\psi\rangle = 1 \Big\} \,. \tag{42}$$

As the set of transformations, we consider the set of all unitary channels: in formula,

$$\mathsf{Transf}(S) = \Big\{ U \cdot U^\dagger \ : \quad U \in M_d(\mathbb{C}) \,, \quad U^\dagger U = U^\dagger U = I \Big\} \,. \tag{43}$$

To agent A, we grant the ability to implement all unitary channels corresponding to diagonal unitary matrices, i.e., matrices of the form

$$U_{\boldsymbol{\theta}} = \sum_k e^{i\theta_k} \, |k\rangle\langle k| \,, \qquad \boldsymbol{\theta} = (\theta_1, \dots, \theta_d) \in [0, 2\pi)^{\times d} \,, \tag{44}$$

where each phase θ_k can vary independently of the other phases. In formula, the set of actions of agent A is

$$\mathsf{Act}(A; S) = \Big\{ U_{\boldsymbol{\theta}} \cdot U_{\boldsymbol{\theta}}^\dagger \ : \quad U_{\boldsymbol{\theta}} \in \mathsf{Lin}(\mathcal{H}_S) \,, \quad U_{\boldsymbol{\theta}} \text{ as in Equation (44)} \Big\}. \tag{45}$$

The peculiarity of this example is that the actions of the maximal adversary A' are exactly the same as the actions of A. It is immediate to see that $\mathsf{Act}(A; S)$ is included in $\mathsf{Act}(A'; S)$ because all operations of agent A commute. With a bit of extra work, one can see that, in fact, $\mathsf{Act}(A; S)$ and $\mathsf{Act}(A'; S)$ coincide.

Let us look at the subsystem associated with agent A. The equivalence relation among states takes a simple form:

Proposition 6. *Two pure states with unit vectors $|\phi\rangle, |\psi\rangle \in \mathcal{H}_S$ are equivalent for A if and only if $|\psi\rangle = U|\phi\rangle$ for some diagonal unitary matrix U.*

Proof. Suppose that there exists a finite sequence $(|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle)$ such that

$$|\psi_1\rangle = |\phi\rangle \,, \quad |\psi_n\rangle = |\psi\rangle \,, \quad \text{and} \quad \mathsf{Deg}_{A'}(|\psi_i\rangle\langle\psi_i|) \cap \mathsf{Deg}_{A'}(|\psi_{i+1}\rangle\langle\psi_{i+1}|) \neq \emptyset \quad \forall i \in \{1, 2, \dots, n-1\} \,.$$

This means that, for every $i \in \{1, \dots, n-1\}$, there exist two diagonal unitary matrices U_i and $\widetilde{U}_i$ such that $U_i|\psi_i\rangle = \widetilde{U}_i|\psi_{i+1}\rangle$, or equivalently,

$$|\psi_{i+1}\rangle = \widetilde{U}_i^\dagger \, U_i |\psi_i\rangle \,. \tag{46}$$

Using the above relation for all values of i, we obtain $|\psi\rangle = U|\phi\rangle$ with $U := \widetilde{U}_{n-1}^\dagger \, U_{n-1} \cdots \widetilde{U}_2^\dagger \, U_2 \widetilde{U}_1^\dagger \, U_1$.

Conversely, suppose that the condition $|\psi\rangle = U|\phi\rangle$ holds for some diagonal unitary matrix U. Then, the intersection $\mathsf{Deg}_{A'}(|\phi\rangle\langle\phi|) \cap \mathsf{Deg}_{A'}(|\psi\rangle\langle\psi|)$ is non-empty, which implies that $|\phi\rangle\langle\phi|$ and $|\psi\rangle\langle\psi|$ are in the same equivalence class. □

Using Proposition 6, it is immediate to see that the equivalence class $[|\psi\rangle\langle\psi|]_{A'}$ is uniquely identified by the diagonal density matrix $\rho = \sum_k |\psi_k|^2 |k\rangle\langle k|$. Hence, the state space of system S_A is the set of diagonal density matrices

$$\mathsf{St}(S_A) = \left\{\rho = \sum_k p_k |k\rangle\langle k| \; : \quad p_k \geq 0 \; \forall k \,, \quad \sum_k p_k = 1\right\}. \tag{47}$$

The set of transformations of system S_A is trivial because the actions of A coincide with the actions of the adversary A', and therefore they are all in the equivalence class of the identity transformation. In formula, one has

$$\mathsf{Transf}(S_A) = \left\{\mathcal{I}_{S_A}\right\}. \tag{48}$$

4.4. Classical Subsystems in Open-System Quantum Theory

This example is of the same flavour as the previous one but is more elaborate and more interesting. Again, we consider a quantum system S with Hilbert space $\mathcal{H} = \mathbb{C}^d$. Now, we take $\mathsf{St}(S)$ to be the whole set of density matrices in $M_d(\mathbb{C})$ and $\mathsf{Transf}(S)$ to be the whole set of quantum channels from $M_d(\mathbb{C})$ to itself.

We grant to agent A the ability to perform every multiphase covariant channel, that is, every quantum channel $\mathcal{M}$ satisfying the condition

$$\mathcal{U}_{\boldsymbol{\theta}} \circ \mathcal{M} = \mathcal{M} \circ \mathcal{U}_{\boldsymbol{\theta}} \qquad \forall \boldsymbol{\theta} = (\theta_1, \theta_2, \dots, \theta_d) \in [0, 2\pi)^{\times d} \,, \tag{49}$$

where $\mathcal{U}_{\boldsymbol{\theta}} = U_{\boldsymbol{\theta}} \cdot U_{\boldsymbol{\theta}}^\dagger$ is the unitary channel corresponding to the diagonal unitary $U_{\boldsymbol{\theta}} = \sum_k e^{i\theta_k} |k\rangle\langle k|$. Physically, we can interpret the restriction to multiphase covariant channels as the lack of a reference for the definition of the phases in the basis $\{|k\rangle \,, k = 1, \dots, d\}$.

It turns out that the maximal adversary of agent A is the agent A' that can perform every *basis-preserving channel* $\mathcal{B}$, that is, every channel satisfying the condition

$$\mathcal{B}(|k\rangle\langle k|) = |k\rangle\langle k| \qquad \forall k \in \{1, \dots, d\} \,. \tag{50}$$

Indeed, we have the following:

Theorem 1. *The monoid of multiphase covariant channels and the monoid of basis-preserving channels are the commutant of one another.*

The proof, presented in Appendix D.1, is based on the characterization of the basis-preserving channels provided in [71,72].

We now show that states of system S_A can be characterized as classical probability distributions.

Proposition 7. *For every pair of states $\rho, \sigma \in \mathsf{St}(S)$, the following are equivalent:*

1. *ρ and σ are equivalent for agent A,*
2. *$\mathcal{D}(\rho) = \mathcal{D}(\sigma)$, where $\mathcal{D}$ is the completely dephasing channel $\mathcal{D}(\cdot) := \sum_k |k\rangle\langle k| \cdot |k\rangle\langle k|$.*

Proof. Suppose that Condition 1 holds, meaning that there exists a sequence $(\rho_1, \rho_2, \dots, \rho_n)$ such that

$$\rho_1 = \rho \,, \qquad \rho_n = \sigma \,, \qquad \forall i \in \{1, \dots, n-1\} \; \exists \mathcal{B}_i \,, \widetilde{\mathcal{B}}_i \in \mathsf{Act}(B; S) : \; \mathcal{B}_i(\rho_i) = \widetilde{\mathcal{B}}_i(\rho_{i+1}) \,, \tag{51}$$

where $\mathcal{B}_i$ and $\widetilde{\mathcal{B}}_i$ are basis-preserving channels. The above equation implies

$$\langle k|\mathcal{B}_i(\rho_i)|k\rangle = \langle k|\widetilde{\mathcal{B}}_i(\rho_{i+1})|k\rangle \,. \tag{52}$$

Now, the relation $\langle k|\mathcal{B}(\rho)|k\rangle = \langle k|\rho|k\rangle$ is valid for every basis-preserving channel $\mathcal{B}$ and for every state ρ [71]. Applying this relation on both sides of Equation (52), we obtain the condition

$$\langle k|\rho_i|k\rangle = \langle k|\rho_{i+1}|k\rangle\,, \tag{53}$$

valid for every $k \in \{1,\dots,d\}$. Hence, all the density matrices $(\rho_1,\rho_2,\dots,\rho_n)$ must have the same diagonal entries, and, in particular, Condition 2 must hold.

Conversely, suppose that Condition 2 holds. Since the dephasing channel $\mathcal{D}$ is obviously basis-preserving, we obtained the condition $\mathsf{Deg}_{A'}(\rho) \cap \mathsf{Deg}_{A'}(\sigma) \neq \emptyset$, which implies that ρ and σ are equivalent for agent A. In conclusion, Condition 1 holds. □

Proposition 7 guarantees that the states of system S_A is in one-to-one correspondence with diagonal density matrices, and therefore, with classical probability distributions: in formula,

$$\mathsf{St}(S_A) = \left\{ (p_k)_{k=1}^d \;:\quad p_k \geq 0\ \forall k\,,\quad \sum_k p_k = 1 \right\}. \tag{54}$$

The transformations of system S_A can be characterized as *transition matrices*, namely

$$\mathsf{Transf}(S_A) = \left\{ [P_{jk}]_{j\leq d, k\leq d} \;:\quad P_{jk} \geq 0\ \forall j,k \in \{1,\dots,d\}\,,\ \sum_j P_{jk} = 1\ \forall k \in \{1,\dots,d\} \right\}. \tag{55}$$

The proof of Equation (55) is provided in Appendix D.2.

In summary, agent A has control on a classical system, whose states are probability distributions, and whose transformations are classical transition matrices.

4.5. Classical Systems From Free Operations in the Resource Theory of Coherence

In the previous example, we have seen that classical systems arise from agents who have access to the monoid of multiphase covariant channels. In fact, classical systems can arise in many other ways, corresponding to agents who have access to different monoids of operations. In particular, we find that several types of free operations in the resource theory of coherence [34–41] identify classical systems. Specifically, consider the monoids of

1. *Strictly incoherent operations* [41], i.e., quantum channels $\mathcal{T}$ with the property that, for every Kraus operator T_i, the map $\mathcal{T}_i(\cdot) = T_i \cdot T_i$ satisfies the condition $\mathcal{D}\circ\mathcal{T}_i = \mathcal{T}_i \circ \mathcal{D}$, where $\mathcal{D}$ is the completely dephasing channel.
2. *Dephasing covariant operations* [38–40], i.e., quantum channels $\mathcal{T}$ satisfying the condition $\mathcal{D}\circ\mathcal{T} = \mathcal{T}\circ\mathcal{D}$.
3. *Phase covariant channels [40]*, i.e., quantum channels $\mathcal{T}$ satisfying the condition $\mathcal{T}\circ\mathcal{U}_\varphi = \mathcal{U}_\varphi \circ \mathcal{T}$, $\forall \varphi \in [0,2\pi)$, where $\mathcal{U}_\varphi$ is the unitary channel associated with the unitary matrix $U_\varphi = \sum_k e^{ik\varphi}\,|k\rangle\langle k|$.
4. *Physically incoherent operations* [38,39], i.e., quantum channels that are convex combinations of channels $\mathcal{T}$ admitting a Kraus representation where each Kraus operator T_i is of the form

$$T_i = U_{\pi_i}\, U_{\boldsymbol{\theta}_i}\, P_i\,, \tag{56}$$

where U_{π_i} is a unitary that permutes the elements of the computational basis, $U_{\boldsymbol{\theta}_i}$ is a diagonal unitary, and P_i is a projector on a subspace spanned by a subset of vectors in the computational basis.

For each of the monoids 1–4, our construction yields the classical subsystem consisting of diagonal density matrices. The transformations of the subsystem are just the classical channels. The proof is presented in Appendix E.1.

Notably, other choices of free operations, such as the *maximally incoherent operations [34]* and the *incoherent operations* [35], do *not* identify classical subsystems. The maximally incoherent operations

are the quantum channels $\mathcal{T}$ that map diagonal density matrices to diagonal density matrices, namely $\mathcal{T} \circ \mathcal{D} = \mathcal{D} \circ \mathcal{T} \circ \mathcal{D}$, where $\mathcal{D}$ is the completely dephasing channel. The incoherent operations are the quantum channels $\mathcal{T}$ with the property that, for every Kraus operator T_i, the map $\mathcal{T}_i(\cdot) = T_i \cdot T_i$ sends diagonal matrices to diagonal matrices, namely $\mathcal{T}_i \circ \mathcal{D} = \mathcal{D} \circ \mathcal{T}_i \circ \mathcal{D}$.

In Appendix E.2, we show that incoherent and maximally incoherent operations do not identify classical subsystems: the subsystem associated with these operations is the whole quantum system. This result can be understood from the analogy between these operations and non-entangling operations in the resource theory of entanglement [38,39]. Non-entangling operations do not generate entanglement, but nevertheless they cannot (in general) be implemented with local operations and classical communication. Similarly, incoherent and maximally incoherent operations do not generate coherence, but they cannot (in general) be implemented with incoherent states and coherence non-generating unitary gates. An agent that performs these operations must have access to more degrees of freedom than just a classical subsystem.

At the mathematical level, the problem is that the incoherent and maximally incoherent operations do not necessarily commute with the dephasing channel $\mathcal{D}$. In our construction, commutation with the dephasing channel is essential for retrieving classical subsystems. In general, we have the following theorem:

Theorem 2. *Every set of operations that*

1. *contains the set of classical channels, and*
2. *commutes with the dephasing channel*

identifies a d-dimensional classical subsystem of the original d-dimensional quantum system.

The proof is provided in Appendix E.1.

5. Key Structures: Partial Trace and No Signalling

In this section, we go back to the general construction of subsystems, and we analyse the main structures arising from it. First, we observe that the definition of subsystem guarantees *by fiat* the validity of the no-signalling principle, stating that operations performed on one subsystem cannot affect the state of an independent subsystem. Then, we show that our construction of subsystems allows one to build a category.

5.1. The Partial Trace and the No Signalling Property

We defined the states of system S_A as equivalence classes. In more physical terms, we can regard the map $\psi \mapsto [\psi]_A$ as an operation of discarding, which takes system S and throws away the degrees of freedom reachable by the maximal adversary A'. In our adversarial picture, "throwing away some degrees of freedom" means leaving them under the control of the adversary, and considering only the part of the system that remains under the control of the agent.

Definition 5. *The* partial trace over A' *is the function* $\mathrm{Tr}_{A'} : \mathsf{St}(S) \to \mathsf{St}(S_A)$, *defined by* $\mathrm{Tr}_{A'}(\psi) = [\psi]_A$ *for a generic* $\psi \in \mathsf{St}(S)$.

The reason for the notation $\mathrm{Tr}_{A'}$ is that in quantum theory the operation $\mathrm{Tr}_{A'}$ coincides with the partial trace of matrices, as shown in the example of Section 4.1. For subsystems associated with von Neumann algebras, the partial trace is the "partial trace over the algebra" defined in Section 4.2. For subsystems associated with multiphase covariant channels or dephasing covariant operations, the partial trace is the completely dephasing channel, which "traces out" the off-diagonal elements of the density matrix.

With the partial trace notation, the states of system S_A can be succinctly written as

$$\mathsf{St}(S_A) = \left\{ \rho = \mathrm{Tr}_{A'}(\psi) \ : \quad \psi \in \mathsf{St}(S) \right\}. \tag{57}$$

Denoting $B := A'$, we have the important relation

$$\mathrm{Tr}_B \circ \mathcal{B} = \mathrm{Tr}_B \qquad \forall \mathcal{B} \in \mathsf{Act}(B; S)\,. \tag{58}$$

Equation (58) can be regarded as the *no signalling property*: the actions of agent B cannot lead to any change on the system of agent A. Of course, here the no signalling property holds *by fiat*, precisely because of the way the subsystems are defined!

The construction of subsystems has the merit to clarify the status of the no-signalling principle. No-signalling is often associated with space-like separation, and is heuristically justified through the idea that physical influences should propagate within the light cones. However, locality is only *a sufficient condition* for the no signalling property. Spatial separation implies no signalling, but the converse is not necessarily true: every pair of distinct quantum systems satisfies the no-signalling condition, even if the two systems are spatially contiguous. In fact, the no-signalling condition holds even for virtual subsystems of a *single*, spatially localized system. Think for example of a quantum particle localized in the xy plane. The particle can be regarded as a composite system, made of two virtual subsystems: a particle localized on the x-axis, and another particle localized on the y-axis. The no-signalling property holds for these two subsystems, even if they are not separated in space. As Equation (58) suggests, the validity of the no-signalling property has more to do with the way subsystems are constructed, rather than the way the subsystems are distributed in space.

5.2. A Baby Category

Our construction of subsystems defines a category, consisting of three objects, S, S_A, and S_B, where S_B is the subsystem associated with the agent $B = A'$. The sets $\mathsf{Transf}(S)$, $\mathsf{Transf}(S_A)$, and $\mathsf{Transf}(S_B)$ are the endomorphisms from S to S, S_A to S_A, and S_B to S_B, respectively. The morphisms from S to S_A and from S to S_B are defined as

$$\mathsf{Transf}(S \to S_A) = \left\{ \mathrm{Tr}_B \circ \mathcal{T} \ : \quad \mathcal{T} \in \mathsf{Transf}(S) \right\} \tag{59}$$

and

$$\mathsf{Transf}(S \to S_B) = \left\{ \mathrm{Tr}_A \circ \mathcal{T} \ : \quad \mathcal{T} \in \mathsf{Transf}(S) \right\}, \tag{60}$$

respectively.

Morphisms from S_A to S, from S_B to S, from S_A to S_B, or from S_B to S_A, are not naturally defined. In Appendix F, we provide a mathematical construction that enlarges the sets of transformations, making all sets non-empty. Such a construction allows us to reproduce a categorical structure known as a *splitting of idempotents* [73,74]

6. Non-Overlapping Agents, Causality, and the Initialization Requirement

In the previous sections, we developed a general framework, applicable to arbitrary physical systems. In this section, we identify some desirable properties that the global systems may enjoy.

6.1. Dual Pairs of Agents

So far, we have taken the perspective of agent A. Let us now take the perspective of the maximal adversary A'. We consider A' as the agent, and denote his maximal adversary as A''. By definition, A'' can perform every action in the commutant of $\mathsf{Act}(A'; S)$, namely

$$\mathsf{Act}(A'';S) = \mathsf{Act}(A';S)' = \mathsf{Act}(A;S)''. \tag{61}$$

Obviously, the set of actions allowed to agent A'' includes the set of actions allowed to agent A. At this point, one could continue the construction and consider the maximal adversary of agent A''. However, no new agent would appear at this point: the maximal adversary of agent A'' is agent A' again. When two agents have this property, we call them a *dual pair:*

Definition 6. *Two agents A and B form a dual pair iff* $\mathsf{Act}(A;S) = \mathsf{Act}(B;S)'$ *and* $\mathsf{Act}(B;S) = \mathsf{Act}(A;S)'$.

All the examples in Section 4 are examples of dual pairs of agents.

It is easy to see that an agent A is part of a dual pair if and only if the set $\mathsf{Act}(A;S)$ coincides with its double commutant $\mathsf{Act}(A;S)''$.

6.2. Non-Overlapping Agents

Suppose that agents A and B form a dual pair. In general, the actions in $\mathsf{Act}(A;S)$ may have a non-trivial intersection with the actions in $\mathsf{Act}(B;S)$. This situation does indeed happen, as we have seen in Sections 4.3 and 4.4. Still, it is important to examine the special case where the actions of A and B have only trivial intersection, corresponding to the identity action $\mathcal{I}_S$. When this is the case, we say that the agents A and B are *non-overlapping:*

Definition 7. *Two agents A and B are non-overlapping iff* $\mathsf{Act}(A;S) \cap \mathsf{Act}(B;S) \subseteq \{\mathcal{I}_S\}$.

Dual pairs of non-overlapping agents are characterized by the fact that the sets of actions have trivial center:

Proposition 8. *Let A and B be a dual pair of agents. Then, the following are equivalent:*

1. *A and B are non-overlapping,*
2. *$\mathsf{Act}(A;S)$ has trivial center,*
3. *$\mathsf{Act}(B;S)$ has trivial center.*

Proof. Since agents A and B are dual to each other, we have $\mathsf{Act}(B;S) = \mathsf{Act}(A;S)'$ and $\mathsf{Act}(A;S) = \mathsf{Act}(B;S)'$. Hence, the intersection $\mathsf{Act}(A;S) \cap \mathsf{Act}(B;S)$ coincides with the center of $\mathsf{Act}(A;S)$, and with the center of $\mathsf{Act}(B;S)$. The non-overlap condition holds if and only if the center is trivial. □

Note that the existence of non-overlapping dual pairs is a condition on the transformations of the whole system S:

Proposition 9. *The following are equivalent:*

1. *system S admits a dual pair of non-overlapping agents,*
2. *the monoid $\mathsf{Transf}(S)$ has trivial center.*

Proof. Assume that Condition 1 holds for a pair of agents A and B. Let $\mathsf{C}(S)$ be the center of $\mathsf{Transf}(S)$. By definition, $\mathsf{C}(S)$ is contained into $\mathsf{Act}(B;S)$ because $\mathsf{Act}(B;S)$ contains all the transformations that commute with those in $\mathsf{Act}(A;S)$. Moreover, the elements of $\mathsf{C}(S)$ commute with all elements of $\mathsf{Act}(B;S)$, and therefore they are in the center of $\mathsf{Act}(B;S)$. Since A and B are a non-overlapping dual pair, the center of $\mathsf{Act}(B;S)$ must be trivial (Proposition 8), and therefore $\mathsf{C}(S)$ must be trivial. Hence, Condition 2 holds.

