Int J Software Informatics, Volume 8, Issue 3-4 (2014), pp. 209–223
International Journal of Software and Informatics, ISSN 1673-7288

E-mail: ijsi@iscas.ac.cn
http://www.ijsi.org
Tel: +86-10-62661040

Distinguishability and Copiability of Programs in General Process Theories

Giulio Chiribella

(Center for Quantum Information, Institute for Interdisciplinary Information Sciences,
Tsinghua University, Beijing 100084, China)

Abstract We propose a notion of state distinguishability that does not refer to probabilities, but rather to the ability of a set of states to serve as programs for a desired set of gates. Using this notion, we reconstruct the structural features of the task of state discrimination, such as the equivalence with cloning and the impossibility to extract information from two non-distinguishable pure states without causing a disturbance. All these features express intrinsic links among operational tasks, which are valid independently of the particular theory under consideration.
Key words: state discrimination; quantum cloning; programmable gates

Chiribella G. Distinguishability and copiability of programs in general process theories. *Int J Software Informatics*, **Vol.8, No.3-4 (2014): 209–223. http://www.ijsi.org/1673-7288/8/i191.htm**

1 Introduction

Quantum information science is making rapid progress towards the realization of a new generation of technologies which promises to revolutionize communication, sensing, and computation[34,35,39]. At the same time, it is also revolutionizing the very notion of information, questioning the preeminence of classical information theory as *the* canonical theory of information.

The sharp contrast between the familiar world of classical information and the exotic features of quantum information quickly leads to questions about alternative theories of information beyond quantum theory: after all, we expected the world to be classical and discovered that it was quantum—what if one day we were to discover another, more fundamental theory of physics, which is neither classical nor quantum? Should we revise the conceptual framework of information theory once more? This type of questions motivated the investigation of a larger class of theories, broadly known as *general probabilistic theories (GPTs)* [5-7,10,11,18,19,24-26,29,32,33,37]. GPTs provide a neutral framework for analyzing high level features of information-processing protocols, independently of the particular laws that govern the hardware level.

This work was supported by the National Basic Research Program of China (973)(Grants 2011CBA00300, 2011CBA00301) and by the National Natural Science Foundation of China (Grants 11350110207, 61033001, 61061130540), by the 1000 Youth Fellowship Program of China, by the Foundational Questions Institute (Grants FQXi-RFP3-1325).
Corresponding author: Giulio Chiribella, Email: gchiribella@mail.tsinghua.edu.cn
Received 2014-11-01; Accepted 2014-11-15.

The GPT framework has been used for characterizing quantum theory in terms of operational axioms[11,18,19,24,32,33] and for establishing direct links among information-theoretic protocols[5-7,10,29].

This analysis has the merit of identifying structures in the family of quantum protocols and of highlighting general "laws of information" that are independent of the specific theory under consideration. An example of such a law is the equivalence between cloning and distinguishability, stating that different pieces of information can be replicated if and only if they are distinguishable from one another.

In the spirit of identifying theory-independent "laws of information" and establishing direct links among protocols one can also go one step further. Instead of probabilistic theories, one can consider more primitive theories that only describe operations, without assigning probabilities to the random events that may be generated by these operations. The study of these theories, now known as *process theories*, has been pioneered by Abramsky and Coecke[1,2,15,17] and has been extensively employed for the reconstruction of quantum protocols over the past ten years[1,3,20,22,36].

While a full characterization of quantum theory in the language of process theories seems to be still far away, it is stimulating to ask how far the probability-free approach can go. At the level of principles this is an important question, because it aims at drawing the line between those aspects of information that are defined only in terms of operations (and therefore can be mechanized) and those that rely on the subjective expectations of an agent. This paper provides a contribution in this direction, presenting a probability-free treatment of the relations between distinguishability, cloning, and programming of gates.

2 Process Theories

The framework of *process theories*[1,15,17] is based on (strict) symmetric monoidal categories (SMC)[4]. Nevertheless, no prior knowledge of category theory is required to understand its basic features: the basic categorical facts are encoded in a graphical language[38] which is identical to the familiar languages of quantum circuits and of classical Boolean circuits. The role of SMCs is just to provide the mathematical foundations of such graphical language.

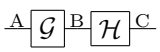
2.1 An abstract circuit model

A process theory describes circuits that transform input data into output data, or, in the terminology of physics, circuits that transform input systems into output systems. Mathematically, a "process theory" is an SMC, here denoted by $\mathbf{C}$. The objects in the category, denoted by $|\mathbf{C}|$, represent different data types (a.k.a. different systems, in the physics terminology). The morphisms in the category represent the different gates (a.k.a. different physical processes) that transform an input system into an output system. A gate of type $\mathrm{A} \to \mathrm{B}$ will be represented as

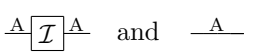
.

The set of all gates of type $\mathrm{A} \to \mathrm{B}$ will be denoted by $\mathbf{C}(\mathrm{A}, \mathrm{B})$. For two gates $\mathcal{G} \in \mathbf{C}(\mathrm{A}, \mathrm{B})$ and $\mathcal{H} \in \mathbf{C}(\mathrm{B}, \mathrm{C})$, we denote the sequential composition as $\mathcal{G}; \mathcal{H} \in \mathbf{C}(\mathrm{A}, \mathrm{C})$

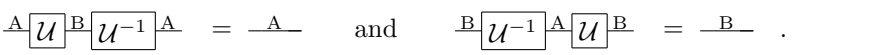
and represent it graphically as



The identity gate on A, denoted by $\mathcal{I}_{\mathrm{A}}$, will be represented equivalently as

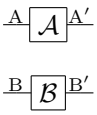


A gate $\mathcal{U} : \mathrm{A} \to \mathrm{B}$ is *reversible* (or equivalently, is an *isomorphism*) iff there exists another gate $\mathcal{U}^{-1} : \mathrm{B} \to \mathrm{A}$ such that

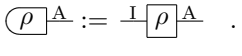


If there exists a reversible gate of type $\mathrm{A} \to \mathrm{B}$, the systems A and B are called *isomorphic*, denoted as $\mathrm{A} \simeq \mathrm{B}$.