Conversely, suppose that Condition 2 holds. In that case, it is enough to take A to be the *maximal agent*, i.e., the agent $A_{\max}$ with $\mathsf{Act}\,(A_{\max};S) = \mathsf{Transf}(S)$. Then, the maximal adversary of $A_{\max}$ is the agent $B = A'_{\max}$ with $\mathsf{Act}(B;S) = \mathsf{Act}\,(A_{\max};S)' = \mathsf{C}(S) = \{\mathcal{I}_S\}$. By definition, the two agents form a non-overlapping dual pair. Hence, Condition 1 holds. □

The existence of dual pairs of non-overlapping agents is a desirable property, which may be used to characterize "good systems":

Definition 8 (Non-Overlapping Agents)**.** *We say that system S satisfies the* Non-Overlapping Agents Requirement *if there exists at least one dual pair of non-overlapping agents acting on S.*

The Non-Overlapping Agents Requirement guarantees that the total system S can be regarded as a subsystem: if $A_{\max}$ is the *maximal agent* (i.e., the agent who has access to all transformations on S), then the subsystem $S_{A_{\max}}$ is the whole system S. A more formal statement of this fact is provided in Appendix G.

6.3. Causality

The Non-Overlapping Agents Requirement guarantees that the subsystem associated with a maximal agent (i.e., an agent who has access to all possible transformations) is the whole system S. On the other hand, it is natural to expect that a minimal agent, who has no access to any transformation, should be associated with the trivial system, i.e., the system with a single state and a single transformation. The fact that the minimal agent is associated with the trivial system is important because it equivalent to a property of causality [8,13,75,76]: indeed, we have the following

Proposition 10. *Let $A_{\min}$ be the minimal agent and let $A_{\max}$ be its maximal adversary, coinciding with the maximal agent. Then, the following conditions are equivalent*

1. *$S_{A_{\min}}$ is the trivial system,*
2. *one has $\mathrm{Tr}_{A_{\max}}[\rho] = \mathrm{Tr}_{A_{\max}}[\sigma]$ for every pair of states $\rho, \sigma \in \mathsf{St}(S)$.*

Proof. $1 \Rightarrow 2$: By definition, the state space of $S_{A_{\min}}$ consists of states of the form $\mathrm{Tr}_{A_{\max}}[\rho]$, $\rho \in \mathsf{St}(S)$. Hence, the state space contains only one state if and only if Condition 2 holds. $2 \Rightarrow 1$: Condition 2 implies that every two states of system S are equivalent for agent $A_{\max}$. The fact that $S_{A_{\min}}$ has only one transformation is true by definition: since the adversary of $A_{\min}$ is the maximal agent, one has $\mathcal{T} \in \mathsf{Deg}_{A_{\max}}(\mathcal{I}_S)$ for every transformation $\mathcal{T} \in \mathsf{Transf}(S)$. Hence, every transformation is in the equivalence class of the identity. □

With a little abuse of notation, we may denote the trace over $A_{\max}$ as Tr_S because $A_{\max}$ has access to all transformations on system S. With this notation, the causality condition reads

$$\mathrm{Tr}_S[\rho] = \mathrm{Tr}_S[\sigma] \qquad \forall \rho, \sigma \in \mathsf{St}(S)\,. \tag{62}$$

It is interesting to note that, unlike no signalling, causality does not necessarily hold in the framework of this paper. This is because the trace Tr_S is defined as the quotient with respect to all possible transformations, and having a single equivalence class is a non-trivial property. One possibility is to demand the validity of this property, and to call a system *proper*, only if it satisfies the causality condition (62). In the following subsection, we will see a requirement that guarantees the validity of the causality condition.

6.4. The Initialization Requirement

The ability to prepare states from a fixed initial state is important in the circuit model of quantum computation, where qubits are initialized to the state $|0\rangle$, and more general states are generated by applying quantum gates. More broadly, the ability to initialize the system in a given state and to generate other states from it is important for applications in quantum control and adiabatic quantum computing. Motivated by these considerations, we formulate the following definition:

Definition 9. *A system S satisfies the* Initialization Requirement *if there exists a state $\psi_0 \in \mathsf{St}(S)$ from which any other state can be generated, meaning that, for every other state $\psi \in \mathsf{St}(S)$, there exists a transformation $\mathcal{T} \in \mathsf{Transf}(S)$ such that $\psi = \mathcal{T}\psi_0$. When this is the case, the state ψ_0 is called* cyclic.

The Initialization Requirement is satisfied in quantum theory, both at the pure state level and at the mixed state level. At the pure state level, every unit vector $|\psi\rangle \in \mathcal{H}_S$ can be generated from a fixed unit vector $|\psi_0\rangle \in \mathcal{H}_S$ via a unitary transformation U. At the mixed state level, every density matrix ρ can be generated from a fixed density matrix ρ_0 via the erasure channel $\mathcal{C}_\rho(\cdot) = \rho\ \mathrm{Tr}[\cdot]$. By the same argument, the initialization requirement is also satisfied when S is a system in an operational-probabilistic theory [8,10–13] and when S is a system in a causal process theory [75,76].

The Initialization Requirement guarantees that minimal agents are associated with trivial systems:

Proposition 11. *Let S be a system satisfying the Initialization Requirement, and let $A_{\min}$ be the* minimal agent, *i.e., the agent that can only perform the identity transformation. Then, the subsystem $S_{A_{\min}}$ is trivial: $\mathsf{St}\left(S_{A_{\min}}\right)$ contains only one state and $\mathsf{Transf}\left(S_{A_{\min}}\right)$ contains only one transformation.*

Proof. By definition, the maximal adversary of $A_{\min}$ is the maximal agent $A_{\max}$, who has access to all physical transformations. Then, every transformation is in the equivalence class of the identity transformation, meaning that system $S_{A_{\min}}$ has a single transformation. Now, let ψ_0 be the cyclic state. By the Initialization Requirement, the set $\mathsf{Deg}_{A_{\max}}(\psi_0)$ is the whole state space $\mathsf{St}(S)$. Hence, every state is equivalent to the state ψ_0. In other words, $\mathsf{St}\left(S_{A_{\min}}\right)$ contains only one state. □

The Initialization Requirement guarantees the validity of causality, thanks to Proposition 10. In addition, the Initialization Requirement is important independently of the causality property. For example, we will use it to formulate an abstract notion of *closed system*.

7. The Conservation of Information

In this section, we consider systems where all transformations are *invertible*. In such systems, every transformation can be thought as the result of some deterministic dynamical law. The different transformations in $\mathsf{Transf}(S)$ can be interpreted as different dynamics, associated with different values of physical parameters, such as coupling constants or external control parameters.

7.1. Logically Invertible vs. Physically Invertible

Definition 10. *A transformation $\mathcal{T} \in \mathsf{Transf}(S)$ is* logically invertible *iff the map*

$$\widehat{\mathcal{T}}: \quad \mathsf{St}(S) \to \mathsf{St}(S), \quad \psi \mapsto \mathcal{T}\psi \tag{63}$$

is injective.

Logically invertible transformations can be interpreted as evolutions of the system that preserve the distictness of states. At the fundamental level, one may require that all physical evolutions be logically invertible, a requirement that is sometimes called the *Conservation of Information* [58]. In the following, we will explore the consequences of such requirement:

Definition 11 (Logical Conservation of Information)**.** *System S satisfies the Logical Conservation of Information if all transformations in $\mathsf{Transf}(S)$ are logically invertible.*

The requirement is well-posed because the invertible transformations form a monoid. Indeed, the identity transformation is logically invertible, and that the composition of two logically invertible transformations is logically invertible.

A special case of logical invertibility is physical invertibility, defined as follows:

Definition 12. *A transformation* $\mathcal{T} \in \mathsf{Transf}(S)$ *is* physically invertible *iff there exists another transformation* $\mathcal{T}' \in \mathsf{Transf}(S)$ *such that* $\mathcal{T}' \circ \mathcal{T} = \mathcal{I}_S$.

Physical invertibility is more than injectivity: not only should the map $\mathcal{T}$ be injective on the state space, but also its inverse should be a physical transformation. In light of this observation, we state a stronger version of the Conservation of Information, requiring physical invertibility:

Definition 13 (Physical Conservation of Information)**.** *System S satisfies the Physical Conservation of Information if all transformations in* $\mathsf{Transf}(S)$ *are physically invertible.*

The difference between Logical and Physical Conservation of Information is highlighted by the following example:

Example 3 (Conservation of Information in closed-system quantum theory)**.** *Let S be a closed quantum system described by a separable, infinite-dimensional Hilbert space* $\mathcal{H}_S$*, and let* $\mathsf{St}(S)$ *be the set of pure states, represented as rank-one density matrices*

$$\mathsf{St}(S) = \Big\{ |\psi\rangle\langle\psi| \;:\quad |\psi\rangle \in \mathcal{H}_S\,, \quad \langle\psi|\psi\rangle = 1 \Big\}\,. \tag{64}$$

One possible choice of transformations is the monoid of isometric channels

$$\mathsf{Transf}(S) = \Big\{ V \cdot V^\dagger \;:\quad V \in \mathsf{Lin}(S)\,, \quad V^\dagger V = I \Big\}\,. \tag{65}$$

This choice of transformations satisfies the Logical Conservation of Information, but violates the Physical Conservation of Information because in general the map $V^\dagger \cdot V$ *fails to be trace-preserving, and therefore fails to be an isometric channel. For example, consider the shift operator*

$$V = \sum_{n=0}^{\infty} |n+1\rangle\langle n|\,. \tag{66}$$

The operator V is an isometry but its left-inverse $V^\dagger$ *is not an isometry. As a result, the channel* $V^\dagger \cdot V$ *is not an allowed physical transformation according to Equation (65).*

An alternative choice of physical transformations is the set of unitary channels

$$\mathsf{Transf}(S) = \Big\{ V \cdot V^\dagger \;:\quad V \in \mathsf{Lin}(S)\,, \quad V^\dagger V = V V^\dagger = I \Big\}\,. \tag{67}$$

With this choice, the Physical Conservation of Information is satisfied: every physical transformation is invertible and the inverse is a physical transformation.

7.2. Systems Satisfying the Physical Conservation of Information

In a system satisfying the Physical Conservation of Information, the transformations are not only physically invertible, but also physically *reversible*, in the following sense:

Definition 14. *A transformation* $\mathcal{T} \in \mathsf{Transf}(S)$ *is* physically reversible *iff there exists another transformation* $\mathcal{T}' \in \mathsf{Transf}(S)$ *such that* $\mathcal{T}' \circ \mathcal{T} = \mathcal{T} \circ \mathcal{T}' = \mathcal{I}_S$.

With the above definition, we have the following:

Proposition 12. *If system S satisfies the Physical Conservation of Information, then every physical transformation is physically reversible. The monoid* $\mathsf{Transf}(S)$ *is a group, hereafer denoted as* $\mathsf{G}(S)$.

Proof. Since $\mathcal{T}$ is physically invertible, there exists a transformation $\mathcal{T}'$ such that $\mathcal{T}' \circ \mathcal{T} = \mathcal{I}_S$. Since the Physical Conservation of Information holds, $\mathcal{T}'$ must be physically invertible, meaning that there exists a transformation $\mathcal{T}''$ such that $\mathcal{T}'' \circ \mathcal{T}' = \mathcal{I}_S$. Hence, we have

$$\mathcal{T}'' = \mathcal{T}'' \circ (\mathcal{T}' \circ \mathcal{T}) = (\mathcal{T}'' \circ \mathcal{T}') \circ \mathcal{T} = \mathcal{T} . \tag{68}$$

Since $\mathcal{T}'' = \mathcal{T}$, the invertibility condition $\mathcal{T}'' \circ \mathcal{T}' = \mathcal{I}_S$ becomes $\mathcal{T} \circ \mathcal{T}' = \mathcal{I}_S$. Hence, $\mathcal{T}$ is reversible and $\mathsf{Transf}(S)$ is a group. □

7.3. Subsystems of Systems Satisfying the Physical Conservation of Information

Imagine that an agent A acts on a system S satisfying the Physical Conservation of Information. We assume that the actions of agent A form a subgroup of $\mathsf{G}(S)$, denoted as G_A. The maximal adversary of A is the adversary $B = A'$, who has access to all transformations in the set

$$\mathsf{G}_B := \mathsf{G}'_A = \left\{ \mathcal{U}_B \in \mathsf{G}(S) \ : \quad \mathcal{U}_B \circ \mathcal{U}_A = \mathcal{U}_A \circ \mathcal{U}_B \, , \quad \forall \mathcal{U}_A \in \mathsf{G}(A) \right\} . \tag{69}$$

It is immediate to see that the set G_B is a group. We call it the *adversarial group*.

The equivalence relations used to define subsystems can be greatly simplified. Indeed, it is easy to see that two states $\psi, \psi' \in \mathsf{St}(S)$ are equivalent for A if and only if there exists a transformation $\mathcal{U}_B \in \mathsf{G}_B$ such that

$$\psi' = \mathcal{U}_B \psi \, . \tag{70}$$

Hence, the states of the subsystem S_A are orbits of the group G_B: for every $\psi \in \mathsf{St}(S)$, we have

$$\mathrm{Tr}_B[\psi] := \left\{ \mathcal{U}_B \psi \ : \quad \mathcal{U}_B \in \mathsf{G}_B \right\} . \tag{71}$$

Similarly, the degradation of a transformation $\mathcal{U} \in \mathsf{G}(S)$ yields the orbit

$$\mathsf{Deg}_B(\mathcal{U}) = \left\{ \mathcal{U}_{B,1} \circ \mathcal{U} \circ \mathcal{U}_{B,2} \ : \qquad \mathcal{U}_{B,1}, \mathcal{U}_{B,2} \in \mathsf{G}_B \right\} . \tag{72}$$

It is easy to show that the transformations of the subsystem S_A are the orbits of the group G_B:

$$\mathsf{Transf}(S_A) = \left\{ \pi_A(\mathcal{U}) \ : \quad \mathcal{U} \in \mathsf{G}''_A \right\} , \qquad \pi_A(\mathcal{U}) := \left\{ \mathcal{U}_B \circ \mathcal{U} \ : \quad \mathcal{U}_B \in \mathsf{G}_B \right\} . \tag{73}$$

8. Closed Systems

Here, we define an abstract notion of "closed systems", which captures the essential features of what is traditionally called a closed system in quantum theory. Intuitively, the idea is that all the states of the closed system are "pure" and all the evolutions are reversible.

An obvious problem in defining closed system is that our framework does not include a notion of "pure state". To circumvent the problem, we define the closed systems in the following way:

Definition 15. *System S is* closed *iff it satisfies the Logical Conservation of Information and the Initialiation Requirement, that is, iff*

1. *every transformation is logically invertible,*
2. *there exists a state $\psi_0 \in \mathsf{St}(S)$ such that, for every other state $\psi \in \mathsf{St}(S)$, one has $\psi = \mathcal{V}\psi_0$ for some suitable transformation $\mathcal{V} \in \mathsf{Transf}(S)$.*

For a closed system, we nominally say that all the states in $\mathsf{St}(S)$ are "pure", or, more precisely, "dynamically pure". This definition is generally different from the usual definition of pure states as

extreme points of convex sets, or from the compositional definition of pure states as states with only product extensions [77]. First of all, dynamically pure states are *not a subset* of the state space: provided that the right conditions are met, they are *all* the states. Other differences between the usual notion of pure states and the notion of dynamically pure states are highlighted by the following example:

Example 4. *Let S be a system in which all states are of the form $U\rho_0 U^\dagger$, where U is a generic 2-by-2 unitary matrix, and $\rho_0 \in M_2(\mathbb{C})$ is a fixed 2-by-2 density matrix. For the transformations, we allow all unitary channels $U \cdot U^\dagger$. By construction, system S satisfies the initialization Requirement, as one can generate every state from the initial state ρ_0. Moreover, all the transformations of system S are unitary and therefore the Conservation of Information is satisfied, both at the physical and the logical level. Therefore, the states of system S are dynamically pure. Of course, the states $U\rho_0 U^\dagger$ need not be extreme points of the convex set of all density matrices, i.e., they need not be rank-one projectors. They are so only when the cyclic state ρ_0 is rank-one.*

On the other hand, consider a similar example, where

- *system S is a qubit,*
- *the states are pure states, of the form $|\psi\rangle\langle\psi|$ for a generic unit vector $|\psi\rangle \in \mathbb{C}^2$,*
- *the transformations are unitary channels $V \cdot V^\dagger$, where the unitary matrix V has* real *entries.*

Using the Bloch sphere picture, the physical transformations are rotations around the y axis. Clearly, the Initialization Requirement is not satisfied because there is no way to generate arbitrary points on the sphere using only rotations around the y-axis. In this case, the states of S are pure in the convex set sense, but not dynamically pure.

For closed systems satisfying the Physical Conservation of Information, every pair of pure states are interconvertible:

Proposition 13 (Transitive action on the pure states)**.** *If system S is closed and satisfies the Physical Conservation of Information, then, for every pair of states $\psi, \psi' \in \mathsf{St}(S)$, there exists a reversible transformation $\mathcal{U} \in \mathsf{G}(S)$ such that $\psi' = \mathcal{U}\psi$.*

Proof. By the Initialization Requirement, one has $\psi = \mathcal{V}\psi_0$ and $\psi' = \mathcal{V}'\psi_0$ for suitable $\mathcal{V}, \mathcal{V}' \in \mathsf{Transf}(S)$. By the Physical Conservation of Information, all the tranformations in $\mathsf{Transf}(S)$ are physically reversible. Hence, $\psi' = \mathcal{V}' \circ \mathcal{V}^{-1}\psi = \mathcal{U}\psi$, having defined $\mathcal{U} = \mathcal{V}' \circ \mathcal{V}^{-1}$. □

The requirement that all pure states be connected by reversible transformations has featured in many axiomatizations of quantum theory, either directly [5,44–46], or indirectly as a special case of other axioms [42,48]. Comparing our framework with the framework of general probabilistic theories, we can see that the dynamical definition of pure states refers to a rather specific situation, in which all pure states are connected, either to each other (in the case of physical reversibility) or with to a fixed cyclic state (in the case of logical reversibility).

9. Purification

Here, we show that closed systems satisfying the Physical Conservation of Information also satisfy the purification property [8,12,13,15,49–51], namely the property that every mixed state can be modelled as a pure state of a larger system in a canonical way. Under a certain regularity assumption, the same holds for closed systems satisfying only the Logical Conservation of Information.

9.1. Purification in Systems Satisfying the Physical Conservation of Information

Proposition 14 (Purification)**.** *Let S be a closed system satisfying the Physical Conservation of Information. Let A be an agent in S, and let $B = A'$ be its maximal adversary. Then, for every state $\rho \in \mathsf{St}(S_A)$, there exists a pure state $\psi \in \mathsf{St}(S)$, called the* purification of ρ*, such that $\rho = \mathrm{Tr}_B[\psi]$. Moreover, the purification*

of ρ is essentially unique*: if $\psi' \in \mathsf{St}(S)$ is another pure state with $\mathrm{Tr}_B[\psi] = \rho$, then there exists a reversible transformation $\mathcal{U}_B \in \mathsf{G}_B$ such that $\psi' = \mathcal{U}_B \psi$.*

Proof. By construction, the states of system S_A are orbits of states of system S under the adversarial group G_B. By Equation (71), every two states $\psi, \psi' \in \mathsf{St}(S)$ in the same orbit are connected by an element of G_B. □

Note that the notion of purification used here is more general than the usual notion of purification in quantum information and quantum foundations. The most important difference is that system S_A need not be a factor in a tensor product. Consider the example of the coherent superpositions vs. classical mixtures (Section 4.3). There, systems S_A and S_B coincide, their states are classical probability distributions, and the purifications are coherent superpositions. Two purifications of the same classical state $\mathbf{p} = (p_1, p_2, \dots, p_d)$ are two rank-one projectors $|\psi\rangle\langle\psi|$ and $|\psi'\rangle\langle\psi'|$ corresponding to unit vectors of the form

$$|\psi\rangle = \sum_n \sqrt{p_n}\, e^{i\theta_n} |n\rangle \qquad \text{and} \qquad |\psi'\rangle = \sum_n \sqrt{p_n}\, e^{i\theta'_n} |n\rangle\,. \tag{74}$$

One purification can be obtained from the other by applying a diagonal unitary matrix. Specifically, one has

$$|\psi'\rangle = U_B |\psi\rangle \qquad \text{with} \quad U_B = \sum_n e^{i(\theta'_n - \theta_n)} |n\rangle\langle n|\,. \tag{75}$$

For finite dimensional quantum systems, the notion of purification proposed here encompasses both the notion of entanglement and the notion of coherent superposition. The case of infinite dimensional systems will be discussed in the next subsection.

9.2. Purification in Systems Satisfying the Logical Conservation of Information

For infinite dimensional quantum systems, every density matrix can be purified, but not all purifications are connected by reversible transformations. Consider for example the unit vectors

$$|\psi\rangle_{AB} = \sqrt{1-x^2} \sum_{n=0}^{\infty} x^n\, |n\rangle_A \otimes |n\rangle_B \qquad \text{and} \qquad |\psi'\rangle_{AB} = \sqrt{1-x^2} \sum_{n=0}^{\infty} x^n\, |n\rangle_A \otimes |n+1\rangle_B\,, \tag{76}$$

for some $x \in [0,1)$.