When two systems A and B are considered together, we denote their tensor as $\mathrm{A} \otimes \mathrm{B}$. The absence of relevant data is represented by the monoidal unit, denoted by I. When two gates $\mathcal{A} \in \mathbf{C}(\mathrm{A}, \mathrm{A}')$ and $\mathcal{B} \in \mathbf{C}(\mathrm{B}, \mathrm{B}')$ operate in parallel, their action is described by the tensor product gate $\mathcal{A} \otimes \mathcal{B} \in \mathbf{C}(\mathrm{A} \otimes \mathrm{B}, \mathrm{A}' \otimes \mathrm{B}')$, graphically represented as

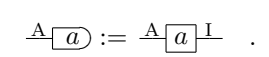


Motivated by the physical interpretation, a gate ρ of type $\mathrm{I} \to \mathrm{A}$ will be called a *state of system* A and will be represented as



(1)

A gate a of type $\mathrm{A} \to \mathrm{I}$ will be called an *effect on system* A and will be represented as



(2)

A gate s of type $\mathrm{I} \to \mathrm{I}$ will be called a *scalar* and will be sometimes represented "out of the box", as

(3)

We denote the identity gate on system I as 1. Recall that scalars in an SMC form a commutative monoid[31], with $s; 1 = 1; s = s$ for every scalar $s \in \mathbf{C}(\mathrm{I}, \mathrm{I})$.

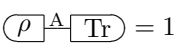
2.2 Causality

An important requirement for a physical theory is *causality*[10,11]. Informally, causality is the requirement that information in a circuit flows from the input to the output, and not vice-versa.

In the categorical language, causality is formulated as *terminality of the tensor unit*[23,28]:

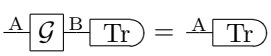
Axiom 1 (Causality). For every system $\mathrm{A} \in |\mathbf{C}|$ there exists one and only one gate of type $\mathrm{A} \to \mathrm{I}$, called the *trace on* A, denoted by Tr_{A}, and represented as  .

Note that, by definition, one has $\mathrm{Tr}_{\mathrm{I}} = 1$. Note also that, by definition, every state $\rho \in \mathbf{C}(\mathrm{I}, \mathrm{A})$ is normalized as



$$= 1 \tag{4}$$

and, more generally, every gate $\mathcal{G} \in \mathbf{C}(\mathrm{A}, \mathrm{B})$ is normalized as

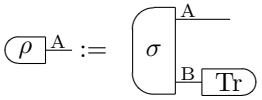


$$= \quad \text{  } \quad . \tag{5}$$

2.3 Marginals and extensions

Thanks to Causality, one can define marginal states:

Definition 2.1. The *marginal on* A of a state $\sigma \in \mathbf{C}(\mathrm{I}, \mathrm{A} \otimes \mathrm{B})$ is the state $\rho \in \mathbf{C}(\mathrm{I}, \mathrm{A})$ defined by

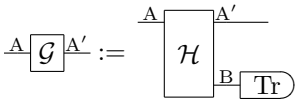


.

When the above equation holds, we say that σ is an *extension of* A *to the context* B.

The same definition can be put forward for general gates:

Definition 2.2. The marginal on system A' of a gate $\mathcal{H} \in \mathbf{C}(\mathrm{A}, \mathrm{A}' \otimes \mathrm{B})$ is the gate $\mathcal{G} \in \mathbf{C}(\mathrm{A}, \mathrm{A}')$ defined by

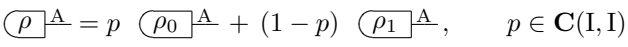


.

When the above equation holds, we say that $\mathcal{H}$ is an *extension of* $\mathcal{G}$ *to the context* B.

2.4 Pure states and pure gates

Pure states are an essential concept both in physics and computer science. Traditionally, they are defined as states that cannot be obtained by randomizing the preparation of the system—equivalently, states that cannot be decomposed as a convex combination of other states. Here, however, we did not introduce any notion of convex combination. An expression like

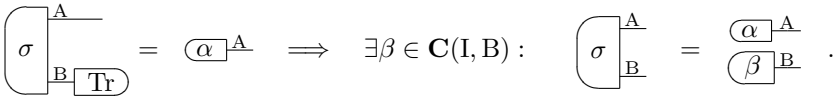


is not legal in our language, because there is no notion of "sum of states" and no notion of "difference of two scalars".