For every fixed $x \neq 0$, there is one and only one operator V_B satisfying the condition $|\psi'\rangle_{AB} = (I_A \otimes V_B)|\psi\rangle_{AB}$, namely the shift operator $V_B = \sum_{n=0}^{\infty} |n+1\rangle\langle n|$. However, V_B is only an isometry, but not a unitary. This means that, if we define the states of system S_A as equivalence classes of pure states under local unitary equivalence, the two states $|\psi\rangle\langle\psi|$ and $|\psi'\rangle\langle\psi'|$ would end up into two different equivalence classes.

One way to address the problem is to relax the requirement of reversibility and to consider the monoid of isometries, defining

$$\mathsf{Transf}(S) := \{V \cdot V^\dagger : \quad V \in \mathsf{Lin}(S)\,,\ V^\dagger V = I\}\,. \tag{77}$$

Given two purifications of the same state, say $|\psi\rangle$ and $|\psi'\rangle$, it is possible to show that at least one of the following possibilities holds:

1. $|\psi'\rangle = (I_A \otimes V_B)\,|\psi\rangle$ for some isometry V_B acting on system S_B,
2. $|\psi\rangle = (I_A \otimes V_B)\,|\psi'\rangle$ for some isometry V_B acting on system S_B.

Unfortunately, this uniqueness property is not automatically valid in every system satisfying the Logical Conservation of Information. Still, we will now show a regularity condition, under which the uniqueness property is satisfied:

Definition 16. *Let S be a system satisfying the Logical Conservation of Information, let $M \subseteq \mathsf{Transf}(S)$ be a monoid, and let $\mathsf{Deg}_{\mathsf{M}}(\psi)$ be the set defined by*

$$\mathsf{Deg}_{\mathsf{M}}(\psi) = \Big\{ \mathcal{V}\,\psi \;:\quad \mathcal{V} \in \mathsf{M} \Big\}\,. \tag{78}$$

We say that the monoid $\mathsf{M} \subseteq \mathsf{Transf}(\mathsf{S})$ is regular *iff*

1. *for every pair of states $\psi, \psi' \in \mathsf{St}(S)$, the condition $\mathsf{Deg}_{\mathsf{M}}(\psi) \cap \mathsf{Deg}_{\mathsf{M}}(\psi') \neq \emptyset$ implies that there exists a transformation $\mathcal{U} \in \mathsf{M}$ such that $\psi' = \mathcal{U}\psi$ or $\psi = \mathcal{U}\psi'$,*
2. *for every pair of transformations $\mathcal{V}, \mathcal{V}' \in \mathsf{M}$, there exists a transformation $\mathcal{W} \in \mathsf{M}$ such that $\mathcal{V} = \mathcal{W} \circ \mathcal{V}'$ or $\mathcal{V}' = \mathcal{W} \circ \mathcal{V}$.*

The regularity conditions are satisfied in quantum theory by the monoid of isometries.

Example 5 (Isometric channels in quantum theory)**.** *Let S be a quantum system with separable Hilbert space $\mathcal{H}$, of dimension $d \leq \infty$. Let $\mathsf{St}(S)$ the set of all pure quantum states, and let $\mathsf{Transf}(S)$ be the monoid of all isometric channels.*

We now show that the monoid $\mathsf{M} = \mathsf{Transf}(\mathsf{S})$ is regular. The first regularity condition is immediate because for every pair of unit vectors $|\psi\rangle$ and $|\psi'\rangle$ there exists an isometry (in fact, a unitary) V such that $|\psi'\rangle = U|\psi\rangle$. Trivially, this implies the relation $|\psi'\rangle\langle\psi'| = U|\psi\rangle\langle\psi|U^\dagger$ at the level of quantum states and isometric channels.

Let us see that the second regularity condition holds. Let $V, V' \in \mathsf{Lin}(\mathcal{H})$ be two isometries on $\mathcal{H}$, and let $\{|i\rangle\}_{i=1}^d$ be the standard basis for $\mathcal{H}$. Then, the isometries V and V' can be written as

$$V = \sum_{i=1}^{d} |\phi_i\rangle\langle i| \qquad \text{and} \qquad V' = \sum_{i} |\phi'_i\rangle\langle i|\,, \tag{79}$$

where $\{|\phi_i\rangle\}_{i=1}^d$ and $\{|\phi'_i\rangle\}_{i=1}^d$ are orthonormal vectors (not necessarily forming bases for the whole Hilbert space $\mathcal{H}$). Define the subspaces $S = \mathsf{Span}\{|\phi_i\rangle\}_{i=1}^d$ and $S' = \mathsf{Span}\{|\phi'_i\rangle\}_{i=1}^d$, and let $\{|\psi_j\rangle\}_{j=1}^r$ and $\{|\psi'_j\rangle\}_{j=1}^{r'}$ be orthonormal bases for the orthogonal complements $S^\perp$ and $S'^\perp$, respectively. If $r \leq r'$, we define the isometry

$$W = \left(\sum_{i=1}^{d} |\phi'_i\rangle\langle\phi_i| \right) + \left(\sum_{j=1}^{r} |\psi'_j\rangle\langle\psi_j| \right)\,, \tag{80}$$

and we obtain the condition $V' = WV$. Alternatively, if $r' \leq r$, we can define the isometry

$$W = \left(\sum_{i=1}^{d} |\phi_i\rangle\langle\phi'_i| \right) + \left(\sum_{j=1}^{r} |\psi_j\rangle\langle\psi'_j| \right)\,, \tag{81}$$

and we obtain the condition $V = WV'$. At the level of isometric channels, we obtained the condition $\mathcal{V}' = \mathcal{W} \circ \mathcal{V}$ or the condition $\mathcal{V} = \mathcal{W} \circ \mathcal{V}'$, with $\mathcal{V}(\cdot) = V \cdot V^\dagger$, $\mathcal{V}'(\cdot) = V' \cdot V'^\dagger$, and $\mathcal{W}(\cdot) = W \cdot W^\dagger$.

The fact that the monoid of all isometric channels is regular implies that other monoids of isometric channels are also regular. For example, if the Hilbert space $\mathcal{H}$ has the tensor product structure $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, then the monoid of local isometric channels, defined by isometries of the form $I_A \otimes V_B$, is regular. More generally, if the Hilbert space is decomposed as

$$\mathcal{H} = \bigoplus_{k} \left(\mathcal{H}_{A,k} \otimes \mathcal{H}_{B,k} \right)\,, \tag{82}$$

then the monoid of isometric channels generated by isometries of the form

$$V = \bigoplus_k (I_{A,k} \otimes V_{B,k}) \tag{83}$$

is regular.

We are now in position to derive the purification property for general closed systems:

Proposition 15. *Let S be a closed system. Let A be an agent and let $B = A'$ be its maximal adversary. If $\mathsf{Act}(B;S)$ is a regular monoid, the condition $\mathrm{Tr}_B[\psi] = \mathrm{Tr}_B[\psi']$ implies that there exists some invertible transformation $\mathcal{V}_B \in \mathsf{Transf}(B;S)$ such that the relation $\psi' = \mathcal{V}_B\psi$ or the relation $\psi = \mathcal{V}_B\psi'$ holds.*

The proof is provided in Appendix H. In conclusion, we obtained the following

Corollary 1 (Purification)**.** *Let S be a closed system, let A be an agent in S, and let $B = A'$ be its maximal adversary. If the monoid $\mathsf{Act}(B;S)$ is regular, then every state $\rho \in \mathsf{St}(S_A)$ has a purification $\psi \in \mathsf{St}(S)$, i.e., a state such that $\rho = \mathrm{Tr}_B[\psi]$. Moreover, the purification is essentially unique: if $\psi' \in \mathsf{St}(S)$ is another state with $\mathrm{Tr}_B[\psi] = \rho$, then there exists a reversible transformation $\mathcal{V}_B \in \mathsf{Act}(B;S)$ such that the relation $\psi' = \mathcal{V}_B\psi$ or the relation $\psi = \mathcal{V}_B\psi'$ holds.*

10. Example: Group Representations on Quantum State Spaces

We conclude the paper with a macro-example, involving group representations in closed-system quantum theory. The point of this example is to illustrate the general notion of purification introduced in this paper and to characterize the sets of mixed states associated with different agents.

As system S, we consider a quantum system with Hilbert space $\mathcal{H}_S$, possibly of infinite dimension. We let $\mathsf{St}(S)$ be the set of pure quantum states, and let $\mathsf{G}(S)$ be the group of all unitary channels. With this choice, the total system is closed and satisfies the Physical Conservation of Information.

Suppose that agent A is able to perform a group of transformations, such as e.g., the group of phase shifts on a harmonic oscillator, or the group of rotations of a spin j particle. Mathematically, we focus our attention on unitary channels arising from some representation of a given compact group G. Denoting the representation as $U : \mathsf{G} \to \mathsf{Lin}(\mathcal{H}_S)\,, g \mapsto U_g$, the group of Alice's actions is

$$G_A = \left\{ \mathcal{U}_g(\cdot) = U_g \cdot U_g^\dagger : \quad g \in \mathsf{G} \right\}. \tag{84}$$

The maximal adversary of A is the agent $B = A'$ who is able to perform all unitary channels $\mathcal{V}$ that commute with those in G_A, namely, the unitary channels in the group

$$\mathsf{G}_B := \left\{ \mathcal{V} \in \mathsf{G}(S) : \quad \mathcal{V} \circ \mathcal{U}_g = \mathcal{U}_g \circ \mathcal{V} \quad \forall g \in \mathsf{G} \right\}. \tag{85}$$

Specifically, the channels $\mathcal{V}$ correspond to unitary operators V satisfying the relation

$$V U_g = \omega(V,g)\, U_g V \qquad \forall g \in \mathsf{G}\,, \tag{86}$$

where, for every fixed V, the function $\omega(V,\cdot) : \mathsf{G} \to \mathbb{C}$ is a multiplicative character, i.e., a one-dimensional representation of the group G.

Note that, if two unitaries V and W satisfy Equation (86) with multiplicative characters $\omega(V,\cdot)$ and $\omega(W,\cdot)$, respectively, then their product VW satisfies Equation (86) with multiplicative character $\omega(VW,\cdot) = \omega(V,\cdot)\,\omega(W,\cdot)$. This means that the function $\omega : \mathsf{G}_B \times \mathsf{G} \to \mathbb{C}$ is a multiplicative *bicharacter:* $\omega(V,\cdot)$ is a multiplicative character for G for every fixed $V \in \mathsf{G}_B$, and, at the same time, $\omega(\cdot,g)$ is a multiplicative character for G_B for every fixed $g \in \mathsf{G}$.

The adversarial group G_B contains the commutant of the representation $U : g \mapsto U_g$, consisting of all the unitaries V such that

$$VU_g = U_g V \qquad \forall g \in \mathsf{G}\,. \tag{87}$$

The unitaries in the commutant satisfy Equation (86) with the trivial multiplicative character $\omega(V, g) = 1$, $\forall g \in \mathsf{G}$. In general, the adversarial group may contain other unitary operators, corresponding to non-trivial multiplicative characters. The full characterization of the adversarial group is provided by the following theorem:

Theorem 3. *Let* G *be a compact group, let* $U : \mathsf{G} \to \mathsf{Lin}(\mathcal{H})$ *be a projective representation of* G*, and let* G_A *be the group of channels* $\mathsf{G}_A := \{U_g \cdot U_g^\dagger \quad g \in \mathsf{G}\}$*. Then, the adversarial group* G_B *is isomorphic to the semidirect product* $\mathsf{A} \ltimes U'$*, where* U' *is the commutant of the set* $\{U_g \ : g \in \mathsf{G}\}$*, and* A *is an Abelian subgroup of the group of permutations of* $\mathsf{Irr}(U)$*, the set of irreducible representations contained in the decomposition of the representation* U_g*.*

The proof is provided in Appendix I, and a simple example is presented in Appendix J.

In the following, we will illustrate the construction of the state space S_A in a the prototypical example where the group G is a compact connected Lie group.

Compact Connected Lie Groups

When G is a compact connected Lie group, the characterization of the adversarial group is simplified by the following theorem:

Theorem 4. *If* G *is a compact connected Lie group, then the Abelian subgroup* A *of Theorem 3 is trivial, and all the solutions of Equation (86) have* $\omega(V, g) = 1\ \forall g \in \mathsf{G}$*.*

The proof is provided in Appendix K.

For compact connected Lie groups, the the adversarial group coincides exactly with the commutant of the representation $U : \mathsf{G} \to \mathsf{Lin}(\mathcal{H}_S)$. An explicit expression can be obtained in terms of the isotypic decomposition [78]

$$U_g = \bigoplus_{j \in \mathsf{Irr}(U)} \left(U_g^{(j)} \otimes I_{\mathcal{M}_j} \right), \tag{88}$$

where $\mathsf{Irr}(U)$ is the set of irreducible representations (irreps) of G contained in the decomposition of U, $U^{(j)} : g \mapsto U_g^{(j)}$ is the irreducible representation of G acting on the representation space $\mathcal{R}_j$, and $I_{\mathcal{M}_j}$ is the identity acting on the multiplicity space $\mathcal{M}_j$. From this expression, it is clear that the adversarial group G_B consists of unitary gates V of the form

$$V = \bigoplus_{j \in \mathsf{Irr}(U)} \left(I_{\mathcal{R}_j} \otimes V_j \right), \tag{89}$$

where $I_{\mathcal{R}_j}$ is the identity operator on the representation space $\mathcal{R}_j$, and V_j is a generic unitary operator on the multiplicity space $\mathcal{M}_j$.

In general, the agents A and $B = A'$ do not form a dual pair. Indeed, it is not hard to see that the maximal adversary of B is the agent $C = A''$ that can perform every unitary channel $\mathcal{U}(\cdot) = U \cdot U^\dagger$, where U is a unitary operator of the form

$$U = \bigoplus_{j \in \mathsf{Irr}(U)} \left(U_j \otimes I_{\mathcal{M}_j} \right), \tag{90}$$

U_j being a generic unitary operator on the representation space $\mathcal{R}_j$. When A and B form a dual par, the groups G_A and G_B are sometimes called *gauge groups* [79].

It is now easy to characterize the subsystem S_A. Its states are equivalence classes of pure states under the relation $|\psi\rangle\langle\psi| \simeq_A |\psi'\rangle\langle\psi'|$ iff

$$\exists U_B \in \mathsf{G}_B \qquad \text{such that} \qquad |\psi'\rangle = U_B|\psi\rangle\,. \tag{91}$$

It is easy to see that two states in the same equivalence class must satisfy the condition

$$\mathrm{Tr}_B(|\psi'\rangle\langle\psi'|) = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)\,, \tag{92}$$

where the "partial trace over agent B" is Tr_B is the map

$$\mathrm{Tr}_B(\rho) := \bigoplus_{j\in\mathsf{Irr}(U)} \mathrm{Tr}_{\mathcal{M}_j}[\Pi_j\,\rho\,\Pi_j]\,, \tag{93}$$

Π_j being the projector on the subspace $\mathcal{R}_j \otimes \mathcal{M}_j$.

Conversely, it is possible to show that the state $\mathrm{Tr}_B(|\psi\rangle\langle\psi|)$ completely identifies the equivalence class $[|\psi\rangle\langle\psi|]_A$.

Proposition 16. *Let $|\psi\rangle, |\psi'\rangle \in \mathcal{H}_S$ be two unit vectors such that $\mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \mathrm{Tr}_B(|\psi'\rangle\langle\psi'|)$. Then, there exists a unitary operator $U_B \in \mathsf{G}_B$ such that $|\psi'\rangle = U_B|\psi\rangle$.*

The proof is provided in Appendix L.

We have seen that the states of system S_A are in one-to-one correspondence with the density matrices of the form $\mathrm{Tr}_B(|\psi\rangle\langle\psi|)$, where $|\psi\rangle \in \mathcal{H}_S$ is a generic pure state. Note that the rank of the density matrices ρ_j in Equation (A109) cannot be larger than the dimensions of the spaces $\mathcal{R}_j$ and $\mathcal{M}_j$, denoted as $d_{\mathcal{R}_j}$ and $d_{\mathcal{M}_j}$, respectively. Taking this fact into account, we can represent the states of S_A as

$$\mathsf{St}(S_A) \simeq \Big\{\rho = \bigoplus_{j\in\mathsf{Irr}(U)} p_j\,\rho_j \;:\; \rho_j \in \mathsf{QSt}(\mathcal{R}_j)\,,\; \mathsf{Rank}(\rho_j) \leq \min\{d_{\mathcal{R}_j}, d_{\mathcal{M}_j}\}\Big\}\,, \tag{94}$$

where $\{p_j\}$ is a generic probability distribution. The state space of system S_A is *not convex*, unless the condition

$$d_{\mathcal{M}_j} \geq d_{\mathcal{R}_j} \qquad \forall j \in \mathsf{Irr}(U) \tag{95}$$

is satisfied. Basically, in order to obtain a convex set of density matrices, we need the total system S to be "sufficiently large" compared to its subsystem S_A. This observation is a clue suggesting that the standard convex framework could be considered as the effective description of subsystems of "large" closed systems.

Finally, note that, in agreement with the general construction, the pure states of system S are *"purifications"* of the states of the system S_A. Every state of system S_A can be obtained from a pure state of system S by *"tracing out"* system S_B. Moreover, every two purifications of the same state are connected by a unitary transformation in G_B.

11. Conclusions

In this paper, we adopted rather minimalistic framework, in which a single physical system was described solely in terms of states and transformations, without introducing measurements. Or at least, without introducing measurements *in an explicit way*: of course, one could always interpret certain transformations as "measurement processes", but this interpretation is not necessary for any of the conclusions drawn in this paper.

Our framework can be interpreted in two ways. One way is to think of it as a fragment of the larger framework of operational-probabilistic theories [8,11–13], in which systems can be freely composed and measurements are explicitly described. The other way is to regard our framework as a dynamicist framework, meant to describe physical systems *per se*, independently of any observer. Both approaches are potentially fruitful.

On the operational-probabilistic side, it is interesting to see how the definition of subsystem adopted in this paper interacts with probabilities. For example, we have seen in a few examples that the state space of a subsystem is not always convex: convex combination of allowed states are not necessarily allowed states. It is then natural to ask: under which condition is convexity retrieved? In a different context, the non-trivial relation between convexity and the dynamical notion of system has been emerged in a work of Galley and Masanes [80]. There, the authors studied alternatives to quantum theory where the closed systems have the same states and the same dynamics of closed quantum systems, while the measurements are different from the quantum measurements. Among these theories, they found that quantum theory is the only theory where subsystems have a convex state space. These and similar clues are an indication that the interplay between dynamical notions and probabilistic notions plays an important role in determining the structure of physical theories. Studying this interplay is a promising avenue of future research.

On the opposite end of the spectrum, it is interesting to explore how far the measurement-free approach can reach. An interesting research project is to analyze the notions of subsystem, pure state, and purification, in the context of algebraic quantum field theory [22] and quantum statistical mechanics [32]. This is important because the notion of pure state as an extreme point of the convex set breaks down for type III von Neumann algebras [81], whereas the notions used in this paper (commutativity of operations, cyclicity of states) would still hold. Another promising clue is the existence of dual pairs of non-overlapping agents, which amounts to the requirement that the set of operations of each agent has trivial center and coincides with its double commutant. A similar condition plays an important role in the algebraic framework, where the operator algebras with trivial center are known as factors, and are at the basis of the theory of von Neumann algebras [82,83].

Finally, another interesting direction is to enrich the structure of system with additional features, such as a metric, quantifying the proximity of states. In particular, one may consider a strengthened formulation of the Conservation of Information, in which the physical transformations are required not only to be invertible, but also to preserve the distances. It is then interesting to consider how the metric on the pure states of the whole system induces a metric on the subsystems, and to search for relations between global metric and local metric. Also in this case, there is a promising precedent, namely the work of Uhlmann [84], which led to the notion of fidelity [85]. All these potential avenues of future research suggest that the notions investigated in this work may find application in a variety of different contexts, and for a variety of interpretational standpoints.

Acknowledgments: It is a pleasure to thank Gilles Brassard and Paul Raymond-Robichaud for stimulating discussions on their recent work [66], Adán Cabello, Markus Müller, and Matthias Kleinmann for providing motivation to the problem of deriving subsystems, Mauro D'Ariano and Paolo Perinotti for the invitation to contribute to this Special Issue, and Christopher Timpson and Adam Coulton for an invitation to present at the Oxford Philosophy of Physics Seminar Series, whose engaging atmosphere stimulated me to think about extensions of the Purification Principle. I am also grateful to the three referees of this paper for useful suggestions, and to Robert Spekkens, Doreen Fraser, Lídia del Rio, Thomas Galley, John Selby, Ryszard Kostecki, and David Schmidt for interesting discussions during the revision of the original manuscript. This work is supported by the Foundational Questions Institute through grant FQXi-RFP3-1325, the National Natural Science Foundation of China through grant 11675136, the Croucher Foundation, the Canadian Institute for Advanced Research (CIFAR), and the Hong Research Grant Council through grant 17326616. This publication was made possible through the support of a grant from the John Templeton Foundation. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation. The authors also acknowledge the hospitality of Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Research, Innovation and Science.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A. Proof That Definitions (20) and (21) Are Well-Posed

We give only the proof for definition (20), as the other proof follows the same argument.

Proposition A1. *If the transformations* $\mathcal{S}, \widetilde{\mathcal{S}}, \mathcal{T}, \widetilde{\mathcal{T}} \in \mathsf{Act}(A;S)''$ *are such that* $[\mathcal{S}]_A = [\widetilde{\mathcal{S}}]_A$ *and* $[\mathcal{T}]_A = [\widetilde{\mathcal{T}}]_A$*, then* $[\mathcal{S}\circ\mathcal{T}]_A = [\widetilde{\mathcal{S}}\circ\widetilde{\mathcal{T}}]_A$.