In order to introduce pure states in the framework, there are a few different options: First, one could introduce probabilities, as it was done in Ref. [10]. In this way, the gates inherit a structure of vector space over the real numbers. An other option is to *assume* that there is a distinguished subset of states and gates that are

nominally regarded as "pure". This approach was followed by Coecke[16] and Coecke-Perdrix[21], who defined the category of *pure processes* as a monoidal subcategory of **C**. In this paper we will follow a third option, in which pure states and pure gates are defined only in terms of the circuit structure. This approach is at the basis of the construction of *categorical purification*, recently put forward by the author[13,14]. In this construction, the pure states are defined as follows

Definition 2.3. A state $\alpha \in \mathbf{C}(\mathrm{I}, \mathrm{A})$ is *pure* iff it has only trivial extensions, that is, iff for every system $\mathrm{B} \in |\mathbf{C}|$ and for every state $\sigma \in \mathbf{C}(\mathrm{I}, \mathrm{A} \otimes \mathrm{B})$ one has the implication



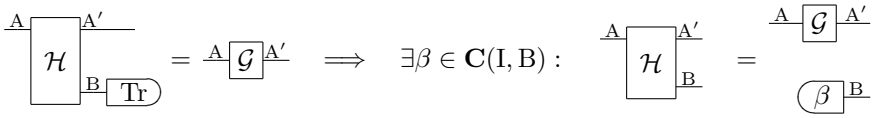
The set of all pure states of system A will be denoted as $\mathsf{Pure}\mathbf{C}(\mathrm{I}, \mathrm{A})$.

Intuitively, a pure state is defined as an "integral piece of information", which is independent of the surrounding context. From the definition it follows that the product of two pure states is a pure state[13,14], namely

$$\alpha \otimes \beta \in \mathsf{Pure}\mathbf{C}(\mathrm{I}, \mathrm{A} \otimes \mathrm{B}) \qquad \forall \alpha \in \mathsf{Pure}\mathbf{C}(\mathrm{I}, \mathrm{A})\,, \forall \beta \in \mathsf{Pure}\mathbf{C}(\mathrm{I}, \mathrm{B})\,. \tag{6}$$

The definition of pure state can be extended in the obvious way to general gates, leading to the following

Definition 2.4. A gate $\mathcal{G} \in \mathbf{C}(\mathrm{A}, \mathrm{A}')$ is *pure* iff it has only trivial extensions, that is, iff for every system $\mathrm{B} \in |\mathbf{C}|$ and for every gate $\mathcal{H} \in \mathbf{C}(\mathrm{A}, \mathrm{A}' \otimes \mathrm{B})$ one has the implication



The set of all pure gates of type $\mathrm{A} \to \mathrm{A}'$ will be denoted as $\mathsf{Pure}\mathbf{C}(\mathrm{A}, \mathrm{A}')$.

3 Programmability, Distinguishability, and Copiability

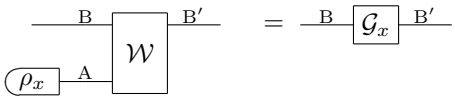
We are now ready to introduce the three tasks that are protagonists of this paper.

3.1 Programmability

Consider the task of programming the operations performed by a machine using a set of instructions, encoded in the state of a physical system. The idea can be formalized as follows:

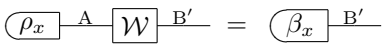
Definition 3.1. Let $\mathsf{S} = \{\rho_x\}_{x \in \mathsf{X}}$ be a set of states of system A and let $\mathsf{G} = \{\mathcal{G}_x\}_{x \in \mathsf{X}}$ be a set of gates of type $\mathrm{B} \to \mathrm{B}'$, with X a suitable index set.

We say that the states in S *program* the gates in G iff there exists a gate $\mathcal{W}$, of type $\mathrm{A} \otimes \mathrm{B} \to \mathrm{B}'$, such that



$$\forall x \in \mathsf{X}\,. \tag{7}$$

In other words, the states in S program the gates in G if there exists a machine that can perform on demand every desired gate in G, controlled by a specific state in S. Note that the gates in G do not need be reversible and, in general, their input and output can differ. For example, the input could be set to be the trivial system $\mathrm{B} \equiv \mathrm{I}$. In this case, the gates in G initialize system B' in a given set of states $\{\beta_x\}_{x\in\mathsf{X}}$ and Eq. (7) becomes



$$\forall x \in \mathsf{X}. \tag{8}$$

3.2 Distinguishability

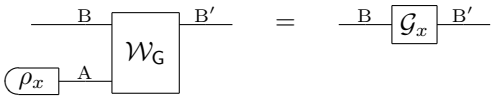
In quantum theory, the density matrices in a given set $\{\rho_x\}_{x\in\mathsf{X}}$ are (perfectly) distinguishable iff there exists a measurement, described by operators $\{P_x\}_{x\in\mathsf{X}}$, satisfying the equation

$$\mathrm{Tr}[P_x\rho_y] = \delta_{xy} \qquad \forall x, y \in \mathsf{X}.$$

This definition cannot be exported to our abstract circuit model, however, because we do not have a notion of measurement. Can we still make sense of the expression that some states are perfectly distinguishable?

To answer this question, we should go at the root of the operational meaning of distinguishability. Operationally, the purpose of distinguishing states is to make decisions. For example, in a quantum state discrimination game the player would use the measurement $\{P_x\}_{x\in\mathsf{X}}$ to decide which answer $x \in \mathsf{X}$ she should send to the referee. One can also think of other types of games, where the player has a set of possible moves, described by a set of gates $\{\mathcal{G}_x\}_{x\in\mathsf{X}}$, and has to choose one move depending on the information contained in the state ρ_x. All these examples suggest that one can *identify* the ability to reliably distinguish states with the ability to use them as programs for a desired set of operations. In the abstract circuit model, this intuition can be formalized as follows:

Definition 3.2. Let $\mathsf{S} = \{\rho_x\}_{x\in\mathsf{X}}$ be a set of states of system A. The states in S are *(perfectly) distinguishable* iff for every pair of systems B, B' and for every indexed set of gates $\mathsf{G} = \{\mathcal{G}_x\}_{x\in\mathsf{X}}$ of type $\mathrm{B} \to \mathrm{B}'$ there exists a gate $\mathcal{W}_\mathsf{G} : \mathrm{A} \otimes \mathrm{B} \to \mathrm{B}'$ such that



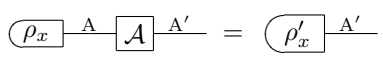
$$\forall x \in \mathsf{X}. \tag{9}$$

In short, the states S are perfectly distinguishable iff they can program every desired set of gates.