Proof. Let $(\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_m) \subset \mathsf{Act}(A;S)''$ and $(\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_n) \subset \mathsf{Act}(A;S)''$ be two finite sequences such that

$$\begin{aligned} &\mathcal{S}_1 = \mathcal{S}\,, \qquad \mathcal{S}_m = \widetilde{\mathcal{S}}\,, \qquad \mathsf{Deg}_{A'}(\mathcal{S}_i) \cap \mathsf{Deg}_{A'}(\mathcal{S}_{i+1}) \neq \emptyset \quad \forall i \in \{1,\ldots,m-1\}, \\ &\mathcal{T}_1 = \mathcal{T}\,, \qquad \mathcal{T}_n = \widetilde{\mathcal{T}}\,, \qquad \mathsf{Deg}_{A'}(\mathcal{T}_j) \cap \mathsf{Deg}_{A'}(\mathcal{T}_{j+1}) \neq \emptyset \quad \forall j \in \{1,\ldots,n-1\}. \end{aligned} \tag{A1}$$

Without loss of generality, we assume that the two finite sequences have the same length $m = n$. When this is not the case, one can always add dummy entries and ensure that the two sequences have the same length: for example, if $m < n$, one can always define $\mathcal{S}_i := \mathcal{S}_m$ for all $i \in \{m+1,\ldots,n\}$.

Equation (A1) mean that for every i and j there exist transformations $\mathcal{B}_i, \widetilde{\mathcal{B}}_i, \mathcal{C}_j, \widetilde{\mathcal{C}}_j \in \mathsf{Act}(A;S)'$ such that

$$\begin{aligned} \mathcal{B}_i \circ \mathcal{S}_i &= \widetilde{\mathcal{B}}_i \circ \mathcal{S}_{i+1}, \\ \mathcal{C}_j \circ \mathcal{T}_j &= \widetilde{\mathcal{C}}_j \circ \mathcal{T}_{j+1}. \end{aligned} \tag{A2}$$

Using the above equalities for $i = j$, and using the fact that transformations in $\mathsf{Act}(A;S)'$ commute with transformations in $\mathsf{Act}(A;S)''$, we obtain

$$\begin{aligned} (\mathcal{B}_i \circ \mathcal{C}_i) \circ (\mathcal{S}_i \circ \mathcal{T}_i) &= (\mathcal{B}_i \circ \mathcal{S}_i) \circ (\mathcal{C}_i \circ \mathcal{T}_i) \\ &= (\widetilde{\mathcal{B}}_i \circ \mathcal{S}_{i+1}) \circ (\widetilde{\mathcal{C}}_i \circ \mathcal{T}_{i+1}) \\ &= (\widetilde{\mathcal{B}}_i \circ \widetilde{\mathcal{C}}_i) \circ (\mathcal{S}_{i+1} \circ \mathcal{T}_{i+1})\,. \end{aligned} \tag{A3}$$

In short, we proved that

$$\mathsf{Deg}_{A'}(\mathcal{S}_i \circ \mathcal{T}_i) \cap \mathsf{Deg}_{A'}(\mathcal{S}_{i+i} \circ \mathcal{T}_{i+1}) \neq \emptyset \qquad \forall i \in \{1,\ldots,n-1\}\,. \tag{A4}$$

To conclude, observe that the sequence $(\mathcal{S}_1 \circ \mathcal{T}_1, \mathcal{S}_2 \circ \mathcal{T}_2, \ldots, \mathcal{S}_n \circ \mathcal{T}_n)$ satisfies $\mathcal{S}_1 \circ \mathcal{T}_1 = \mathcal{S} \circ \mathcal{T}$, $\mathcal{S}_n \circ \mathcal{T}_n = \widetilde{\mathcal{S}} \circ \widetilde{\mathcal{T}}$, and Equation (A4). By definition, this means that the transformations $\mathcal{S} \circ \mathcal{T}$ and $\widetilde{\mathcal{S}} \circ \widetilde{\mathcal{T}}$ are in the same equivalence class. □

Appendix B. The Commutant of the Local Channels

Here, we show that the commutant of the quantum channels of the form $\mathcal{A} \otimes \mathcal{I}_B$ consists of quantum channels of the form $\mathcal{I}_A \otimes \mathcal{B}$.

Let $\mathcal{C} \in \mathsf{Chan}(S)$ be a quantum channel that commutes with all channels of the form $\mathcal{A} \otimes \mathcal{I}_B$, with $\mathcal{A} \in \mathsf{Chan}(A)$. For a fixed unit vector $|\alpha\rangle \in \mathcal{H}_A$, consider the erasure channel $\mathcal{A}_\alpha \in \mathsf{Chan}(A)$ defined by

$$\mathcal{A}_\alpha(\rho) = |\alpha\rangle\langle\alpha|\ \mathrm{Tr}[\rho] \qquad \forall \rho \in \mathsf{Lin}(A)\,. \tag{A5}$$

Then, the commutation condition $\mathcal{C} \circ (\mathcal{A}_\alpha \otimes \mathcal{I}_B) = (\mathcal{A}_\alpha \otimes \mathcal{I}_B) \circ \mathcal{C}$ implies

$$\begin{aligned} \mathcal{C}\Big(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\Big) &= \mathcal{C}\Big[\Big(\mathcal{A}_\alpha \otimes \mathcal{I}_B\Big)\Big(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\Big)\Big] \\ &= \Big(\mathcal{A}_\alpha \otimes \mathcal{I}_B\Big)\Big[\mathcal{C}\Big(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\Big)\Big] \\ &= |\alpha\rangle\langle\alpha| \otimes \mathrm{Tr}_A\Big[\mathcal{C}\Big(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\Big)\Big] \qquad \forall |\beta\rangle \in \mathcal{H}_B\,. \end{aligned} \tag{A6}$$

Tracing over B on both sides of Equation (A6), we obtain

$$\mathrm{Tr}_B\Big[\mathcal{C}\Big(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\Big)\Big] = |\alpha\rangle\langle\alpha|\,. \tag{A7}$$

The above relation implies that the state $\mathcal{C}\Big(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\Big)$ is of the form

$$\mathcal{C}\Big(|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\Big) = |\alpha\rangle\langle\alpha| \otimes \mathcal{B}(|\beta\rangle\langle\beta|)\,, \tag{A8}$$

for some suitable channel $\mathcal{B} \in \mathsf{Chan}(B)$. Since $|\alpha\rangle$ and $|\beta\rangle$ are arbitrary, we obtained $\mathcal{C} = \mathcal{I}_A \otimes \mathcal{B}$.

Appendix C. Subsystems Associated to Finite Dimensional Von Neumann Algebras

Here, we prove the statements made in the main text about quantum channels with Kraus operators in a given algebra.

Appendix C.1. The Commutant of $\mathsf{Chan}(\mathsf{A})$

The purpose of this subsection is to prove the following theorem:

Theorem A1. *Let* A *be a von Neumann subalgebra of* $M_d(\mathbb{C})$, $d < \infty$, *and let* $\mathsf{Chan}(\mathsf{A})$ *be the set of quantum channels with Kraus operators in* A. *Then, the commutant of* $\mathsf{Chan}(\mathsf{A})$ *is the set of channels with Kraus operators in the algebra* A'. *In formula,*

$$\mathsf{Chan}(\mathsf{A})' = \mathsf{Chan}(\mathsf{A}')\,. \tag{A9}$$

The proof consists of a few lemmas, provided in the following.

Lemma A1. *Every channel* $\mathcal{D} \in \mathsf{Chan}(A)'$ *must satisfy the condition*

$$\mathcal{P}_l \circ \mathcal{D} \circ \mathcal{P}_k = 0 \qquad \forall l \neq k\,, \tag{A10}$$

where $\mathcal{P}_k$ *is the CP map* $\mathcal{P}_k(\cdot) := \Pi_k \cdot \Pi_k$, *and* Π_k *is the projector on the subspace* $\mathcal{H}_{A_k} \otimes \mathcal{H}_{B_k}$ *in Equation (31).*

Proof. Consider the quantum channel $\mathcal{C} \in \mathsf{Chan}(\mathsf{A})$ defined as

$$\mathcal{C} := \bigoplus_k \Big(|\alpha_k\rangle\langle\alpha_k|\ \mathrm{Tr}_{A_k} \otimes \mathcal{I}_{B_k}\Big) \circ \mathcal{P}_k\,, \tag{A11}$$

where each $|\alpha_k\rangle$ is a generic (but otherwise fixed) unit vector in $\mathcal{H}_{A_k}$ and $\mathcal{I}_{B_k}$ is the identity map on $\mathsf{Lin}(\mathcal{H}_{B_k})$. By definition, every channel $\mathcal{D} \in \mathsf{Chan}(\mathsf{A})'$ must satisfy the condition $\mathcal{C} \circ \mathcal{D} = \mathcal{D} \circ \mathcal{C}$. In particular, we must have

$$\begin{aligned}\mathcal{D}(|\alpha_k\rangle\langle\alpha_k| \otimes |\beta_k\rangle\langle\beta_k|) &= (\mathcal{D} \circ \mathcal{C})(|\alpha_k\rangle\langle\alpha_k| \otimes |\beta_k\rangle\langle\beta_k|) \\ &= (\mathcal{C} \circ \mathcal{D})(|\alpha_k\rangle\langle\alpha_k| \otimes |\beta_k\rangle\langle\beta_k|) \\ &= \bigoplus_l \Big(|\alpha_l\rangle\langle\alpha_l| \otimes \mathrm{Tr}_{A_l} \Big[(\mathcal{P}_l \circ \mathcal{D})(|\alpha_k\rangle\langle\alpha_k| \otimes |\beta_k\rangle\langle\beta_k|) \Big] \Big). \end{aligned} \tag{A12}$$

Applying the CP map $\mathcal{P}_l$ on both sides of the above equality, we obtain the relation

$$(\mathcal{P}_l \circ \mathcal{D})(|\alpha_k\rangle\langle\alpha_k| \otimes |\beta_k\rangle\langle\beta_k|) = |\alpha_l\rangle\langle\alpha_l| \otimes \mathcal{M}_l(|\alpha_k\rangle\langle\alpha_k| \otimes |\beta_k\rangle\langle\beta_k|)\,, \tag{A13}$$

where $\mathcal{M}_l$ is the map from $M_d(\mathbb{C})$ to $\mathsf{Lin}(\mathcal{H}_{A_l})$ defined as $\mathcal{M}_l := \mathrm{Tr}_{A_l} \circ \mathcal{P}_l \circ \mathcal{D}$.

Note that the right-hand side of Equation (A13) depends on the choice of vector $|\alpha_l\rangle$, which is arbitrary. On the other hand, the left-hand side does not depend on $|\alpha_l\rangle$. Hence, the only way that the two sides of Equation (A13) can be equal for $k \neq l$ is that they are both equal to 0. Moreover, since $|\alpha_k\rangle$ and $|\beta_k\rangle$ are arbitrary vectors in $\mathcal{H}_{A_k}$ and $\mathcal{H}_{B_k}$, respectively, Equation (A13) implies the relation

$$(\mathcal{P}_l \circ \mathcal{D})(\rho) = 0 \qquad \forall \rho \in \mathsf{Lin}(\mathcal{H}_{A_k} \otimes \mathcal{H}_{B_k})\,, \quad \forall l \neq k\,. \tag{A14}$$

Since ρ is an arbitrary operator in $\mathsf{Lin}(\mathcal{H}_{A_k} \otimes \mathcal{H}_{B_k})$, we conclude that the relation $\mathcal{P}_l \circ \mathcal{D} \circ \mathcal{P}_k = 0$ holds for every $l \neq k$. □

Lemma A2. *Every channel $\mathcal{D} \in \mathsf{Chan}(A)'$ must satisfy the conditions*

$$\mathcal{D} \circ \mathcal{P}_k = \mathcal{P}_k \circ \mathcal{D} \circ \mathcal{P}_k \qquad \forall k \tag{A15}$$

and

$$\mathcal{P}_k \circ \mathcal{D} = \mathcal{P}_k \circ \mathcal{D} \circ \mathcal{P}_k \qquad \forall k\,. \tag{A16}$$

In short: $\mathcal{D} \circ \mathcal{P}_k = \mathcal{P}_k \circ \mathcal{D}$ for every k.

Proof. Define $\mathcal{D}_k := \mathcal{D} \circ \mathcal{P}_k$. Then, the Cauchy–Schwarz inequality yields

$$\begin{aligned}\Big|\langle\phi|\Pi_i\,\mathcal{D}_k(\rho)\,\Pi_j\,|\phi\rangle\Big| &\leq \sqrt{\langle\phi|\Pi_i\,\mathcal{D}_k(\rho)\,\Pi_i\,|\phi\rangle\ \langle\phi|\Pi_j\,\mathcal{D}_k(\rho)\,\Pi_j\,|\phi\rangle} \\ &\leq \sqrt{\langle\phi|(\mathcal{P}_i \circ \mathcal{D} \circ \mathcal{P}_k)(\rho)\,|\phi\rangle\ \langle\phi|(\mathcal{P}_j \circ \mathcal{D} \circ \mathcal{P}_k)(\rho)\,|\phi\rangle}\,. \end{aligned} \tag{A17}$$

Thanks to Lemma A1, we know the right-hand side is 0 unless $i = j = k$. Since the vector $|\phi\rangle$ is are arbitrary, the condition $|\langle\phi|\Pi_i\,\mathcal{D}_k(\rho)\,\Pi_j\,|\phi\rangle| = 0$ implies the relation $\Pi_i\,\mathcal{D}_k(\rho)\,\Pi_j = 0$. Using this fact, we obtain the relation

$$\begin{aligned}(\mathcal{D} \circ \mathcal{P}_k)(\rho) &= \mathcal{D}_k(\rho) \\ &= \sum_{i,j} \Pi_i\,\mathcal{D}_k(\rho)\,\Pi_j \\ &= \Pi_k\,\mathcal{D}_k(\rho)\,\Pi_k \\ &= (\mathcal{P}_k \circ \mathcal{D} \circ \mathcal{P}_k)(\rho)\,, \end{aligned} \tag{A18}$$

valid for arbitrary density matrices ρ, and therefore for arbitrary matrices in $M_d(\mathbb{C})$. In conclusion, Equation (A16) holds.

The proof of Equation (A15) is analogous to that of Equation (A16), with the only difference that it uses the *adjoint map*, which for a generic linear map $\mathcal{L} : \mathsf{Lin}(\mathcal{H}_S) \to \mathsf{Lin}(\mathcal{H}_S)$ is defined by the relation

$$\mathrm{Tr}[\mathcal{L}^\dagger(O)\,\rho] := \mathrm{Tr}[O\,\mathcal{L}(\rho)] \qquad \forall O \in M_d(\mathbb{C})\,,\ \forall \rho \in M_d(\mathbb{C})\,. \tag{A19}$$

Specifically, we define the map $\widetilde{\mathcal{D}}_k := \mathcal{P}_k \circ \mathcal{D}$. Then, we obtain the relation

$$\begin{aligned}
\Big|\,\langle\phi|\,\widetilde{\mathcal{D}}_k(\Pi_i\rho\Pi_j)\,|\phi\rangle\Big| &= \Big|\,\mathrm{Tr}\left[\widetilde{\mathcal{D}}_k^\dagger(|\phi\rangle\langle\phi|)\Pi_i\rho\Pi_j\right]\Big| \\
&= \left|\mathrm{Tr}\left[\left(\sqrt{\widetilde{\mathcal{D}}_k^\dagger(|\phi\rangle\langle\phi|)}\Pi_i\sqrt{\rho}\right)\left(\sqrt{\rho}\Pi_j\sqrt{\widetilde{\mathcal{D}}_k^\dagger(|\phi\rangle\langle\phi|)}\right)\right]\right| \\
&\le \sqrt{\mathrm{Tr}\left[\mathcal{D}_k^\dagger(|\phi\rangle\langle\phi|)\,\Pi_i\rho\Pi_i\right]\ \mathrm{Tr}\left[\mathcal{D}_k^\dagger(|\phi\rangle\langle\phi|)\,\Pi_j\rho\Pi_j\right]} \\
&= \sqrt{\langle\phi|\,\widetilde{\mathcal{D}}_k(\Pi_i\rho\Pi_i)\,|\phi\rangle\ \langle\psi|\,\widetilde{\mathcal{D}}_k(\Pi_j\rho\Pi_j)\,|\psi\rangle} \\
&= \sqrt{\langle\phi|\,(\mathcal{P}_k\circ\mathcal{D}\circ\mathcal{P}_i)(\rho)\,|\phi\rangle\ \langle\psi|\,(\mathcal{P}_k\circ\mathcal{D}\circ\mathcal{P}_j)(\rho)\,|\psi\rangle}\,,
\end{aligned} \tag{A20}$$

where the right-hand side is 0 unless $i = j = k$ (cf. Lemma A2). Since the condition $|\,\langle\phi|\,\widetilde{\mathcal{D}}_k(\Pi_i\rho\Pi_j)\,|\phi\rangle| = 0$, $\forall|\phi\rangle \in \mathcal{H}_S$ implies the condition $\widetilde{\mathcal{D}}_k(\Pi_i\rho\Pi_j) = 0$, we obtained the relation

$$\widetilde{\mathcal{D}}_k(\Pi_i\rho\Pi_j) = 0 \qquad \text{unless} \quad i = j = k\,. \tag{A21}$$

Using this fact, we obtain the equality

$$\begin{aligned}
(\mathcal{P}_k\circ\mathcal{D})(\rho) &= \widetilde{\mathcal{D}}_k(\rho) \\
&= \sum_{i,j}\widetilde{\mathcal{D}}_k(\Pi_i\rho\Pi_j) \\
&= (\widetilde{\mathcal{D}}_k\circ\mathcal{P}_k)(\rho) \\
&= (\mathcal{P}_k\circ\mathcal{D}\circ\mathcal{P}_k)(\rho)\,.
\end{aligned} \tag{A22}$$

Since the equality holds for every ρ, this proves Equation (A16). □

Lemma A2 guarantees that the linear map $\mathcal{D}\circ\mathcal{P}_k$ sends $\mathsf{Lin}(\mathcal{R}_k\otimes\mathcal{M}_k)$ into itself. It is also easy to see that the map $\mathcal{D}\circ\mathcal{P}_k$ has a simple form:

Lemma A3. *For every channel $\mathcal{D} \in \mathsf{Chan}(A)'$, one has*

$$\mathcal{D}\circ\mathcal{P}_k = (\mathcal{I}_{A_k}\otimes\mathcal{B}_k)\circ\mathcal{P}_k \qquad \forall k, \tag{A23}$$

where $\mathcal{I}_{A_k}$ is the identity map from $\mathsf{Lin}(\mathcal{H}_{A_k})$ to itself, and $\mathcal{B}_k$ is a quantum channel from $\mathsf{Lin}(\mathcal{H}_{A_k})$ to itself.

Proof. Straightforward extension of the proof in Appendix B. □

Using the notion of adjoint, we can now prove the following

Lemma A4. *For every channel $\mathcal{D} \in \mathsf{Chan}(A)'$, the adjoint $\mathcal{D}^\dagger$ preserves the elements of the algebra A, namely $\mathcal{D}^\dagger(C) = C$ for all $C \in \mathsf{A}$.*

Proof. Let C be a generic element of A. By Equation (31), one has the equality

$$C = \bigoplus_k (C_k\otimes I_{B_k}) = \bigoplus_k \mathcal{P}_k(C). \tag{A24}$$

Using Lemma A3 and the definition of adjoint, we obtain

$$\begin{aligned}\mathrm{Tr}[\mathcal{D}^\dagger(C)\,\rho] &= \mathrm{Tr}[C\,\mathcal{D}(\rho)]\\ &= \sum_k \mathrm{Tr}[\mathcal{P}_k(C)\,\mathcal{D}(\rho)]\\ &= \sum_k \mathrm{Tr}[C\,(\mathcal{P}_k\circ\mathcal{D})(\rho)]\\ &= \sum_k \mathrm{Tr}[C\,(\mathcal{P}_k\circ\mathcal{D}\circ\mathcal{P}_k)(\rho)]\\ &= \sum_k \mathrm{Tr}\left[\mathcal{P}_k(C)\;(\mathcal{D}\circ\mathcal{P}_k)(\rho)\right]\\ &= \sum_k \mathrm{Tr}\left\{(C_k\otimes I_{B_k})\;[(\mathcal{I}_{A_k}\otimes\mathcal{B}_k)\circ\mathcal{P}_k](\rho)\right\},\end{aligned} \tag{A25}$$

having used Lemma A3 in the last equality. Then, we use the fact that the channel $\mathcal{B}_k$ is trace-preserving, and therefore its adjoint $\mathcal{B}_k^\dagger$ preserves the identity. Using this fact, we can continue the chain of equalities as

$$\begin{aligned}\mathrm{Tr}[\mathcal{D}^\dagger(C)] &= \sum_k \mathrm{Tr}\Big\{[C_k\otimes\mathcal{B}_k^\dagger(I_{B_k})]\;\mathcal{P}_k(\rho)\Big\}\\ &= \sum_k \mathrm{Tr}\left[(C_k\otimes I_{B_k})\;\mathcal{P}_k(\rho)\right]\\ &= \sum_k \mathrm{Tr}\left[\mathcal{P}_k(C_k\otimes I_{B_k})\;\rho\right]\\ &= \mathrm{Tr}\left[\left(\bigoplus_k C_k\otimes I_{B_k}\right)\;\rho\right]\\ &= \mathrm{Tr}[C\rho]\,,\end{aligned} \tag{A26}$$

having used Equation (A24) in the last equality. Since the equality holds for every density matrix ρ, we proved the equality $\mathcal{D}^\dagger(C) = C$. □

We are now in position to prove Theorem A1.

Proof of Theorem A1. Let $\mathcal{D}$ be a quantum channel in $\mathsf{Chan}(\mathsf{A})'$. Then, Lemma A4 guarantees that the adjoint $\mathcal{D}^\dagger$ preserves all operators in the algebra A. Then, a result due to Lindblad [86] guarantees that all the Kraus operators of $\mathcal{D}$ belong to the algebra A'. This proves the inclusion $\mathsf{Chan}(\mathsf{A})' \subseteq \mathsf{Chan}(\mathsf{A}')$.

The converse inclusion is immediate: if a channel $\mathcal{D}$ belongs to $\mathsf{Chan}(A')$, it commutes with all channels in $\mathsf{Chan}(\mathsf{A})$ thanks to the block diagonal form of the Kraus operators (cf. Equations (32) and (33)). □

Appendix C.2. States of Subsystems Associated to Finite Dimensional Von Neumann algebras

Here, we provide the proof of Proposition 5, adopting the notation $\mathsf{B} := \mathsf{A}'$.

The proof uses the following lemma:

Lemma A5 (No signalling condition)**.** *For every channel* $\mathcal{D} \in \mathsf{Chan}(\mathsf{B})$*, one has* $\mathrm{Tr}_\mathsf{B}\circ\mathcal{D} = \mathrm{Tr}_\mathsf{B}$.

Proof. By definition, the partial trace channel Tr_B can be written as

$$\mathrm{Tr}_\mathsf{B} = \bigoplus_k (\mathcal{I}_{A_k}\otimes\mathrm{Tr}_{B_k})\circ\mathcal{P}_k. \tag{A27}$$

For every channel $\mathcal{D} \in \mathsf{Chan}(\mathsf{B})$, we have

$$\begin{aligned}\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{D} &= \bigoplus_k (\mathcal{I}_{A_k} \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k \circ \mathcal{D} \\ &= \bigoplus_k (\mathcal{I}_{A_k} \otimes \mathrm{Tr}_{B_k}) \circ (\mathcal{I}_{A_k} \otimes \mathcal{B}_k) \circ \mathcal{P}_k \\ &= \bigoplus_k \Big[\mathcal{I}_{A_k} \otimes (\mathrm{Tr}_{B_k} \circ \mathcal{B}_k)\Big] \circ \mathcal{P}_k \\ &= \bigoplus_k (\mathcal{I}_{A_k} \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k \\ &= \mathrm{Tr}_{\mathsf{B}}, \end{aligned} \tag{A28}$$

where the second equality follows from Lemma A3, and the third equality follows from the fact that $\mathcal{B}_k$ is trace-preserving. □

Proof of Proposition 5. Suppose that ρ and σ are equivalent for A. By definition, this means that there exists a finite sequence $(\rho_1, \rho_2, \dots, \rho_n)$ such that

$$\rho_1 = \rho\,, \qquad \rho_n = \sigma\,, \qquad \text{and} \qquad \mathsf{Deg}_B(\rho_i) \cap \mathsf{Deg}_B(\rho_{i+1}) \neq \emptyset \quad \forall i \in \{1, 2, \dots, n-1\}\,. \tag{A29}$$

The condition of non-trivial intersection implies that, for every $i \in \{1, 2, \dots, n-1\}$, one has

$$\mathcal{D}_i\,(\rho_i) = \widetilde{\mathcal{D}}_i\,(\rho_{i+1})\,, \tag{A30}$$

where $\mathcal{D}_i$ and $\widetilde{\mathcal{D}}_i$ are two quantum channels in $\mathsf{Chan}(\mathsf{B})$. Tracing over B on both sides we obtain the relation

$$(\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{D}_i)\,(\rho_i) = (\mathrm{Tr}_{\mathsf{B}} \circ \widetilde{\mathcal{D}}_i)\,(\rho_{i+1})\,, \tag{A31}$$

and, thanks to Lemma A5, $\mathrm{Tr}_{\mathsf{B}}[\rho_i] = \mathrm{Tr}_{\mathsf{B}}[\rho_{i+1}]$. Since the equality holds for every $i \in \{1, \dots, n-1\}$, we obtained the condition $\mathrm{Tr}_{\mathsf{B}}[\rho] = \mathrm{Tr}_{\mathsf{B}}[\sigma]$. In summary, if two states ρ and σ are equivalent for A, then $\mathrm{Tr}_{\mathsf{B}}[\rho] = \mathrm{Tr}_{\mathsf{B}}[\sigma]$.

To prove the converse, it is enough to define the channel $\mathcal{D}_0 \in \mathsf{Chan}(\mathsf{B})$ as

$$\mathcal{D}_0(\rho) := \bigoplus_k \mathrm{Tr}_{B_k}[\mathcal{P}_k(\rho)] \otimes \beta_k\,, \tag{A32}$$

where each β_k is a fixed (but otherwise generic) density matrix in $\mathsf{Lin}(\mathcal{H}_{B_k})$. Now, if the equality $\mathrm{Tr}_{\mathsf{B}}[\rho] = \mathrm{Tr}_{\mathsf{B}}[\sigma]$ holds, then also the equality $\mathcal{D}_0(\rho) = \mathcal{D}_0(\sigma)$ holds. This proves that the intersection between $\mathsf{Deg}_B(\rho)$ and $\mathsf{Deg}_B(\sigma)$ is non-empty, and therefore ρ and σ are equivalent for A. □

Appendix C.3. Transformations of Subsystems Associated to Finite Dimensional von Neumann algebras

Here, we prove that all transformations of system S_A are of the form $\mathcal{A} = \bigoplus_k \mathcal{A}_k$, where each $\mathcal{A}_k$ is a quantum channel from $\mathsf{Lin}(\mathcal{H}_{A_k})$ to itself. The proof is based on the following lemmas:

Lemma A6. *For every channel $\mathcal{C} \in \mathsf{Chan}(\mathsf{A})$, one has the relation*

$$\mathcal{P}_k \circ \mathcal{C} = (\mathcal{A}_k \otimes \mathcal{I}_{B_k}) \circ \mathcal{P}_k\,, \tag{A33}$$

where $\mathcal{A}_k$ is a quantum channel from $\mathsf{Lin}(\mathcal{H}_{A_k})$ to itself.

Proof. Let

$$\mathcal{C}(\rho) = \sum_i C_i \rho C_i^\dagger , \qquad C_i = \bigoplus_k (C_{ik} \otimes I_{B_k}) \tag{A34}$$

be a Kraus representation of channel $\mathcal{C}$. The preservation of the trace amounts to the condition

$$\begin{aligned} I &= \sum_i C_i^\dagger C_i \\ &= \bigoplus_k \left(\sum_i C_{ik}^\dagger C_{ik} \otimes I_{B_k} \right) , \end{aligned} \tag{A35}$$

which implies

$$\sum_i C_{ik}^\dagger C_{I_k} = I_{A_k} \qquad \forall k . \tag{A36}$$

Now, we have

$$\begin{aligned} (\mathcal{P}_k \circ \mathcal{C})(\rho) &= \sum_i (C_{ik} \otimes I_{B_k}) \, \mathcal{P}_k(\rho) \, (C_{ik} \otimes I_{B_k})^\dagger \\ &= (\mathcal{A}_k \otimes \mathcal{I}_{B_k}) \left[\mathcal{P}_k(\rho) \right] , \end{aligned} \tag{A37}$$

where the channel $\mathcal{A}_k$ is defined as

$$\mathcal{A}_k(\sigma) := \sum_i C_{ik} \sigma C_{ik}^\dagger \qquad \forall \sigma \in \mathsf{Lin}(\mathcal{H}_{A_k}) . \tag{A38}$$

Since the density matrix ρ in Equation (A37) is arbitrary, we proved the relation $\mathcal{P}_k \circ \mathcal{C} = (\mathcal{A}_k \otimes \mathcal{I}_{B_k}) \circ \mathcal{P}_k$. □

Lemma A7. *For two channels $\mathcal{C}, \mathcal{C}' \in \mathsf{Chan}(\mathsf{A})$, let $\mathcal{A}_k$ and $\mathcal{A}'_k$ be the quantum channels defined in Lemma A6. Then, the following are equivalent:*

1. $\mathrm{Tr}_\mathsf{B} \circ \mathcal{C} = \mathrm{Tr}_\mathsf{B} \circ \mathcal{C}'$,
2. $\mathcal{A}_k = \mathcal{A}'_k$ *for every k.*

Proof. 2 $\Longrightarrow$ 1. For channel $\mathcal{C}$, we have

$$\begin{aligned} \mathrm{Tr}_\mathsf{B} \circ \mathcal{C} &= \bigoplus_k (\mathcal{I}_{A_k} \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k \circ \mathcal{C} \\ &= \bigoplus_k (\mathcal{I}_{A_k} \otimes \mathrm{Tr}_{B_k}) \circ (\mathcal{A}_k \otimes \mathcal{I}_{B_k}) \circ \mathcal{P}_k \\ &= \bigoplus_k (\mathcal{A}_k \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k . \end{aligned} \tag{A39}$$

Similarly, for channel $\mathcal{C}'$, we have

$$\mathrm{Tr}_\mathsf{B} \circ \mathcal{C}' = \bigoplus_k (\mathcal{A}'_k \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k . \tag{A40}$$

Clearly, if $\mathcal{A}_k$ and $\mathcal{A}'_k$ are equal for every k, then the partial traces $\mathrm{Tr}_\mathsf{B} \circ \mathcal{C}$ and $\mathrm{Tr}_\mathsf{B} \circ \mathcal{C}'$ are equal.

1 $\Longrightarrow$ 2. Suppose that partial traces $\mathrm{Tr}_\mathsf{B} \circ \mathcal{C}$ and $\mathrm{Tr}_\mathsf{B} \circ \mathcal{C}'$ are equal. Then, Equations (A39) and (A40) imply the equality

$$(\mathcal{A}_k \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k = (\mathcal{A}'_k \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k \qquad \forall k . \tag{A41}$$

In turn, the above equality implies $\mathcal{A}_k = \mathcal{A}'_k$, $\forall k$, as one can easily verify by applying both sides of Equation (A41) to a generic product operator $X_k \otimes Y_k$, with $X_k \in \mathsf{Lin}(\mathcal{H}_{A_k})$ and $Y_k \in \mathsf{Lin}(\mathcal{H}_{B_k})$. □

Lemma A8. *Two channels $\mathcal{C}, \mathcal{C}' \in \mathsf{Chan}(\mathsf{A})$ are equivalent for A if and only if $\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C} = \mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C}'$.*

Proof. Suppose that $\mathcal{C}$ and $\mathcal{C}'$ are equivalent for A. By definition, this means that there exists a finite sequence $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_n) \subset \mathsf{Chan}(\mathsf{A})$ such that

$$\mathcal{C}_1 = \mathcal{C}\,, \qquad \mathcal{C}_n = \mathcal{C}'\,, \qquad \mathsf{Deg}_B(\mathcal{C}_i) \cap \mathsf{Deg}_B(\mathcal{C}_{i+1}) \neq \emptyset \quad \forall i \in \{1, \ldots, n-1\}\,. \tag{A42}$$

This means that, for every i, there exist two channels $\mathcal{D}_i, \widetilde{\mathcal{D}}_i \in \mathsf{Chan}(\mathsf{B})$ such that

$$\mathcal{D}_i \circ \mathcal{C}_i = \widetilde{\mathcal{D}}_i \circ \mathcal{C}_{i+1}\,. \tag{A43}$$

Tracing over B on both sides, we obtain

$$\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{D}_i \circ \mathcal{C}_i = \mathrm{Tr}_{\mathsf{B}} \circ \widetilde{\mathcal{D}}_i \circ \mathcal{C}_{i+1}\,, \tag{A44}$$

and, using the no signalling condition of Lemma A5,

$$\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C}_i = \mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C}_{i+1}\,. \tag{A45}$$

Since the above relation holds for every i, we obtained the equality $\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C} = \mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C}'$.
Conversely, suppose that $\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C} = \mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C}'$. Then, Lemma A7 implies the equality

$$\mathcal{A}_k = \mathcal{A}'_k \qquad \forall k\,, \tag{A46}$$

where $\mathcal{A}_k$ and $\mathcal{A}'_k$ are the quantum channels defined in Lemma A6.
Now, let $\mathcal{D}_0$ be the channel in $\mathsf{Chan}(\mathsf{B})$ defined in Equation (A32). By definition, we have

$$\begin{aligned} \mathcal{D}_0 \circ \mathcal{C} &= \bigoplus_k (\mathcal{I}_{A_k} \otimes \beta_k\ \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k \circ \mathcal{C} \\ &= \bigoplus_k (\mathcal{I}_{A_k} \otimes \beta_k\ \mathrm{Tr}_{B_k}) \circ (\mathcal{A}_k \otimes \mathcal{I}_{B_k}) \circ \mathcal{P}_k \\ &= \bigoplus_k (\mathcal{A}_k \otimes \beta_k\ \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k\,. \end{aligned} \tag{A47}$$

Similarly, we have

$$\mathcal{D}_0 \circ \mathcal{C} = \bigoplus_k (\mathcal{A}'_k \otimes \beta_k\ \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k\,. \tag{A48}$$

Since $\mathcal{A}_k$ and $\mathcal{A}'_k$ are equal for every k, we conclude that $\mathcal{D}_0 \circ \mathcal{C}$ is equal to $\mathcal{D}_0 \circ \mathcal{C}'$. This means that the intersection between $\mathsf{Deg}(\mathcal{C})$ and $\mathsf{Deg}(\mathcal{C}')$ is non-empty, and, therefore $\mathcal{C}$ is equivalent to $\mathcal{C}'$ modulo B. □

Combining Lemmas A7 and A8, we obtain the following corollary:

Corollary A1. *For two channels $\mathcal{C}, \mathcal{C}' \in \mathsf{Chan}(\mathsf{A})$, let $\mathcal{A}_k$ and $\mathcal{A}'_k$ be the quantum channels defined in Lemma A6. Then, the following are equivalent:*

1. *$\mathcal{C}$ and $\mathcal{C}'$ are equivalent for A,*
2. *$\bigoplus_k \mathcal{A}_k = \bigoplus_k \mathcal{A}'_k$.*

Proof. By Lemma A8, $\mathcal{C}$ and $\mathcal{C}'$ are equivalent for A if and only if the condition $\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C} = \mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C}'$ holds. By Lemma A7, the condition $\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C} = \mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C}'$ holds if and only if one has $\mathcal{A}_k = \mathcal{A}'_k$ for every k. In turn, the latter condition holds if and only if the equality $\bigoplus_k \mathcal{A}_k = \bigoplus_k \mathcal{A}'_k$ holds. □

In summary, the transformations of system S_A are characterized as

$$\mathsf{Transf}(S_A) = \bigoplus_k \mathsf{Chan}(A_k)\,, \tag{A49}$$

where $\mathsf{Chan}(A_k)$ is the set of all quantum channels from $\mathsf{Lin}(\mathcal{H}_{A_k})$ to itself.

To conclude, we observe that the transformations of S_A act in the expected way. To this purpose, we consider the *restriction map*

$$\pi_{\mathsf{A}} : \mathsf{Chan}(\mathsf{A}) \to \bigoplus_{\mathsf{k}} \mathsf{Chan}(\mathsf{A_k})\,, \quad \mathcal{C} \mapsto \bigoplus_{\mathsf{k}} \mathcal{A}_{\mathsf{k}}\,, \tag{A50}$$

where $\mathcal{A}_k$ is defined as in Lemma A6.

Using the restriction map, we can prove the following propositions:

Proposition A2. *For every channel $\mathcal{C} \in \mathsf{Chan}(\mathsf{A})$, we have the relation*

$$\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C} = \pi_{\mathsf{A}}(\mathcal{C}) \circ \mathrm{Tr}_{\mathsf{B}}\,. \tag{A51}$$

In words, evolving system S with $\mathcal{C}$ and then computing the local state of system S_A is the same as computing the local state of system S_A and then evolving it with $\pi_{\mathsf{A}}(\mathcal{C})$.

Proof. Using Lemma A6, the proof is straightforward:

$$\begin{aligned}
\mathrm{Tr}_{\mathsf{B}} \circ \mathcal{C} &= \bigoplus_k (\mathcal{I}_{A_k} \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k \circ \mathcal{C} \\
&= \bigoplus_k (\mathcal{I}_{A_k} \otimes \mathrm{Tr}_{B_k}) \circ (\mathcal{A}_k \otimes \mathcal{I}_{B_k}) \circ \mathcal{P}_k \\
&= \bigoplus_k \mathcal{A}_k \circ (\mathcal{I}_{A_k} \otimes \mathrm{Tr}_{B_k}) \circ \mathcal{P}_k \\
&= \left(\bigoplus_k \mathcal{A}_k \right) \circ \left[\bigoplus_l (\mathcal{I}_{A_l} \otimes \mathrm{Tr}_{B_l}) \circ \mathcal{P}_l \right] \\
&= \pi_{\mathsf{A}}(\mathcal{C}) \circ \mathrm{Tr}_{\mathsf{B}}\,.
\end{aligned} \tag{A52}$$

□

Proposition A3. *For every pair of channels $\mathcal{C}_1, \mathcal{C}_2 \in \mathsf{Chan}(\mathsf{A})$, we have the homomorphism relation*

$$\pi_{\mathsf{A}}(\mathcal{C}_1 \circ \mathcal{C}_2) = \pi_{\mathsf{A}}(\mathcal{C}_1) \circ \pi_{\mathsf{A}}(\mathcal{C}_2)\,. \tag{A53}$$

Proof. Let us write the channels $\pi_{\mathsf{A}}(\mathcal{C}_1)$, $\pi_{\mathsf{A}}(\mathcal{C}_2)$, and $\pi_{\mathsf{A}}(\mathcal{C}_1 \circ \mathcal{C}_2)$ as

$$\pi_{\mathsf{A}}(\mathcal{C}_1) = \bigoplus_k \mathcal{A}_{1k}\,, \qquad \pi_{\mathsf{A}}(\mathcal{C}_2) = \bigoplus_k \mathcal{A}_{2k}\,, \qquad \text{and} \qquad \pi_{\mathsf{A}}(\mathcal{C}_1 \circ \mathcal{C}_2) = \bigoplus_k \mathcal{A}_{12k}\,. \tag{A54}$$

With this notation, we have

$$\begin{aligned}(\mathcal{A}_{12k} \otimes \mathcal{I}_{B_k}) \circ \mathcal{P}_k &= \mathcal{P}_k \circ \mathcal{C}_1 \circ \mathcal{C}_2 \\ &= (\mathcal{A}_{1k} \otimes \mathcal{I}_{B_k}) \circ \mathcal{P}_k \circ \mathcal{C}_2 \\ &= (\mathcal{A}_{1k} \otimes \mathcal{I}_{B_k}) \circ (\mathcal{A}_{2k} \otimes I_{B_k}) \circ \mathcal{P}_k \\ &= \left[(\mathcal{A}_{1k} \circ \mathcal{A}_{2k}) \otimes \mathcal{I}_{B_k}\right] \circ \mathcal{P}_k \qquad \forall k\,. \end{aligned} \tag{A55}$$

From the above equation, we obtain the equality $\mathcal{A}_{12k} = \mathcal{A}_{1k} \circ \mathcal{A}_{2k}$ for all k. In turn, this equality implies the desired result:

$$\begin{aligned}\pi_{\mathsf{A}}(\mathcal{C}_1) \circ \pi_{\mathsf{A}}(\mathcal{C}_2) &= \left(\bigoplus_k \mathcal{A}_{1k}\right) \circ \left(\bigoplus_l \mathcal{A}_{2l}\right) \\ &= \bigoplus_k \mathcal{A}_{1k} \circ \mathcal{A}_{2k} \\ &= \bigoplus_k \mathcal{A}_{12k} \\ &= \pi_{\mathsf{A}}(\mathcal{C}_1 \circ \mathcal{C}_2)\,. \end{aligned} \tag{A56}$$

□

Appendix D. Basis-Preserving and Multiphase-Covariant Channels

Appendix D.1. Proof of Theorem 1

Here, we prove that the monoid of multiphase covariant channels on S (denoted as $\mathsf{MultiPCov}(S)$) and the monoid of basis-preserving channels on S (denoted as $\mathsf{BPres}(S)$) are one the commutant of the other.

The proof uses a few lemmas, the first of which is fairly straightforward:

Lemma A9. $\mathsf{BPres}(S)' \subseteq \mathsf{MultiPCov}(S)$.

Proof. Every unitary channel of the form $\mathcal{U}_{\boldsymbol{\theta}} = U_{\boldsymbol{\theta}} \cdot U_{\boldsymbol{\theta}}^\dagger$ is basis-preserving, and therefore every channel $\mathcal{C}$ in the commutant of $\mathsf{BPres}(S)$ must commute with it. By definition, this means that $\mathcal{C}$ is multiphase covariant. □

To prove the converse inclusion, we use the following characterization of multiphase covariant channels:

Lemma A10 (Characterization of $\mathsf{MultiPCov}(S)$)**.** *A channel $\mathcal{M} \in \mathsf{Chan}(S)$ is multiphase covariant if and only if it has a Kraus representation of the form*

$$\mathcal{M}(\rho) = \sum_{i=1}^{r} M_i \rho M_i^\dagger + \sum_{k=1}^{d} \sum_{j \neq k} p(j|k)\, |j\rangle\langle k|\, \rho |k\rangle\langle j|\,, \tag{A57}$$

where each operator M_i is diagonal in the computational basis, and each $p(j|k)$ is non-negative.