3.3 Distinguishability of the output implies distinguishability of the input

An obvious consequence of definition 3.2 is the following: if the states in S can be transformed into a set of distinguishable states, then they must be perfectly distinguishable:

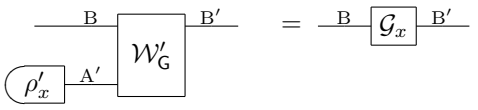
Proposition 3.1. Let $\mathsf{S}' = \{\rho'_x\}_{x\in\mathsf{X}}$ be a set of perfectly distinguishable states of system A'. If there exists a gate $\mathcal{A} : \mathrm{A} \to \mathrm{A}'$ such that



$$\forall x \in \mathsf{X}, \tag{10}$$

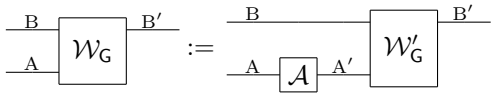
then the states $\{\rho_x\}_{x\in\mathsf{X}}$ are perfectly distinguishable.

Proof Since the states in S' are perfectly distinguishable, for every indexed set of gates $\mathsf{G} = \{\mathcal{G}_x\}_{x\in\mathsf{X}}$ there exists a gate $\mathcal{W}'_{\mathsf{G}}$ such that



$\forall x \in \mathsf{X}\,.$

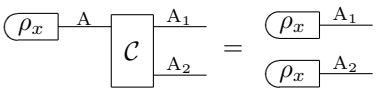
Defining



one obtains that the states in S program the gates in G. Since G is arbitrary, this means that the states in S are distinguishable. □

3.4 Copiability

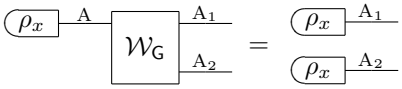
Suppose that we are given a physical system A, with the promise that the system is in a state ρ_x chosen from a set $\mathsf{S} = \{\rho_x\}_{x\in\mathsf{X}}$. Thinking of the state as a piece of information, it is natural to ask whether it is possible to make copies of it. In the abstract gate model, we say that the states in S are *copiable* iff there exists a gate $\mathcal{C} : \mathrm{A} \to \mathrm{A}_1 \otimes \mathrm{A}_2$, with $\mathrm{A}_1 \simeq \mathrm{A}_2 \simeq \mathrm{A}$, such that



$\forall x \in \mathsf{X}\,.$ (11)

3.5 Distinguishability implies copiability

Suppose that the states in S are distinguishable. Then, an immediate consequence of definition 3.2 is that they can be copied. Indeed, we can choose the set G to consist of gates that initialize two systems of type A in the states $\{\rho_x \otimes \rho_x\}_{x\in\mathsf{X}}$. Applying Eq. (9) to this particular set of gates we obtain a gate $\mathcal{W}_{\mathsf{G}}$ such that



$\forall x \in \mathsf{X}\,.$ (12)

A natural question is whether the converse is also true, namely whether copiable states are also distinguishable. This result does *not* follow from the definitions given so far and requires some additional assumptions regarding distinguishability with multiple copies. These assumptions are spelt out in the next two sections.

4 Asymptotic Distinguishability

In this section we introduce a notion of distinguishability in the asymptotic limit. In order to do that, we introduce a topology on top of the abstract circuit model.

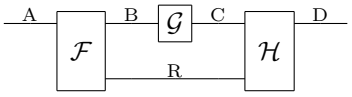
4.1 Approximation of a gate

The most primitive notion of "closeness" is the topological one. In order to express the fact that two gates are "close to one another" we introduce the following:

Definition 4.1. A *topology for the circuit model* C consists in the assignment of a family of open subsets $\mathcal{O}_{\mathrm{A}\to\mathrm{B}}$ to every set of gates $\mathbf{C}(\mathrm{A},\mathrm{B})$, in accordance with the following requirements

1. $\mathcal{O}_{\mathrm{A}\to\mathrm{A}'} \times \mathcal{O}_{\mathrm{B}\to\mathrm{B}'} \subseteq \mathcal{O}_{\mathrm{A}\otimes\mathrm{B}\to\mathrm{A}'\otimes\mathrm{B}'}$ for arbitrary systems $\mathrm{A},\mathrm{A}',\mathrm{B},\mathrm{B}' \in |\mathbf{C}|$
2. the insertion of a gate in a circuit is continuous: for all systems $\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D},\mathrm{R} \in |\mathbf{C}|$, for every pair of gates $\mathcal{F} : \mathrm{A} \to \mathrm{B}\otimes\mathrm{R}$ and $\mathcal{H} : \mathrm{C}\otimes\mathrm{R} \to \mathrm{D}$ and for every open set $\mathsf{O} \in \mathcal{O}_{\mathrm{A}\to\mathrm{D}}$, the set of gates

$$(\mathcal{F},\mathcal{H})^{-1}\mathsf{O} := \left\{ \mathcal{G} \in \mathbf{C}(\mathrm{B}\to\mathrm{C}) \text{ such that } \right.$$



$$\left. \in \mathsf{O} \right\}$$

is open.