Proof. Let $M \in \mathsf{Lin}(\mathcal{H}_S \otimes \mathcal{H}_S)$ be the Choi operator of channel $\mathcal{M}$. For a multiphase covariant channel, the Choi operator must satisfy the commutation relation [87,88]

$$[M, U_{\boldsymbol{\theta}} \otimes \overline{U}_{\boldsymbol{\theta}}] = 0 \qquad \forall \boldsymbol{\theta} \in [0, 2\pi)^{\otimes d}\,. \tag{A58}$$

This condition implies that M must have the form

$$M = \sum_{s,t} M_{ss,tt} \, |s\rangle\langle t| \otimes |s\rangle\langle t| + \sum_k \sum_{j \neq k} M_{jk,jk} \, |j\rangle\langle j| \otimes |k\rangle\langle k| \,, \tag{A59}$$

where the $d \times d$ matrix $[\Gamma_{s,t}] := [M_{ss,tt}]_{s,t \in \{1,\ldots,d\}}$ is positive semidefinite and each coefficient $M_{st,st}$ is non-negative. Then, Equation (A57) follows from diagonalizing the matrix Γ and using the relation $\mathcal{M}(\rho) = \mathrm{Tr}[M \, (I \otimes \rho^T)]$, where ρ^T is the transpose of ρ in the computational basis. □

From Equation (A57), one can show every multiphase covariant channel commutes with every basis-preserving channel:

Lemma A11. $\mathsf{MultiPCov}(S) \subseteq \mathsf{BPres}(S)'$.

Proof. Let $\mathcal{B} \in \mathsf{BPres}(S)$ be a generic basis-preserving channel, and let $\mathcal{M} \in \mathsf{MultiPCov}(S)$ be a generic multiphase covariant channel. Using the characterization of Equation (A57), we obtain

$$\begin{aligned}
\mathcal{M} \circ \mathcal{B}(\rho) &= \sum_i M_i \mathcal{B}(\rho) M_i^\dagger + \sum_k \sum_{j \neq k} p(j|k) |j\rangle\langle k| \mathcal{B}(\rho) |k\rangle\langle j| \\
&= \sum_i \mathcal{B}(M_i \rho M_i^\dagger) + \sum_k \sum_{j \neq k} p(j|k) |j\rangle\langle k| \mathcal{B}(\rho) |k\rangle\langle j| \\
&= \sum_i \mathcal{B}(M_i \rho M_i^\dagger) + \sum_k \sum_{j \neq k} p(j|k) |j\rangle \, \langle k|\rho|k\rangle \, \langle j| \\
&= \sum_i \mathcal{B}(M_i \rho M_i^\dagger) + \sum_k \sum_{j \neq k} p(j|k) \, \mathcal{B}(|j\rangle\langle j|) \, \langle k|\rho|k\rangle \\
&= \mathcal{B}\left(\sum_i M_i \rho M_i^\dagger + \sum_k \sum_{j \neq k} p(j|k) |j\rangle \, \langle k|\rho|k\rangle \, \langle j| \right) \\
&= \mathcal{B} \circ \mathcal{M}(\rho) \qquad \forall \rho \in \mathsf{Lin}(S) \,.
\end{aligned} \tag{A60}$$

The second equality used the fact that the Kraus operators of $\mathcal{B}$ are diagonal in the computational basis [71,72] and therefore commute with each operator M_i. The third equality uses the relation $\langle k|\mathcal{B}(\rho)|k\rangle = \langle k|\rho|k\rangle$, following from the fact that $\mathcal{B}$ preserves the computational basis [71,72]. □

Summarizing, we have shown that the multiphase covariant channels are the commutant of the basis-preserving channels:

Corollary A2. $\mathsf{MultiPCov}(S) = \mathsf{BPres}(S)'$.

Note that Corollary A2 implies the relation

$$\mathsf{MultiPCov}(S)' = \mathsf{BPres}(S)'' \supseteq \mathsf{BPres}(S) \,. \tag{A61}$$

To conclude the proof of Theorem 1, we prove the converse inclusion:

Lemma A12. $\mathsf{MultiPCov}(S)' \subseteq \mathsf{BPres}(S)$.

Proof. A special case of multiphase covariant channel is the erasure channel $\mathcal{M}_k$ defined by $\mathcal{M}_k(\rho) = |k\rangle\langle k|$ for every $\rho \in \mathsf{Lin}(S)$. For a generic channel $\mathcal{C} \in \mathsf{MultiPCov}(S)'$, one must have

$$\mathcal{C}(|k\rangle\langle k|) = \mathcal{C} \circ \mathcal{M}_k(|k\rangle\langle k|) = \mathcal{M}_k \circ \mathcal{C}(|k\rangle\langle k|) = |k\rangle\langle k| \,. \tag{A62}$$

Since the above condition must hold for every k, the channel $\mathcal{C}$ must be basis-preserving. □

Combining Lemma A12 and Equation (A61), we obtain:

Corollary A3. $\mathsf{MultiPCov}(S)' = \mathsf{BPres}(S)$.

Putting Corollaries A2 and A3 together, we have an immediate proof of Theorem 1.

Appendix D.2. Proof of Equation (55)

Here, we show that the transformations on system S_A are classical channels. To construct the transformations of S_A, we have to partition the double commutant of $\mathsf{Act}(A;S) = \mathsf{MultiPCov}(S)$ into equivalence classes.

First, recall that $\mathsf{MultiPCov}(S)'' = \mathsf{MultiPCov}(S)$ (by Theorem 1). Then, note the following property:

Lemma A13. *If two channels* $\mathcal{M}, \widetilde{\mathcal{M}} \in \mathsf{MultiPCov}(S)$ *satisfy the condition*

$$\langle k| \mathcal{M}(|j\rangle\langle j|) |k\rangle = \langle k| \widetilde{\mathcal{M}}(|j\rangle\langle j|) |k\rangle \,, \tag{A63}$$

then $[\mathcal{M}]_{A'} = [\widetilde{\mathcal{M}}]_{A'}$.

Proof. Define the completely dephasing channel $\mathcal{D} = \sum_k |k\rangle\langle k| \cdot |k\rangle\langle k|$. Clearly, $\mathcal{D}$ is basis-preserving. Using the idempotence relation $\mathcal{D} \circ \mathcal{D} = \mathcal{D}$, we obtain

$$\begin{aligned}
\Big(\mathcal{D} \circ \mathcal{M}\Big)(\rho) &= \Big(\mathcal{D} \circ \mathcal{D} \circ \mathcal{M}\Big)(\rho) \\
&= \Big(\mathcal{D} \circ \mathcal{M} \circ \mathcal{D}\Big)(\rho) \\
&= \Big(\mathcal{D} \circ \mathcal{M}\Big)\Big(\sum_j |j\rangle\langle j| \, \langle j|\rho|j\rangle\Big) \\
&= \sum_j \langle j|\rho|j\rangle \, \mathcal{D}\Big(\mathcal{M}(|j\rangle\langle j|)\Big) \\
&= \sum_{j,k} \langle j|\rho|j\rangle \, \langle k|\mathcal{M}(|j\rangle\langle j|)|k\rangle \, |k\rangle\langle k| \,.
\end{aligned} \tag{A64}$$

Likewise, we have

$$\Big(\mathcal{D} \circ \widetilde{\mathcal{M}}\Big)(\rho) = \sum_{j,k} \langle j|\rho|j\rangle \, \langle k|\widetilde{\mathcal{M}}(|j\rangle\langle j|)|k\rangle \, |k\rangle\langle k| \,. \tag{A65}$$

If condition (A63) holds, then the equality $\mathcal{D} \circ \mathcal{M} = \mathcal{D} \circ \widetilde{\mathcal{M}}$ holds, meaning that $\mathsf{Deg}(\mathcal{M})$ and $\mathsf{Deg}(\widetilde{\mathcal{M}})$ have non-empty intersection. Hence, $\mathcal{M}$ and $\widetilde{\mathcal{M}}$ must be in the same equivalence class. □

The converse of Lemma A13 holds:

Lemma A14. *If two channels* $\mathcal{M}, \widetilde{\mathcal{M}} \in \mathsf{MultiPCov}(S)$ *are in the same equivalence class, then they must satisfy condition (A63).*

Proof. If $\mathcal{M}$ and $\widetilde{\mathcal{M}}$ are in the same equivalence class, then there exists a finite sequence $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_n)$ such that

$$\mathcal{M}_1 = \mathcal{M} \,, \qquad \mathcal{M}_n = \widetilde{\mathcal{M}} \,, \qquad \forall i \in \{1, \ldots, n-1\} \; \exists \mathcal{B}_i, \widetilde{\mathcal{B}}_i \in \mathsf{BPres}(S) : \quad \mathcal{B}_i \circ \mathcal{M}_i = \widetilde{\mathcal{B}}_i \circ \mathcal{M}_{i+1} \,.$$

The above condition implies

$$l\langle k|\,\mathcal{M}_i(\rho)\,|k\rangle = \mathrm{Tr}[\mathcal{M}_i(\rho)\,|k\rangle\langle k|] = \langle k|\,\mathcal{B}_i\circ\mathcal{M}_i(\rho)\,|k\rangle = \langle k|\,\widetilde{\mathcal{B}}_i\circ\mathcal{M}_{i+1}(\rho)\,|k\rangle \\ = \langle k|\,\mathcal{M}_{i+1}(\rho)\,|k\rangle\,, \tag{A66}$$

for all $i\in\{1,\ldots,n-1\}$ and for all $\rho\in\mathsf{Lin}(\rho)$. In particular, choosing $\rho=|j\rangle\langle j|$ we obtain

$$\langle k|\,\mathcal{M}_i(|j\rangle\langle j|)\,|k\rangle = \langle k|\,\mathcal{M}_{i+1}(|j\rangle\langle j|)\,|k\rangle \qquad \forall i\in\{1,\ldots,n-1\}\,,\forall j,k\in\{1,\ldots,d\}\,. \tag{A67}$$

Hence, Equation (A63) follows. □

Appendix E. Classical Systems and the Resource Theory of Coherence

Here, we consider agents who have access to various types of free operations in the resource theory of coherence. We start from the types of operations that give rise to classical systems, and then show two examples that do not have this property.

Appendix E.1. Operations That Lead to Classical Subsystems

Consider the following monoids of operations

1. *Strictly incoherent operations [41],* i.e., quantum channels $\mathcal{T}$ with the property that, for every Kraus operator T_i, the map $\mathcal{T}_i(\cdot)=T_i\cdot T_i$ satisfies the condition $\mathcal{D}\circ\mathcal{T}_i=\mathcal{T}_i\circ\mathcal{D}$, where $\mathcal{D}$ is the completely dephasing channel.
2. *Dephasing covariant operations* [38–40], i.e., quantum channels $\mathcal{T}$ satisfying the condition $\mathcal{D}\circ\mathcal{T}=\mathcal{T}\circ\mathcal{D}$.
3. *Phase covariant channels* [40], i.e., quantum channels $\mathcal{T}$ satisfying the condition $\mathcal{T}\circ\mathcal{U}_\varphi=\mathcal{U}_\varphi\circ\mathcal{T}$, $\forall\varphi\in[0,2\pi)$, where $\mathcal{U}_\varphi$ is the unitary channel associated with the unitary matrix $U_\varphi=\sum_k e^{ik\varphi}\,|k\rangle\langle k|$.
4. *Physically incoherent operations* [38,39], i.e., quantum channels that are convex combinations of channels $\mathcal{T}$ admitting a Kraus representation where each Kraus operator T_i is of the form

$$T_i = U_{\pi_i}\,U_{\boldsymbol{\theta}_i}\,P_i\,, \tag{A68}$$

   where U_{π_i} is a unitary that permutes the elements of the computational basis, $U_{\boldsymbol{\theta}_i}$ is a diagonal unitary, and P_i is a projector on a subspace spanned by a subset of vectors in the computational basis.
5. *Classical channels* i.e., channels satisfying $\mathcal{T}=\mathcal{D}\circ\mathcal{T}\circ\mathcal{D}$.

We now show that all the above operations define classical subsystems according to our construction.

The first ingredient in the proof is the observation that each of the monoids 1–5 contains the monoid of classical channels. Then, we can apply the following lemma:

Lemma A15. *Let* $\mathsf{M}\subseteq\mathsf{Chan}(\mathsf{S})$ *be a monoid of quantum channels, and let* M' *be its commutant. If* M *contains the monoid of classical channels, then* M' *is contained in the set of basis-preserving channels.*

Proof. Consider the erasure channel $\mathcal{C}_k$ defined by $\mathcal{C}_k(\rho):=|k\rangle\langle k|\,\mathrm{Tr}[\rho]$, $\forall\rho\in\mathsf{Lin}(\mathcal{H}_S)$. Clearly, the erasure channel is a classical channel. Then, every channel $\mathcal{B}\in\mathsf{M}'$ must satisfy the condition

$$\mathcal{B}(|k\rangle\langle k|)=\mathcal{B}\circ\mathcal{C}_k(|k\rangle\langle k|)=\mathcal{C}_k\circ\mathcal{B}(|k\rangle\langle k|)=|k\rangle\langle k|\,. \tag{A69}$$

Since k is generic, this implies that $\mathcal{B}$ must be basis-preserving. □

Furthermore, we have the following

Lemma A16. *Let* $\mathsf{Act}(A;S) \subseteq \mathsf{Chan}(S)$ *be a set of quantum channels that contains the monoid of classical channels. If two quantum states* $\rho, \sigma \in \mathsf{St}(S)$ *are equivalent for* A*, then they must have the same diagonal entries. Equivalently, they must satisfy* $\mathcal{D}(\rho) = \mathcal{D}(\sigma)$*.*

Proof. Same as the first part of the proof of Proposition 7. Suppose that Condition 1 holds, meaning that there exists a sequence $(\rho_1, \rho_2, \dots, \rho_n)$ such that

$$\rho_1 = \rho\,, \qquad \rho_n = \sigma\,, \qquad \forall i \in \{1, \dots, n-1\}\; \exists \mathcal{B}_i\,, \widetilde{\mathcal{B}}_i \in \mathsf{Act}(B;S) :\; \mathcal{B}_i(\rho_i) = \widetilde{\mathcal{B}}_i(\rho_{i+1})\,, \tag{A70}$$

where $\mathcal{B}_i$ and $\widetilde{\mathcal{B}}_i$ are channels in the commutant $\mathsf{Act}(A;S)'$. The above equation implies

$$\langle k|\mathcal{B}_i(\rho_i)|k\rangle = \langle k|\widetilde{\mathcal{B}}_i(\rho_{i+1})|k\rangle\,. \tag{A71}$$

Now, we know that the commutant $\mathsf{Act}(A;S)'$ consists of basis-preserving channels (Lemma A15). Since every basis-preserving channel satisfies the relation $\langle k|\mathcal{B}(\rho)|k\rangle = \langle k|\rho|k\rangle$ [71,72], we obtain that all the density matrices $(\rho_1, \rho_2, \dots, \rho_n)$ must have the same diagonal entries, namely $\mathcal{D}(\rho_1) = \mathcal{D}(\rho_2) = \cdots = \mathcal{D}(\rho_n)$. □

Now, we observe that the completely dephasing channel $\mathcal{D}$ is contained in the commutant of all the monoids 1–5. This fact is evident for the monoids 1, 2 and 5, where the commutation with $\mathcal{D}$ holds by definition. For the monoid 3, the commutation with $\mathcal{D}$ has been proven in [38,39], and for the monoid 4 it has been proven in [40].

Since $\mathcal{D}$ is contained in the commutant of all the monoids 1–5, we can use the following obvious fact:

Lemma A17. *Let* $\mathsf{Act}(A;S) \subseteq \mathsf{Chan}(S)$ *be a monoid of quantum channels and suppose that its commutant* $\mathsf{Act}(A;S)'$ *contains the dephasing channel* $\mathcal{D}$*. If two quantum states* $\rho, \sigma \in \mathsf{St}(S)$ *satisfy* $\mathcal{D}(\rho) = \mathcal{D}(\sigma)$*, then they are equivalent for* A*.*

Proof. Trivial consequence of the definition. □

Combining Lemmas A16 and A17, we obtain the following

Proposition A4. *Let* $\mathsf{Act}(A;S) \subseteq \mathsf{Chan}(S)$ *be a monoid of quantum channels on system* S*. If* $\mathsf{Act}(A;S)$ *contains the monoid of classical channels, and if the the commutant* $\mathsf{Act}(A;S)'$ *contains the completely dephasing channel* $\mathcal{D}$*, then two states* $\rho, \sigma \in \mathsf{St}(S)$ *are equivalent for* A *if and only if* $\mathcal{D}(\rho) = \mathcal{D}(\sigma)$*.*

Proof. Same as the proof of Proposition 7. □

Proposition A4 implies that the states of the subsystem S_A are in one-to-one correspondence with diagonal density matrices. Since the conditions of the proposition are satisfied by all the monoids 1–5, each of these monoids defines the same state space.

The same result holds for the transformations:

Proposition A5. *Let* $\mathsf{Act}(A;S) \subseteq \mathsf{Chan}(S)$ *be a monoid of quantum channels. If* $\mathsf{Act}(A;S)$ *contains the monoid of classical channels, and if the the commutant* $\mathsf{Act}(A;S)'$ *contains the completely dephasing channel* $\mathcal{D}$*, then two transformations* $\mathcal{S}, \mathcal{T} \in \mathsf{Transf}(S)$ *are equivalent for* A *if and only if* $\mathcal{D} \circ \mathcal{T} \circ \mathcal{D} = \mathcal{D} \circ \mathcal{T} \circ \mathcal{D}$*.*

Proof. Same as the proofs of Lemmas A13 and A14. □

Proposition A5 implies that the transformations of subsystem S_A can be identified with classical channels. Hence, system S_A is exactly the d-dimensional classical subsystem of the quantum system S. In summary, each of the monoids 1–5 defines the same d-dimensional classical subsystem.

Appendix E.2. Operations That Do Not Lead to Classical Subsystems

Here, we show that our construction does not associate classical subsystems with the monoids of incoherent and maximally incoherent operations. To start with, we recall the definitions of these two subsets:

1. The *maximally incoherent operations* are the quantum channels $\mathcal{T}$ that map diagonal density matrices to diagonal density matrices, namely $\mathcal{T} \circ \mathcal{D} = \mathcal{D} \circ \mathcal{T} \circ \mathcal{D}$, where $\mathcal{D}$ is the completely dephasing channel.
2. The *Incoherent operations* are the quantum channels $\mathcal{T}$ with the property that, for every Kraus operator T_i, the map $\mathcal{T}_i(\cdot) = T_i \cdot T_i$ sends diagonal matrices to diagonal matrices, namely $\mathcal{T}_i \circ \mathcal{D} = \mathcal{D} \circ \mathcal{T}_i \circ \mathcal{D}$.

Note that each set of operations contains the set of classical channels. Hence, the commutant of each set of operation consists of (some subset of) basis-preserving channels (by Lemma A15).

Moreover, both sets of operations 1 and 2 contain the set of quantum channels $\mathcal{C}_\psi$ defined by the relation

$$\mathcal{C}_\psi(\rho) = |1\rangle\langle 1| \, \langle\psi|\rho|\psi\rangle + \frac{I - |1\rangle\langle 1|}{d-1} \, \mathrm{Tr}[(I - |\psi\rangle\langle\psi|)\, \rho] \qquad \forall \rho \in \mathsf{Lin}(\mathcal{H}_S)\,, \tag{A72}$$

where $|\psi\rangle \in \mathcal{H}_S$ is a fixed (but otherwise arbitrary) unit vector. The fact that both monoids contain the channels $\mathcal{C}_\psi$ implies a strong constraint on their commutants:

Lemma A18. *The only basis-preserving quantum quantum channel $\mathcal{B} \in \mathsf{BPres}(S)$ satisfying the property $\mathcal{B} \circ \mathcal{C}_\psi = \mathcal{C}_\psi \circ \mathcal{B}$ for every $|\psi\rangle \in \mathcal{H}_S$ is the identity channel.*

Proof. The commutation property implies the relation

$$\begin{aligned} (\mathcal{C}_\psi \circ \mathcal{B})\,(|\psi\rangle\langle\psi|) &= (\mathcal{B} \circ \mathcal{C}_\psi)\,(|\psi\rangle\langle\psi|) \\ &= \mathcal{B}(|1\rangle\langle 1|) \\ &= |1\rangle\langle 1|\,, \end{aligned} \tag{A73}$$

where we used the fact that $\mathcal{B}$ is basis-preserving. Tracing both sides of the equality with the projector $|1\rangle\langle 1|$, we obtain the relation

$$\begin{aligned} 1 &= \langle 1|(\mathcal{C}_\psi \circ \mathcal{B})\,(|\psi\rangle\langle\psi|)|1\rangle \\ &= \langle\psi|\,\mathcal{B}(|\psi\rangle\langle\psi|)\,|\psi\rangle\,, \end{aligned} \tag{A74}$$

the second equality following from the definition of channel $\mathcal{C}_\psi$. In turn, Equation (A74) implies the relation $\mathcal{B}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$. Since $|\psi\rangle$ is arbitrary, this means that $\mathcal{B}$ must be the identity channel. □

In summary, the commutant of the set of incoherent channels consists only of the identity channel, and so is the the commutant of the set of maximally incoherent channels. Since the commutant is trivial, the equivalence classes are trivial, meaning that the subsystem S_A has exactly the same states and the same transformations of the original system S. In short, the subsystem associated with the incoherent (or maximally incoherent) channels is the full quantum system.

Appendix F. Enriching the Sets of Transformations

Here, we provide a mathematical construction that enlarges the sets of transformations in the "baby category" with objects S, S_A, and S_B. This construction provides a realization of a catagorical structure known as splitting of idempotents [73,74].

As we have seen in the main text, our basic construction does not provide transformations from the subsystem S_A to the global system S. One could introduce such transformations by hand, by defining an *embedding* [63]:

Definition A1. *An* embedding *of S_A into S is a map $\mathcal{E}_A : \mathsf{St}(S_A) \to \mathsf{St}(S)$ satisfying the property*

$$\mathrm{Tr}_B \circ \mathcal{E}_A = \mathcal{I}_{S_A} . \tag{A75}$$

In other words, $\mathcal{E}_A$ associates a representative to every equivalence class $\rho \in \mathsf{St}(S_A)$.

A priori, embeddings need not be physical processes. Consider the example of a classical system, viewed as a subsystem of a closed quantum system as in Section 4.3. An embedding would map each classical probability distribution $(p_1, p_2, \dots, p_d)$ into a pure quantum state $|\psi\rangle = \sum_k c_k |k\rangle$ satisfying the condition $|c_k|^2 = p_k$ for all $k \in \{1, \dots, d\}$. If the embedding were a physical transformation, there would be a way to physically transform every classical probability distributions into a corresponding pure quantum state, a fact that is impossible in standard quantum theory.

When building a new physical theory, one could *postulate* that there exists an embedding $\mathcal{E}_A$ that is physically realizable. In that case, the transformations from S_A to S would be those in the set

$$\mathsf{Transf}(S_A \to S) = \Big\{ \mathcal{T} \circ \mathcal{E}_A \ : \quad \mathcal{T} \in \mathsf{Transf}(S) \Big\} , \tag{A76}$$

and similarly for the transformations from S_B to S. The transformations from S_A to S_B would be those in the set

$$\mathsf{Transf}(S_A \to S_B) = \Big\{ \mathrm{Tr}_A \circ \mathcal{T} \circ \mathcal{E}_A \ : \quad \mathcal{T} \in \mathsf{Transf}(S) \Big\} , \tag{A77}$$

and similarly for the transformations from S_B to S_A. In that new theory, the old set of transformations from S_A should be replaced by the new set:

$$\widetilde{\mathsf{Transf}}(S_A) = \Big\{ \mathrm{Tr}_B \circ \mathcal{T} \circ \mathcal{E}_A \ : \quad \mathcal{T} \in \mathsf{Transf}(S) \Big\} , \tag{A78}$$

so that the structure of category is preserved. Similarly, the old set of transformations from S_B to S_B should be replaced by the new set .

$$\widetilde{\mathsf{Transf}}(S_B) = \Big\{ \mathrm{Tr}_A \circ \mathcal{T} \circ \mathcal{E}_B \ : \quad \mathcal{T} \in \mathsf{Transf}(S) \Big\} . \tag{A79}$$

When this is done, the embeddings define two idempotent morphisms $\mathcal{P}_A := \mathcal{E}_A \circ \mathrm{Tr}_B$ and $\mathcal{P}_B := \mathcal{E}_B \circ \mathrm{Tr}_A$, i.e., two morphisms satisfying the conditions

$$\mathcal{P}_A \circ \mathcal{P}_A = \mathcal{P}_A \qquad \text{and} \qquad \mathcal{P}_B \circ \mathcal{P}_B = \mathcal{P}_B . \tag{A80}$$

The partial trace and the embedding define a *splitting of idempotents*, in the sense of Refs. [73,74]. The splitting of idempotents was considered in the categorical framework as a way to define general decoherence maps, and, more specifically, decoherence maps to classical subsystems [74,89].

Appendix G. The Total System as a Subsystem

For every system satisfying the Non-Overlapping Agents Requirement, the system S can be regarded as a subsystem:

Proposition A6. *Let S be a system satisfying the Non-Overlapping Agents Requirement, let $A_{\max}$ be the maximal agent, and $S_{A_{\max}}$ be the associated subsystem. Then, one has $S_{A_{\max}} \simeq S$, meaning that there exist two isomorphisms $\gamma : \mathsf{St}(S) \to \mathsf{St}\,(S_{A_{\max}})$ and $\delta : \mathsf{Transf}(S) \to \mathsf{Transf}\,(S_{A_{\max}})$ satisfying the condition*

$$\gamma(\mathcal{T}\psi) = \delta(\mathcal{T})\,\gamma(\psi)\,, \qquad \forall \psi \in \mathsf{St}(S)\,, \forall \mathcal{T} \in \mathsf{Transf}(S)\,. \tag{A81}$$

Proof. The Non-Overlapping Agents Requirement guarantees that the commutant $\mathsf{Act}(A_{\max}; S)'$ contains only the identity transformation. Hence, the equivalence class $[\psi]_{A_{\max}}$ contains only the state ψ. Hence, the partial trace $\mathrm{Tr}_{A'_{\max}} : \psi \mapsto [\psi]_{A_{\max}}$ is a bijection from $\mathsf{St}(S)$ to $\mathsf{St}\,(S_{A_{\max}})$. Similarly, the equivalence class $[\mathcal{T}]_{A_{\max}}$ contains only the transformation $\mathcal{T}$. Hence, the restriction $\pi_{A_{\max}} : \mathcal{T} \mapsto [\mathcal{T}]_{A_{\max}}$ is a bijective function between $\mathsf{Transf}(S)$ and $\mathsf{Transf}\,(S_{A_{\max}})$. Such a function is an homomorphism of monoids, by Equation (20). Setting $\delta := \pi_{A_{\max}}$ and $\gamma := \mathrm{Tr}_{A'_{\max}}$, the condition (A81) is guaranteed by Equation (21). □

Appendix H. Proof of Proposition 15

By definition, the condition $\mathrm{Tr}_B[\psi] = \mathrm{Tr}_B[\psi']$ holds if and only if there exists a finite sequence $(\psi_1, \psi_2, \dots, \psi_n)$ such that

$$\psi_1 = \psi\,, \qquad \psi_n = \psi'\,, \qquad \forall i \in \{1, \dots, n-1\} \quad \exists \mathcal{V}_i\,, \widetilde{\mathcal{V}}_i \in \mathsf{Act}(B; S) : \; \mathcal{V}_i \psi_i = \widetilde{\mathcal{V}}_i \psi_{i+1}\,. \tag{A82}$$

Our goal is to prove that there exists an adversarial action $\mathcal{V}_B \in \mathsf{Act}(B; S)$ such that the relation $\psi' = \mathcal{V}_B \psi$ or $\psi = \mathcal{V}_B \psi'$ holds.

We will proceed by induction on n, starting from the base case $n = 2$. In this case, we have $\mathsf{Deg}_B(\psi) \cap \mathsf{Deg}_B(\psi') \neq \emptyset$. Then, the first regularity condition implies that there exists a transformation $\mathcal{V}_B \in \mathsf{Act}(B; S)$ such that at least one of the relations $\mathcal{V}_B \psi = \psi'$ and $\psi = \mathcal{V}_B \psi'$ holds. This proves the validity of the base case.

Now, suppose that the induction hypothesis holds for all sequences of length n, and suppose that ψ and ψ' are equivalent through a sequence of length $n+1$, say $(\psi_1, \psi_2, \dots, \psi_n, \psi_{n+1})$. Applying the induction hypothesis to the sequence $(\psi_1, \psi_2, \dots, \psi_n)$, we obtain that there exists a transformation $\mathcal{V} \in \mathsf{Act}(B; S)$ such that at least one of the relations $\psi_n = \mathcal{V}\psi$ and $\psi = \mathcal{V}\psi_n$ holds. Moreover, applying the induction hypothesis to the pair (ψ_n, ψ_{n+1}) we obtain that there exists a transformation $\mathcal{V}' \in \mathsf{Act}(B; S)$ such that $\psi_{n+1} = \mathcal{V}'\psi_n$, or $\psi_n = \mathcal{V}'\psi_{n+1}$. Hence, there are four possible cases:

1. $\psi_n = \mathcal{V}\psi$ and $\psi_{n+1} = \mathcal{V}'\psi_n$. In this case, we have $\psi_{n+1} = (\mathcal{V}' \circ \mathcal{V})\psi$, which proves the desired statement.
2. $\psi_n = \mathcal{V}\psi$ and $\psi_n = \mathcal{V}'\psi_{n+1}$. In this case, we have $\mathcal{V}\psi = \mathcal{V}'\psi_{n+1}$, or equivalently $\mathsf{Deg}_B(\psi) \cap \mathsf{Deg}_B(\psi_{n+1}) \neq \emptyset$. Applying the induction hypothesis to the sequence (ψ, ψ_{n+1}), we obtain the desired statement.
3. $\psi = \mathcal{V}\psi_n$ and $\psi_{n+1} = \mathcal{V}'\psi_n$. Using the second regularity condition, we obtain that there exists a transformation $\mathcal{W} \in \mathsf{Act}(B; S)$ such that at least one of the relations $\mathcal{V} = \mathcal{W} \circ \mathcal{V}'$ and $\mathcal{V}' = \mathcal{W} \circ \mathcal{V}$ holds. Suppose that $\mathcal{V} = \mathcal{W} \circ \mathcal{V}'$. In this case, we have

$$\psi = \mathcal{V}\psi_n = (\mathcal{W} \circ \mathcal{V}')\psi_n = \mathcal{W}\psi_{n+1}\,. \tag{A83}$$

Alternatively, suppose that $\mathcal{V}' = \mathcal{W} \circ \mathcal{V}$. In this case, we have

$$\psi_{n+1} = \mathcal{V}'\psi_n = (\mathcal{W} \circ \mathcal{V})\psi_n = \mathcal{W}\psi\,. \tag{A84}$$

In both cases, we proved the desired statement.
4. $\psi = \mathcal{V}\psi_n$ and $\psi_n = \mathcal{V}'\psi_{n+1}$. In this case, we have $\psi = (\mathcal{V} \circ \mathcal{V}')\psi_{n+1}$, which proves the desired statement.

□

Appendix I. Characterization of the Adversarial Group

Here, we provide the proof of Theorem 3, proving a canonical decomposition of the elements of the adversarial group. The proof proceeds in a few steps:

Lemma A19 (Canonical form of the elements of the adversarial group)**.** *Let $U : g \mapsto U_g$ be a projective representation of the group G, let $\mathsf{Irr}(U)$ be the set of irreducible representations contained in the isotypic decomposition of U, and let $\omega : \mathsf{G} \to \mathbb{C}$ be a multiplicative character of G. Then, the commutation relation*

$$V U_g = \omega(g)\, U_g V \qquad \forall g \in \mathsf{G} \tag{A85}$$

holds iff

1. *The map $U^{(j)} \mapsto \omega\, U^{(j)}$ is a permutation of the set $\mathsf{Irr}(U)$, denoted as $\pi : \mathsf{Irr}(U) \to \mathsf{Irr}(U)$. In other words, for every irrep $U^{(j)}$ with $j \in \mathsf{Irr}(U)$, the irrep $\omega\, U^{(j)}$ is equivalent to an irrep $k \in \mathsf{Irr}(U)$, and the correspondence between j and k is bijective.*
2. *The multiplicity spaces $\mathcal{M}_j$ and $\mathcal{M}_{\pi(j)}$ have the same dimension.*
3. *The unitary operator V has the canonical form $V = U_\pi V_0$, where V_0 is an unitary operator in the commutant U' and U_π is a permutation operator satisfying*

$$U_\pi\Big(\mathcal{R}_j \otimes \mathcal{M}_j\Big) = \Big(\mathcal{R}_{\pi(j)} \otimes \mathcal{M}_{\pi(j)}\Big) \qquad \forall j \in \mathsf{Irr}(U)\,. \tag{A86}$$

Proof. Let us use the isotypic decomposition of U, as in Equation (88). We define

$$V_{j,k} := \Pi_j\, V\, \Pi_k\,, \tag{A87}$$

where Π_j (Π_k) is the projector onto $\mathcal{R}_j \otimes \mathcal{M}_j$ ($\mathcal{R}_k \otimes \mathcal{M}_k$). Then, Equation (A85) is equivalent to the condition

$$V_{j,k}\left(U_g^{(k)} \otimes I_{\mathcal{M}_k}\right) = \omega(g)\left(U_g^{(j)} \otimes I_{\mathcal{M}_j}\right) V_{jk}\,, \qquad \forall g \in \mathsf{G}\,, \forall j,k\,, \tag{A88}$$

which in turn is equivalent to the condition

$$\langle\alpha|V_{j,k}|\beta\rangle\; U_g^{(k)} = \omega(g)\, U_g^{(j)}\, \langle\alpha|V_{j,k}|\beta\rangle\,, \qquad \forall g \in \mathsf{G}\,, \forall j,k\,, \forall|\alpha\rangle \in \mathcal{M}_j\,, \forall|\beta\rangle \in \mathcal{M}_k\,, \tag{A89}$$

where $\langle\alpha|V_{j,k}|\beta\rangle$ is a shorthand for the partial matrix element $(I_{\mathcal{R}_j} \otimes \langle\alpha|)\, V_{j,k}\, (I_{\mathcal{R}_k} \otimes |\beta\rangle)$.

Equation (A89) means that each operator $\langle\alpha|V_{j,k}|\beta\rangle$ intertwines the two representations $U^{(k)}$ and $\omega\, U^{(j)}$. Recall that each representation is irreducible. Hence, the second Schur's lemma [78] implies that $\langle\alpha|\, V_{j,k}\, |\beta\rangle$ is zero if the two representations are not equivalent. Note that there can be *at most* one value of j such that $U^{(k)}$ is equivalent to $\omega\, U^{(j)}$. If such a value exists, we denote it as $j = \pi(k)$. By construction, the function $\pi : \mathsf{Irr}(U) \to \mathsf{Irr}(U)$ must be injective.

When $j = \pi(k)$, the first Schur's lemma [78] guarantees that the operator $\langle\alpha|\, V_{\pi(k),k}|\beta\rangle$ is proportional to the partial isometry $T_{\pi(k),k}$ that implements the equivalence of the two representations. Let us write

$$\langle\alpha|\, V_{\pi(k),k}\, |\beta\rangle = M_{\alpha,\beta}\, T_{\pi(k),k}\,, \tag{A90}$$

for some $M^{(k)}_{\alpha,\beta} \in \mathbb{C}$. Note also that, since the left-hand side is sesquilinear in $|\alpha\rangle$ and $|\beta\rangle$, the right-hand side should also be sesquilinear. Hence, we can find an operator $M_{\pi(k),k} : \mathcal{M}_k \to \mathcal{M}_{\pi(k)}$ such that $M^{(k)}_{\alpha,\beta} = \langle\alpha| M_{\pi(k),k} |\beta\rangle$. Putting everything together, the operator V can be written as

$$V = \bigoplus_{k \in \mathsf{Irr}(U)} \Big(T_{\pi(k),k} \otimes M_{\pi(k),k} \Big) . \tag{A91}$$

Now, the operator V must be unitary, and, in particular, it should satisfy the condition $VV^\dagger = I$, which reads

$$\bigoplus_{k \in \mathsf{Irr}(U)} \Big(I_{\mathcal{R}_{\pi(k)}} \otimes M_{\pi(k),k} M^\dagger_{\pi(k),k} \Big) = I . \tag{A92}$$

The above condition implies that: (i) the function π must be surjective, and (ii) the operator $M_{\pi(k),k}$ must be a co-isometry. From the relation $V^\dagger V$, we also obtain that $M_{\pi(k),k}$ must be an isometry. Hence, $M_{\pi(k)}$ is unitary.

Summarizing, the condition (A85) can be satisfied only if there exists a permutation $\pi : \mathsf{Irr}(U) \to \mathsf{Irr}(U)$ such that, for every j,

1. the irreps $\omega\, U^{(k)}$ and $U^{\pi(k)}$ are equivalent,
2. the multiplicity spaces $\mathcal{M}_k$ and $\mathcal{M}_{\pi(k)}$ are unitarily isomorphic.

Fixing a unitary isomorphism $S_{\pi(k),k} : \mathcal{M}_k \to \mathcal{M}_{\pi(k)}$, we can write every element of the adversarial group in the canonical form $V = U_\pi V_0$, where U_π is the permutation operator

$$U_\pi = \bigoplus_{k \in \mathsf{Irr}(U)} \Big(T_{\pi(k),k} \otimes S_{\pi(k),k} \Big) , \tag{A93}$$

and V_0 is an element of the commutant U', i.e., a generic unitary operator of the form

$$V_0 = \bigoplus_{k \in \mathsf{Irr}(U)} \Big(I_j \otimes V_{0,k} \Big) . \tag{A94}$$

Conversely, if a permutation π exists with the properties that for every $k \in \mathsf{Irr}(U)$

1. $\omega\, U^{(k)}$ and $U^{(\pi(k))}$ are equivalent irreps,
2. $\mathcal{M}_k$ and $\mathcal{M}_{\pi(k)}$ are unitarily equivalent,

and if the operator V has the form $V = U_\pi V_0$, with U_π and V_0 as in Equations (A93) and (A94), then V satisfies the commutation relation (A85). □

We have seen that every element of the adversarial group can be decomposed into the product of a permutation operator, which permutes the irreps, and an operator in the commutant of the original group representation $U : \mathsf{G} \to \mathsf{Lin}(\mathcal{H})$. We now observe that the allowed permutations have an additional structure: they must form an Abelian group, denoted as A.

Lemma A20. *The permutations π arising from Equation (A85) with a generic multiplicative character $\omega(V, \cdot)$ form an Abelian subgroup A of the group of all permutations of $\mathsf{Irr}(U)$.*

Proof. Let V and W be two elements of the adversarial group G_B, let $\omega(V, \cdot)$ and $\omega(W, \cdot)$ be the corresponding characters, and let π_V and π_W be the permutations associated with $\omega(V, \cdot)$ and $\omega(W, \cdot)$ as in Theorem A19, i.e., through the relation

$$\begin{aligned} j = \pi_V(k) \quad &\Longleftrightarrow \quad U^{(j)} \text{ is equivalent to } \omega(V, \cdot)\, U^{(k)}, \\ j = \pi_W(k) \quad &\Longleftrightarrow \quad U^{(j)} \text{ is equivalent to } \omega(W, \cdot)\, U^{(k)} . \end{aligned} \tag{A95}$$

Now, the element VW is associated with the permutation $\pi_V \circ \pi_W$, while the element WV is associated with the permutation $\pi_W \circ \pi_V$. On the other hand, the characters obey the equality

$$\omega(VW, g) = \omega(V, g)\omega(W, g) = \omega(WV, g) \qquad \forall g \in \mathsf{G}\,. \tag{A96}$$

Hence, we conclude that $\pi_V \circ \pi_W$ and $\pi_W \circ \pi_V$ are, in fact, the same permutation. Hence, the elements of the adversarial group must correspond to an Abelian subgroup of the permutations of $\mathsf{Irr}(U)$. □

Combining Lemmas A19 and A20, we can now prove Theorem 3.

Proof of Theorem 3. For different permutations in A, we can choose the isomorphisms $S_{\pi(k),k} : \mathcal{M}_k \to \mathcal{M}_{\pi(k)}$ such that the following property holds:

$$S_{\pi_2 \circ \pi_2(k),k} = S_{\pi_2(\pi_1(k)),\pi_1(k)}\, S_{\pi_1(k),k}\,, \qquad \forall \pi_1, \pi_2 \in \mathsf{A}\,. \tag{A97}$$

When this is done, the unitary operators U_π defined in Equation (A93) form a faithful representation of the Abelian group A. Using the canonical decomposition of Theorem A19, every element of $V \in \mathsf{G}_B$ is decomposed *uniquely* as $V = U_\pi V_0$, where V_0 is an element of the commutant U'. Note also that the commutant U' is a normal subgroup of the adversarial group: indeed, for every element $V \in \mathsf{G}_B$ we have $VU'V^\dagger = U'$. Since U' is a normal subgroup and the decomposition $V = U_\pi V_0$ is unique for every $V \in \mathsf{G}_B$, it follows that the adversarial group G_B is the semidirect product $\mathsf{A} \ltimes U'$. □

Appendix J. Example: The Phase Flip Group

Consider the Hilbert space $\mathcal{H}_S = \mathbb{C}^2$, and suppose that agent A can only perform the identity channel and the phase flip channel $\mathcal{Z}$, defined as

$$\mathcal{Z}(\cdot) = Z \cdot Z\,, \qquad Z = |0\rangle\langle 0| - |1\rangle\langle 1|\,. \tag{A98}$$

Then, the actions of agent A correspond to the unitary representation

$$U : \mathbb{Z}_2 \to \mathsf{Lin}(S)\,, \qquad k \mapsto U_k = Z^k\,. \tag{A99}$$

The representation can be decomposed into two irreps, corresponding to the one-dimensional subspaces $\mathcal{H}_0 = \mathsf{Span}\{|0\rangle\}$ and $\mathcal{H}_1 = \mathsf{Span}\{|1\rangle\}$. The corresponding irreps, denoted by

$$\begin{aligned} \omega_0 :&\quad \mathbb{Z}_2 \to \mathbb{C}\,, \quad \omega(k) = 1, \\ \omega_1 :&\quad \mathbb{Z}_2 \to \mathbb{C}\,, \quad \omega(k) = (-1)^k, \end{aligned} \tag{A100}$$

are the only two irreps of the group and are multiplicative characters.