Using the above definition, we can express the fact that a sequence of gates converges to a specified gate. Precisely, the sequence $(\mathcal{G}_n)_{n\in\mathbb{N}} \subset \mathbf{C}(\mathrm{A},\mathrm{B})$ converges to the gate $\mathcal{G}$ iff for every open set $\mathsf{O} \in \mathcal{O}_{\mathrm{A}\to\mathrm{B}}$ there exists an integer N_{O} such that one has

$$\mathcal{G}_n \in \mathsf{O} \qquad \forall n > N_{\mathsf{O}}\,.$$

When this is the case, we write $\lim_{n\to\infty} \mathcal{G}_n = \mathcal{G}$.

In this paper, we assume the following

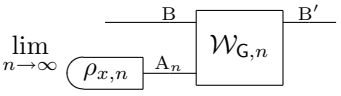
Axiom 2. For every pair of systems $\mathrm{A},\mathrm{B} \in |\mathbf{C}|$, we assume that the set of gates $\mathbf{C}(\mathrm{A},\mathrm{B})$ is compact, meaning that for every sequence of gates $(\mathcal{G}_n)_{n\in\mathbb{N}} \subset \mathbf{C}(\mathrm{A},\mathrm{B})$ one can find a subsequence $(\mathcal{G}_{n_k})_{k\in\mathbb{N}}$ and a gate $\mathcal{G}$ such that $\lim_{k\to\infty} \mathcal{G}_{n_k} = \mathcal{G}$.

4.2 Approximate programmability

The notion of approximation of gates allow us to discuss approximate programmability:

Definition 4.2. For every integer n, let A_n be a system in $\mathbf{C}$ and let $\mathsf{S}_n := \{\rho_{x,n}\}$ be a set of states of system A_n. We say that the states in S_n *asymptotically program* the gates in $\mathsf{G} = \{\mathcal{G}_x\}_{x\in\mathsf{X}}$ iff there exists a gate $\mathcal{W}_{\mathsf{G},n} : \mathrm{A}_n \otimes \mathrm{B} \to \mathrm{B}'$ such that

$$\lim_{n\to\infty}$$



$$=$$

(13)

uniformly for every $x \in \mathsf{X}$.

Note that we required that the convergence should be uniform in x, because this is the appropriate requirement when the set X is infinite.

4.3 Asymptotic distinguishablity

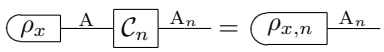
Using definition 4.2 it is immediate to give a notion of asymptotic distinguishability of states:

Definition 4.3. For every integer n, let A_n be a system in $\mathbf{C}$ and let $\mathsf{S}_n := \{\rho_{x,n}\}$ be a set of states of system A_n. We say that the states S_n are *asymptotically distinguishable in the limit* $n \to \infty$ iff, for every pair of systems $\mathrm{B},\mathrm{B}' \in |\mathbf{C}|$ and every

set of gates $\mathsf{G} = \{\mathcal{G}_x\}_{x\in\mathsf{X}} \subset \mathbf{C}(\mathrm{B},\mathrm{B}')$, the states in S_n asymptotically program the gates in $\mathcal{G}$.

The notion of asymptotic distinguishability is very useful. Its usefulness is mostly due to the following proposition, which links distinguishability with its asymptotic version:

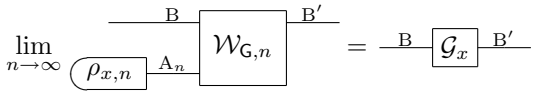
Proposition 4.1. Let $\mathsf{S} = \{\rho_x\}_{x\in\mathsf{X}}$ be set of states of system A and, for every $n \in \mathbb{N}$, let $\mathsf{S}_n = \{\rho_{x,n}\}_{x\in\mathsf{X}}$ be a set of states of system A_n. If the states in S_n are asymptotically distinguishable and if there exists a gate $\mathcal{C}_n : \mathrm{A} \to \mathrm{A}_n$ such that



$\forall x \in \mathsf{X}\,,$

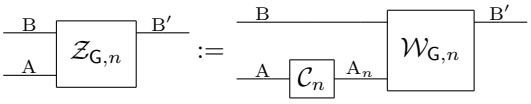
then the states in S are distinguishable.

Proof Since the states in S_n are asymptotically distinguishable, for every pair of systems $\mathrm{B},\mathrm{B}' \in |\mathbf{C}|$ and every set of gates $\mathsf{G} = \{\mathcal{G}_x\}_{x\in\mathsf{X}} \subset \mathbf{C}(\mathrm{B},\mathrm{B}')$ there exists a gate $\mathcal{W}_{\mathsf{G},n}$ such that

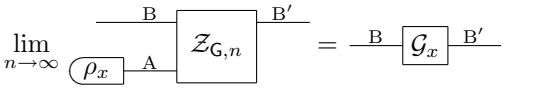


$\forall x \in \mathsf{X}\,.$

Defining the gate

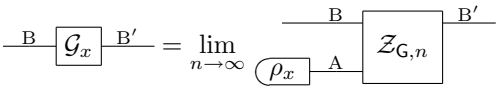


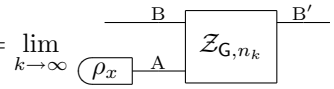
and combining the two equations above, one obtains

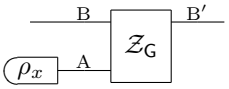


$\forall x \in \mathsf{X}\,.$

Now, Axiom 2 guarantees that there exists a subsequence $(\mathcal{Z}_{\mathsf{G},n_k})_{k\in\mathbb{N}}$ and a gate $\mathcal{Z}_{\mathsf{G}}$ such that $\lim_{k\to\infty} \mathcal{Z}_{\mathsf{G},n_k} = \mathcal{Z}_{\mathsf{G}}$. Hence, one has







$\forall x \in \mathsf{X}\,,$

where the last equality used the fact that the composition of gates is continuous (cf. item 2 of definition 4.1). In conclusion, we proved that every set of gates G can be programmed by the states in S. By definition 3.2, this means that the states in S are distinguishable. □