The condition $VU_k = U_k V$ yields the solutions

$$V = e^{i\theta_0}\,|0\rangle\langle 0| + e^{i\theta_1}\,|1\rangle\langle 1|\,, \qquad \theta_0, \theta_1 \in [0, 2\pi)\,, \tag{A101}$$

corresponding to the commutant U'. The condition $VU_k = (-1)^k\, U_k V$ yields the solutions

$$V = e^{i\theta_0}\,|0\rangle\langle 1| + e^{i\theta_1}\,|1\rangle\langle 0|\,, \qquad \theta_0, \theta_1 \in [0, 2\pi)\,. \tag{A102}$$

It is easy to see that the adversarial group G_B acts irreducibly on $\mathcal{H}_S$.

Let us consider now the subsystem S_A. The states of S_A are equivalence classes under the relation

$$|\psi\rangle \simeq_A |\psi'\rangle \qquad \exists V \in \mathsf{G}_B : \quad |\psi'\rangle = V|\psi\rangle\,. \tag{A103}$$

It is not hard to see that the equivalence class of the state $|\psi\rangle$ is uniquely determined by the *unordered* pair $\{|\langle 0|\psi\rangle|\,,\,|\langle 1|\psi\rangle|\}$. In other words, the state space of system S_A is

$$\mathsf{St}(S_A) = \Big\{\ \{p, 1-p\}\,, : \quad p \in [0,1]\Big\}\,. \tag{A104}$$

Note that, in this case, the state space is not a convex set of density matrices. Instead, it is the quotient of the set of diagonal density matrices, under the equivalence relation that two matrices with the same spectrum are equivalent.

Finally, note that the transformations of system S_A are trivial: since the adversarial group G_B contains the group G_A, the group $\mathsf{G}(S_A) = \pi_A(G_A)$ is trivial, namely

$$\mathsf{G}(S_A) = \Big\{\mathcal{I}_{S_A}\Big\}\,. \tag{A105}$$

Appendix K. Proof of Theorem 4

Let G be a connected Lie group, and let $\mathfrak{g}$ be the Lie algebra. Since G is connected, the exponential map reaches every element of the group, namely $\mathsf{G} = \exp[i\mathfrak{g}]$.

Let $h \in \mathsf{G}$ be a generic element of the group, written as $h = \exp[iX]$ for some $X \in \mathfrak{g}$, and consider the one-parameter subgroup $\mathsf{H} = \{\exp[i\lambda X]\,, \lambda \in \mathbb{R}\}$. For a generic element $g \in \mathsf{H}$, the corresponding unitary operator can be expressed as $U_g = \exp[i\lambda K]$, where $K \in \mathsf{Lin}(S)$ is a suitable self-adjoint operator. Similarly, the multiplicative character has the form $\omega(g) = \exp[i\lambda\mu]$, for some real number $\mu \in \mathbb{R}$.

Now, every element V of the adversarial group must satisfy the relation

$$V \exp[i\lambda K] = \exp[i\lambda(K + \mu\, I_S)]V \qquad \forall \lambda \in \mathbb{R}\,, \tag{A106}$$

or equivalently,

$$\exp[i\lambda K] = V^\dagger \exp[i\lambda(K + \mu\, I_S)]\, V \qquad \forall \lambda \in \mathbb{R}\,. \tag{A107}$$

Since the operators $\exp[i\lambda K]$ and $\exp[i\lambda(K + \mu\, I_S)]$ are unitarily equivalent, they must have the same spectrum. This is only possible if the operators K and $K + \mu\, I_S$ have the same spectrum, which happens only if $\mu = 0$.

Now, recall that the one-parameter Abelian subgroup H is generic. Since every element of G is contained in some one-parameter Abelian subgroup H, we showed that $\omega(g) = 1$ for every $g \in \mathsf{G}$.

To conclude the proof, observe that the map $U^{(j)} \mapsto \omega\, U^{(j)}$ is the identity, and therefore induces the trivial permutation on the set of irreps $\mathsf{Irr}(U)$. Hence, the group of permutations A induced by multiplication by ω contains only the identity element. □

Appendix L. Proof of Proposition 16

Proof. It is enough to decompose the two states as

$$|\psi\rangle = \bigoplus_{j\in\mathsf{Irr}(U)} \sqrt{p_j}\,|\psi_j\rangle \qquad \text{and} \qquad |\psi'\rangle = \bigoplus_{j\in\mathsf{Irr}(U)} \sqrt{p'_j}\,|\psi'_j\rangle\,, \tag{A108}$$

where $|\psi_j\rangle$ and $|\psi'_j\rangle$ are unit vectors in $\mathcal{R}_j \otimes \mathcal{M}_j$. Using this decomposition, we obtain

$$\mathcal{T}_B(|\psi\rangle\langle\psi|) = \bigoplus_{j\in \mathsf{Irr}(U)} p_j \rho_j \qquad \text{and} \qquad \mathcal{T}_B(|\psi\rangle\langle\psi|) = \bigoplus_{j\in \mathsf{Irr}(U)} p'_j \rho'_j\,, \tag{A109}$$

where ρ_j (ρ'_j) is the marginal of $|\psi_j\rangle$ ($|\psi'_j\rangle$) on system $\mathcal{R}_j$. It is then clear that the equality $\mathcal{T}_B(|\psi\rangle\langle\psi|) = \mathcal{T}_B(|\psi'\rangle\langle\psi'|)$ implies $p_j = p'_j$ and $\rho_j = \rho'_j$ for every j. Since the states $|\psi_j\rangle$ and $|\psi'_j\rangle$ have the same marginal on system $\mathcal{R}_j$, there must exist a unitary operator $U_j : \mathcal{M}_j \to \mathcal{M}_j$ such that

$$|\psi'_j\rangle = (I_{\mathcal{R}_j} \otimes U_j)\,|\psi_j\rangle\,. \tag{A110}$$

We can then define the unitary gate

$$U_B = \bigoplus_{j\in \mathsf{Irr}(U)} \left(I_{\mathcal{R}_j} \otimes U_j\right), \tag{A111}$$

which satisfies the property $U_B|\psi\rangle = |\psi'\rangle$. By the characterization of Equation (89), U_B is an element of G_B. □

References

1. Nielsen, M.; Chuang, I. Quantum information and computation. *Nature* **2000**, *404*, 247.
2. Kitaev, A.Y.; Shen, A.; Vyalyi, M.N. *Classical and Quantum Computation*; Number 47; American Mathematical Society: Providence, RI, USA, 2002.
3. Einstein, A.; Podolsky, B.; Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **1935**, *47*, 777. [CrossRef]
4. Schrödinger, E. Discussion of probability relations between separated systems. In *Mathematical Proceedings of the Cambridge Philosophical Society*; Cambridge University Press: Cambrdige, UK, 1935; Volume 31, pp. 555–563.
5. Hardy, L. Quantum theory from five reasonable axioms. *arXiv* **2001**, arXiv:quant-ph/0101012.
6. Barnum, H.; Barrett, J.; Leifer, M.; Wilce, A. Generalized no-broadcasting theorem. *Phys. Rev. Lett.* **2007**, *99*, 240501. [CrossRef] [PubMed]
7. Barrett, J. Information processing in generalized probabilistic theories. *Phys. Rev. A* **2007**, *75*, 032304. [CrossRef]
8. Chiribella, G.; D'Ariano, G.; Perinotti, P. Probabilistic theories with purification. *Phys. Rev. A* **2010**, *81*, 062348. [CrossRef]
9. Barnum, H.; Wilce, A. Information processing in convex operational theories. *Electron. Notes Theor. Comput. Sci.* **2011**, *270*, 3–15. [CrossRef]
10. Hardy, L. Foliable operational structures for general probabilistic theories. In *Deep Beauty: Understanding the Quantum World through Mathematical Innovation*; Halvorson, H., Ed.; Cambridge University Press: Cambrdige, UK, 2011; p. 409.
11. Hardy, L. A formalism-local framework for general probabilistic theories, including quantum theory. *Math. Struct. Comput. Sci.* **2013**, *23*, 399–440. [CrossRef]
12. Chiribella, G. Dilation of states and processes in operational-probabilistic theories. In Proceedings of the 11th workshop on Quantum Physics and Logic, Kyoto, Japan, 4–6 June 2014; Coecke, B., Hasuo, I., Panangaden, P., Eds.; Electronic Proceedings in Theoretical Computer Science; Volume 172, pp. 1–14.
13. Chiribella, G.; D'Ariano, G.M.; Perinotti, P. Quantum from principles. In *Quantum Theory: Informational Foundations and Foils*; Springer: Dordrecht, The Netherlands, 2016; pp. 171–221.
14. Hardy, L. Reconstructing quantum theory. In *Quantum Theory: Informational Foundations and Foils*; Springer: Dordrecht, The Netherlands, 2016; pp. 223–248.
15. Mauro D'Ariano, G.; Chiribella, G.; Perinotti, P. Quantum Theory from First Principles. In *Quantum Theory from First Principles*; D'Ariano, G.M., Chiribella, G., Perinotti, P., Eds.; Cambridge University Press: Cambridge, UK, 2017.

16. Abramsky, S.; Coecke, B. A categorical semantics of quantum protocols. In Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, Turku, Finland, 17 July 2004; pp. 415–425.
17. Coecke, B. Kindergarten quantum mechanics: Lecture notes. In Proceedings of the AIP Conference Quantum Theory: Reconsideration of Foundations-3, Växjö, Sweden, 6–11 June 2005; American Institute of Physics: Melville, NY, USA, 2006; Volume 810, pp. 81–98.
18. Coecke, B. Quantum picturalism. *Contemp. Phys.* **2010**, *51*, 59–83. [CrossRef]
19. Abramsky, S.; Coecke, B. Categorical quantum mechanics. In *Handbook of Quantum Logic and Quantum Structures: Quantum Logic*; Elsevier Science: New York, NY, USA, 2008; pp. 261–324.
20. Coecke, B.; Kissinger, A. *Picturing Quantum Processes*; Cambridge University Press: Cambridge, UK, 2017.
21. Selinger, P. A survey of graphical languages for monoidal categories. In *New Structures for Physics*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 289–355.
22. Haag, R. *Local Quantum Physics: Fields, Particles, Algebras*; Springer: Berlin/Heidelberg, Germany, 2012.
23. Viola, L.; Knill, E.; Laflamme, R. Constructing qubits in physical systems. *J. Phys. A Math. Gen.* **2001**, *34*, 7067. [CrossRef]
24. Zanardi, P.; Lidar, D.A.; Lloyd, S. Quantum tensor product structures are observable induced. *Phys. Rev. Lett.* **2004**, *92*, 060402. [CrossRef] [PubMed]
25. Palma, G.M.; Suominen, K.A.; Ekert, A.K. Quantum computers and dissipation. *Proc. R. Soc. Lond. A* **1996**, *452*, 567–584. [CrossRef]
26. Zanardi, P.; Rasetti, M. Noiseless quantum codes. *Phys. Rev. Lett.* **1997**, *79*, 3306. [CrossRef]
27. Lidar, D.A.; Chuang, I.L.; Whaley, K.B. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.* **1998**, *81*, 2594. [CrossRef]
28. Knill, E.; Laflamme, R.; Viola, L. Theory of quantum error correction for general noise. *Phys. Rev. Lett.* **2000**, *84*, 2525. [CrossRef] [PubMed]
29. Zanardi, P. Stabilizing quantum information. *Phys. Rev. A* **2000**, *63*, 012301. [CrossRef]
30. Kempe, J.; Bacon, D.; Lidar, D.A.; Whaley, K.B. Theory of decoherence-free fault-tolerant universal quantum computation. *Phys. Rev. A* **2001**, *63*, 042307. [CrossRef]
31. Zanardi, P. Virtual quantum subsystems. *Phys. Rev. Lett.* **2001**, *87*, 077901. [CrossRef] [PubMed]
32. Bratteli, O.; Robinson, D.W. *Operator Algebras and Quantum Statistical Mechanics 1*; Springer: Berlin/Heidelberg, Germany, 1987.
33. Kraemer, L.; Del Rio, L. Operational locality in global theories. *arXiv* **2017**, arXiv:1701.03280.
34. Åberg, J. Quantifying superposition. *arXiv* **2006**, arXiv:quant-ph/0612146.
35. Baumgratz, T.; Cramer, M.; Plenio, M. Quantifying coherence. *Phys. Rev. Lett.* **2014**, *113*, 140401. [CrossRef] [PubMed]
36. Levi, F.; Mintert, F. A quantitative theory of coherent delocalization. *New J. Phys.* **2014**, *16*, 033007. [CrossRef]
37. Winter, A.; Yang, D. Operational resource theory of coherence. *Phys. Rev. Lett.* **2016**, *116*, 120404. [CrossRef] [PubMed]
38. Chitambar, E.; Gour, G. Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence. *Phys. Rev. Lett.* **2016**, *117*, 030401. [CrossRef] [PubMed]
39. Chitambar, E.; Gour, G. Comparison of incoherent operations and measures of coherence. *Phys. Rev. A* **2016**, *94*, 052336. [CrossRef]
40. Marvian, I.; Spekkens, R.W. How to quantify coherence: Distinguishing speakable and unspeakable notions. *Phys. Rev. A* **2016**, *94*, 052324. [CrossRef]
41. Yadin, B.; Ma, J.; Girolami, D.; Gu, M.; Vedral, V. Quantum processes which do not use coherence. *Phys. Rev. X* **2016**, *6*, 041028. [CrossRef]
42. Chiribella, G.; D'Ariano, G.; Perinotti, P. Informational derivation of quantum theory. *Phys. Rev. A* **2011**, *84*, 012311. [CrossRef]
43. Hardy, L. Reformulating and reconstructing quantum theory. *arXiv* **2011**, arXiv:1104.2066.
44. Masanes, L.; Müller, M.P. A derivation of quantum theory from physical requirements. *New J. Phys.* **2011**, *13*, 063001. [CrossRef]
45. Dakic, B.; Brukner, C. Quantum Theory and Beyond: Is Entanglement Special? In *Deep Beauty: Understanding the Quantum World through Mathematical Innovation*; Halvorson, H., Ed.; Cambridge University Press: Cambridge, UK, 2011; pp. 365–392.

46. Masanes, L.; Müller, M.P.; Augusiak, R.; Perez-Garcia, D. Existence of an information unit as a postulate of quantum theory. *Proc. Natl. Acad. Sci. USA* **2013**, *110*, 16373–16377. [CrossRef] [PubMed]
47. Wilce, A. Conjugates, Filters and Quantum Mechanics. *arXiv* **2012**, arXiv:1206.2897.
48. Barnum, H.; Müller, M.P.; Ududec, C. Higher-order interference and single-system postulates characterizing quantum theory. *New J. Phys.* **2014**, *16*, 123029. [CrossRef]
49. Chiribella, G.; D'Ariano, G.; Perinotti, P. Quantum Theory, namely the pure and reversible theory of information. *Entropy* **2012**, *14*, 1877–1893. [CrossRef]
50. Chiribella, G.; Yuan, X. Quantum theory from quantum information: The purification route. *Can. J. Phys.* **2013**, *91*, 475–478. [CrossRef]
51. Chiribella, G.; Scandolo, C.M. Conservation of information and the foundations of quantum mechanics. In *EPJ Web of Conferences*; EDP Sciences: Les Ulis, France, 2015; Volume 95, p. 03003.
52. Chiribella, G.; Scandolo, C.M. Entanglement and thermodynamics in general probabilistic theories. *New J. Phys.* **2015**, *17*, 103027. [CrossRef]
53. Chiribella, G.; Scandolo, C.M. Microcanonical thermodynamics in general physical theories. *New J. Phys.* **2017**, *19*, 123043. [CrossRef]
54. Chiribella, G.; Scandolo, C.M. Entanglement as an axiomatic foundation for statistical mechanics. *arXiv* **2016**, arXiv:1608.04459.
55. Lee, C.M.; Selby, J.H. Generalised phase kick-back: The structure of computational algorithms from physical principles. *New J. Phys.* **2016**, *18*, 033023. [CrossRef]
56. Lee, C.M.; Selby, J.H. Deriving Grover's lower bound from simple physical principles. *New J. Phys.* **2016**, *18*, 093047. [CrossRef]
57. Lee, C.M.; Selby, J.H.; Barnum, H. Oracles and query lower bounds in generalised probabilistic theories. *arXiv* **2017**, arXiv:1704.05043.
58. Susskind, L. *The Black Hole War: My Battle with Stephen Hawking to Make the World Safe for Quantum Mechanics*; Hachette UK: London, UK, 2008.
59. Takesaki, M. *Theory of Operator Algebras I*; Springer: New York, NY, USA, 1979.
60. Barnum, H.; Knill, E.; Ortiz, G.; Somma, R.; Viola, L. A subsystem-independent generalization of entanglement. *Phys. Rev. Lett.* **2004**, *92*, 107902. [CrossRef] [PubMed]
61. Barnum, H.; Knill, E.; Ortiz, G.; Viola, L. Generalizations of entanglement based on coherent states and convex sets. *Phys. Rev. A* **2003**, *68*, 032308. [CrossRef]
62. Barnum, H.; Ortiz, G.; Somma, R.; Viola, L. A generalization of entanglement to convex operational theories: entanglement relative to a subspace of observables. *Int. J. Theor. Phys.* **2005**, *44*, 2127–2145. [CrossRef]
63. Del Rio, L.; Kraemer, L.; Renner, R. Resource theories of knowledge. *arXiv* **2015**, arXiv:1511.08818.
64. Del Rio, L. Resource Theories of Knowledge. Ph.D. Thesis, ETH Zürich, Zürich, Switzerland, 2015. [CrossRef]
65. Kraemer Gabriel, L. Restricted Agents in Thermodynamics and Quantum Information Theory. Ph.D. Thesis, ETH Zürich, Zürich, Switzerland, 2016. [CrossRef]
66. Brassard, G.; Raymond-Robichaud, P. The equivalence of local-realistic and no-signalling theories. *arXiv* **2017**, arXiv:1710.01380.
67. Holevo, A.S. *Statistical Structure of Quantum Theory*; Springer: Berlin/Heidelberg, Germany, 2003; Volume 67.
68. Kraus, K. *States, Effects and Operations: Fundamental Notions of Quantum Theory*; Springer: Berlin/Heidelberg, Germany, 1983.
69. Haag, R.; Schroer, B. Postulates of quantum field theory. *J. Math. Phys.* **1962**, *3*, 248–256. [CrossRef]
70. Haag, R.; Kastler, D. An algebraic approach to quantum field theory. *J. Math. Phys.* **1964**, *5*, 848–861. [CrossRef]
71. Buscemi, F.; Chiribella, G.; D'Ariano, G.M. Inverting quantum decoherence by classical feedback from the environment. *Phys. Rev. Lett.* **2005**, *95*, 090501. [CrossRef] [PubMed]
72. Buscemi, F.; Chiribella, G.; D'Ariano, G.M. Quantum erasure of decoherence. *Open Syst. Inf. Dyn.* **2007**, *14*, 53–61. [CrossRef]
73. Selinger, P. Idempotents in dagger categories. *Electron. Notes Theor. Comput. Sci.* **2008**, *210*, 107–122. [CrossRef]
74. Coecke, B.; Selby, J.; Tull, S. Two Roads to Classicality. *Electron. Proc. Theor. Comput. Sci.* **2018**, *266*, 104–118. [CrossRef]

75. Coecke, B.; Lal, R. Causal categories: relativistically interacting processes. *Found. Phys.* **2013**, *43*, 458–501. [CrossRef]
76. Coecke, B. Terminality implies no-signalling... and much more than that. *New Gener. Comput.* **2016**, *34*, 69–85. [CrossRef]
77. Chiribella, G. Distinguishability and copiability of programs in general process theories. *Int. J. Softw. Inform.* **2014**, *8*, 209–223.
78. Fulton, W.; Harris, J. *Representation Theory: A First Course*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 129.
79. Marvian, I.; Spekkens, R.W. A generalization of Schur–Weyl duality with applications in quantum estimation. *Commun. Math. Phys.* **2014**, *331*, 431–475. [CrossRef]
80. Galley, T.D.; Masanes, L. Impossibility of mixed-state purification in any alternative to the Born Rule. *arXiv* **2018**, arXiv:1801.06414.
81. Yngvason, J. Localization and entanglement in relativistic quantum physics. In *The Message of Quantum Science*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 325–348.
82. Murray, F.J.; Neumann, J.V. On rings of operators. *Ann. Math.* **1936**, *37*, 116–229. [CrossRef]
83. Murray, F.J.; von Neumann, J. On rings of operators. II. *Trans. Am. Math. Soc.* **1937**, *41*, 208–248. [CrossRef]
84. Uhlmann, A. The transition probability in the state space of a *-algebra. *Rep. Math. Phys.* **1976**, *9*, 273–279. [CrossRef]
85. Jozsa, R. Fidelity for mixed quantum states. *J. Mod. Opt.* **1994**, *41*, 2315–2323. [CrossRef]
86. Lindblad, G. A general no-cloning theorem. *Lett. Math. Phys.* **1999**, *47*, 189–196. [CrossRef]
87. D'Ariano, G.M.; Presti, P.L. Optimal nonuniversally covariant cloning. *Phys. Rev. A* **2001**, *64*, 042308. [CrossRef]
88. Chiribella, G.; D'Ariano, G.; Perinotti, P.; Cerf, N. Extremal quantum cloning machines. *Phys. Rev. A* **2005**, *72*, 042336. [CrossRef]
89. Coecke, B.; Selby, J.; Tull, S. Categorical Probabilistic Theories. *Electron. Proc. Theor. Comput. Sci.* **2018**, *266*, 367–385.