5 Asymptotic i.i.d. Distinguishability

Suppose that we are given a large number of identical systems of type A, prepared in the i.i.d. state $\rho_x^{\otimes N}$, $x \in \mathsf{X}$. Intuitively, if the states S are distinct from one another, then it should be possible to find out the value of x with vanishing error. This is the case in quantum theory, where one can perform quantum state tomography and identify the state ρ_x up to an error that vanishes when the number of copies goes to infinity. Of course, the tomography argument requires one to have a notion of measurement, which has not been introduced in the framework so far. In order to express the intuitive property of asymptotic i.i.d. distinguishability, one has two alternatives: The first alternative is to introduce measurements and probabilities. When this is done, one can *prove* a theorem stating that the probability of error in the identification of the label x vanishes in the limit $N \to \infty$[10,29]. The second alternative is to *assume* asymptotic i.i.d. distinguishability as an axiom. Here we follow this route:

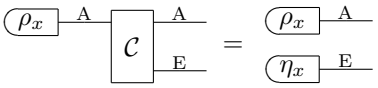
Axiom 3. For every system $\mathrm{A} \in |\mathbf{C}|$ and for every set of distinct states of A, say $S = \{\rho_x\}_{x\in\mathsf{X}}$, the i.i.d states $\{\rho_x^{\otimes n}\}_{x\in\mathsf{X}}$ are asymptotically distinguishable.

In the next sections we will explore the consequences of this requirement.

6 Distinguishability and Generation of Side Information

Distinguishability is closely related with another operational task, which consists in generating some additional piece of data from a given state. Formally, the task is defined as follows:

Definition 6.1. Let $\mathsf{S} = \{\rho_x\}_{x\in\mathsf{X}}$ be a set of distinct states of system A. We say that the gate $\mathcal{C} : \mathrm{A} \to \mathrm{A} \otimes \mathrm{E}$ *generates side information* for the states in S iff there exists a set of states of system E, say $\{\eta_x\}_{x\in\mathsf{X}}$, such that



$$\forall x \in \mathsf{X}\,, \tag{14}$$

and at least two states η_{x_0} and η_{x_1} are distinct. Moreover, we say that the gate $\mathcal{C}$ *generates faithful side information* iff the states $\{\eta_x\}_{x\in\mathsf{X}}$ are all distinct.

One example of process that generates faithful side information is copying: in this particular case, one has $\mathrm{E} = \mathrm{A}$ and $\eta_x = \rho_x$ for every $x \in \mathsf{X}$.

We now show that only distinguishable states allow one to generate *faithful* side information:

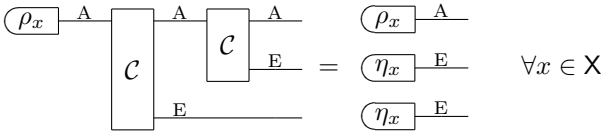
Proposition 6.1. The following are equivalent:

1. the states S are distinguishable

2. there exists a gate that generates faithful side information for S.

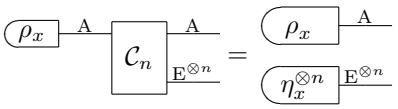
Proof: Clearly, if the states are distinguishable, one can use them to program the preparation of the states $\{\rho_x \otimes \eta_x\}_{x\in\mathsf{X}}$ for every desired set of states $\{\eta_x\}_{x\in\mathsf{X}}$ of every desired system E. Conversely, suppose that there exists a gate $\mathcal{C}$ that generates side

information for the states in S. By applying the gate $\mathcal{C}$ twice, one obtains



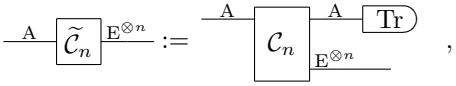
$\forall x \in \mathsf{X}\,.$

More generally, applying $\mathcal{C}$ for n times one obtains a gate $\mathcal{C}_n : \mathrm{A} \to \mathrm{A} \otimes \mathrm{E}^{\otimes n}$ such that



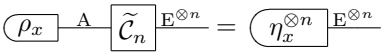
$\forall x \in \mathsf{X}\,,$

Discarding the output system A, one obtains the gate



,

which satisfies



$\forall x \in \mathsf{X}\,,$

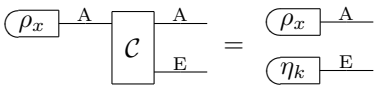
due to the normalization condition of Eq. (4). Now, by hypothesis the states $\{\eta_x\}_{x\in\mathsf{X}}$ are distinct. Hence, by Axiom 3 the states in the set $\mathsf{S}_n := \{\eta_x^{\otimes n}\}_{x\in\mathsf{X}}$ are asymptotically distinguishable. Proposition 4.1 then guarantees that the states in S are distinguishable. □

When the side information is not faithful, the situation is slightly more diversified. In analogy with Refs. [12,27,30] we define the *confusability graph* of a set of states $\mathsf{S} = \{\rho_x\}_{x\in\mathsf{X}}$ as the graph where

1. the vertices are the elements of X
2. two vertices x and y are adjacent iff the corresponding states ρ_x and ρ_y are not distinguishable.

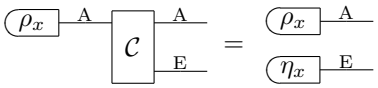
Let us denote by $\{\mathsf{X}_k\}_{k=1}^K$ the connected components of the confusability graph. We then have the following

Proposition 6.2. If the gate $\mathcal{C} : \mathrm{A} \to \mathrm{A} \otimes \mathrm{E}$ generates side information for the set S, then for every connected component X_k there exists a state $\eta_k \in \mathbf{C}(\mathrm{I}, \mathrm{E})$ such that



$\forall x \in \mathsf{X}_k\,.$

Proof: By definition, the fact that the gate $\mathcal{C}$ generates side information amounts to the condition



$\forall x \in \mathsf{X}\,.$

We have to show that η_x does not depend on the particular element x, but only to the connected component it belongs to. This is easily done thanks to proposition 6.1, which guarantees that if x and y are connected, then $\eta_x = \eta_y$. □

7 Copiability-Distinguishability Equivalence

In the previous section we saw that only distinguishable states can generate faithful side information. This fact implies a fundamental equivalence between copiability and distinguishability.

Proposition 7.1. Let $\mathsf{S} \subset \mathbf{C}(\mathrm{I}, \mathrm{A})$ be a finite set of distinct states. The states S are copiable if and only if they are distinguishable.

Proof: We already saw in subsection 3.5 that distinguishable states are copiable.

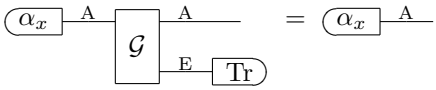
Conversely, suppose that the states in S are copiable with a gate $\mathcal{C}$, as in Eq. (11). By definition, the gate $\mathcal{C}$ generates faithful side information. Hence, by proposition 6.1 the states S must be perfectly distinguishable. □

8 Cryptographic No Information Without Disturbance

At the qualitative level, the security of the many quantum key distribution protocols (such as e.g. Ref. [8]) is based on the fact that when a quantum system is prepared in a pure state chosen from a set of two (or more) non-orthogonal states, an eavesdropper cannot extract any information about the state of the system without changing the state of the system. We refer to this feature as the Cryptographic No Information Without Disturbance property. An iconic demonstration of this working principle is the B92 protocol[9], which employs the transmission of just two non-orthogonal states.

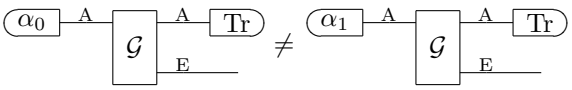
It is then natural to wonder under which conditions this feature can be reproduced in a general process theory, other than quantum theory.

Here we show that, if one accepts the definitions given in this paper, the Cryptographic No Information Without Disturbance is a logical implication, valid in arbitrary theories. We model the process of extracting information from system A as a gate $\mathcal{G}$ of type $\mathrm{A} \to \mathrm{A} \otimes \mathrm{E}$, where E is the system held by the eavesdropper. For the information encoded in the states α_0 and α_1, the condition of no disturbance is



$$\forall x \in \{0, 1\}\,, \tag{15}$$

meaning that the marginal state of system A is not affected by the presence of the gate $\mathcal{G}$. On the other hand, the condition that the gate $\mathcal{G}$ extracts information from the input is that the marginal state of system E depends on the input label x, namely



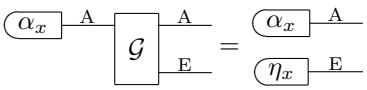
$$. \tag{16}$$

With these definitions we have the following

Proposition 8.1. Let α_0 and α_1 be two pure states of system A. If the two states not distinguishable, then no information can be extracted without disturbance, that is, Eqs. (15) and (16) cannot be jointly satisfied.

Proof: Suppose that the no disturbance condition of Eq. (15) is satisfied. Then,

by definition of pure state (definition 2.3), one must have



$\forall x \in \{0, 1\}$

for some (not necessarily pure) states η_0 and η_1. Now, if $\eta_0 \neq \eta_1$, then the gate $\mathcal{G}$ generates faithful side information for the states $\{\alpha_0, \alpha_1\}$. By proposition 6.1, this implies that α_0 and α_1 are distinguishable. Since by hypothesis the states α_0 and α_1 are not distinguishable by hypothesis, we conclude that Eq. (16) cannot be satisfied. □

9 Summary and Outlook

In this paper we formulated the basic notion of distinguishability without reference to probabilities. Our definition, formulated in an abstract circuit model, expresses the intuitive fact that two pieces of information are distinguishable if they can be used as instructions to program every two desired operations. We then examined the relation between distinguishability and copiability, which required us to enrich the circuit model with a topology. Thanks to this enrichment, we have been able to discuss a notion of asymptotic distinguishability and to require as an axiom that a state can be identified with arbitrary precision from a sufficiently large number of copies.

Once the above notions have been put into place, we established a number of relations among the notions of distinguishability, copiability, and programming. First of all, we showed that the states in a given set are distinguishable if and only if one can generate some side information from them. From this basic result we derived two facts: *i)* the equivalence between distinguishability and copiability, and *ii)* the Cryptographic No Information Without Disturbance.

The present work is part of a larger program of categorification of the framework of operational-probabilistic theories[10], which aims at reducing the probabilistic part of the framework at the advantage of the operational one. In this spirit, an interesting open question for future research is whether the notion of state broadcasting and the no-broadcasting theorem for general probabilistic theories[29] can be imported to the probability-free scenario.

Acknowledgement

This work was supported by the National Basic Research Program of China (973)(Grants 2011CBA00300, 2011CBA00301) and by the National Natural Science Foundation of China (Grants 11350110207, 61033001, 61061130540), by the 1000 Youth Fellowship Program of China, by the Foundational Questions Institute (Grants FQXi-RFP3-1325). GC acknowledges the hospitality of Perimeter Institute for Theoretical Physics. Research at Perimeter Institute for Theoretical Physics is supported in part by the Government of Canada through NSERC and by the Province of Ontario through MRI.

References

[1] Abramsky S, Coecke B. A categorical semantics of quantum protocols. Proc. of the 19th Annual

IEEE Symposium on Logic in Computer Science. 2004. 415–425.
[2] Abramsky S, Coecke B. Categorical quantum mechanics. In: Engesser K, Gabbay DM, Lehmann D. eds. Handbook of Quantum Logic and Quantum Structures. Elsevier. 2008. 261–324.
[3] Abramsky S. No cloning in categorical quantum mechanics. In: Gay S, Mackie I, eds. Semantic Techniques in Quantum Computation. Cambridge University Press. 2010. 1–28.
[4] Awodey S. Category Theory. Oxford University Press, 2010.
[5] Barrett J. Information processing in generalized probabilistic theories. Phys. Rev. A, 2007(75): 032304.
[6] Barnum H, Barrett J, Leifer M, Wilce A. Teleportation in general probabilistic theories. Proc. of Symposia in Applied Mathematics, 2012(71): 25–48.
[7] Barnum H, Wilce A. Information processing in convex operational theories. Electronic Notes in Theoretical Computer Science, 2011, 270(1): 3–15.
[8] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Proc. of IEEE International Conference on Computers, Systems and Signal Processing. New York. 1984, 175. 8.
[9] Bennet CH. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 1992, 68. 3121.
[10] Chiribella G, D'Ariano GM, Perinotti P. Probabilistic theories with purification. Phys. Rev. A, 2010, 81: 062348.
[11] Chiribella G, D'Ariano GM, Perinotti P. Informational derivation of quantum theory. Phys. Rev. A, 2011, 84: 012311.
[12] Chiribella G, Yang Y. Confusability graphs for symmetric sets of quantum states. In: Bai CM, Gazeau JP, Ge ML, eds. Symmetries and Groups in Contemporary Physics. Nankai Series in Pure, Applied Mathematics and Theoretical Physics. 2013, 11.
[13] Chiribella G. Categorical purification. http://www.cs.ox.ac.uk/CQM2014/programme/Giulio.pdf. 2014.
[14] Chiribella G. Purity without probability, manuscript in preparation. 2014.
[15] Coecke B. Kindergarten quantum mechanics: lecture notes. AIP Conf. Proc., 2006, 810: 81–98.
[16] Coecke B. Axiomatic description of mixed states from Selinger's CPM-construction. Electronic Notes in Theoretical Computer Science, 2008, 210: 3–13.
[17] Coecke B. Quantum picturalism. Contemporary Physics, 2010, 51(1): 59–83.
[18] Hardy L. Quantum theory from five reasonable axioms. arXiv:quant-ph/0101012. 2001.
[19] Hardy L. Reformulating and reconstructing quantum theory. arXiv preprint arXiv:1104.2066. 2011.
[20] Horseman C. Quantum picturalism for topological cluster-state computing. New J. Phys. 2011, 13, 095011.
[21] Coecke B, Perdrix S. Environment and classical channels in categorical quantum mechanics. Computer Science Logic. Springer. 2010. 230–244.
[22] Coecke B, Duncan R, Kissinger A, Wang Q. Strong complementarity and non-locality in categorical quantum mechanics. Proc. of the 27th Annual IEEE/ACM Symposium on Logic in Computer Science. 2012. 245–254.
[23] Coecke B. Terminality implies non-signalling. arXiv preprint arXiv:1405.3681. 2014.
[24] Dakic B, Bruckner C. Quantum theory and beyond: Is entanglement special? In: Halvorson H, ed. Deep Beauty: Understanding the Quantum World through Mathematical Innovation. Cambridge University Press. Cambridge. 2011. 365–392.
[25] D'Ariano GM. On the missing axiom of quantum mechanics. AIP Conf. Proc. 2006, 810: 114–130.
[26] D'Ariano GM. Probabilistic theories: what is special about quantum mechanics. In: Bokulich A, Jaeger G, eds. Philosophy of quantum information and entanglement. 2010. 85.
[27] Duan R, Severini S, Winter A. Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovász θ-function. IEEE Trans. Inf. Theory, 2013, 59(2): 1164–1174.
[28] Coecke B, Lal RA. Causal categories: relativistically interacting processes. Found. Phys., 2012, 43(4): 458–501.

[29] Barnum H, Barrett J, Leifer M, Wilce A. Generalized no-broadcasting theorem. Phys. Rev. Lett., 2007, 99(24): 240501.
[30] Lovász L. On the Shannon capacity of a graph. IEEE Trans. Inform. Th. IT. 1979, 25:1.
[31] Kelly GM, Laplaza ML. Coherence for compact closed categories. Journal of Pure and Applied Algebra, 1980, 19: 193–213.
[32] Masanes L, Müller MP. A derivation of quantum theory from physical requirements. New J. Phys., 2011, 13: 063001.
[33] Masanes L, Müller MP, Augusiak R, Pérez-García D. A digital approach to quantum theory. Proc. of the National Academy of Sciences, 2013, 110: 16373.
[34] Mermin ND. Quantum Computer Science: an Introduction. Cambridge University Press, 2007.
[35] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information. Cambridge University Press, 2001.
[36] Ranchin A, Coecke B. Complete set of circuit equations for stabilizer quantum mechanics. Phys. Rev. A, 2014, 90: 012109.
[37] Spekkens RW. Evidence for the epistemic view of quantum states: A toy theory. Phys. Rev. A, 2007, 75(3): 032110.
[38] Selinger P. A survey of graphical languages for monoidal categories. In: Coecke B, ed. New Structures for Physics, Springer, 2011: 289–355.
[39] Wilde M. Quantum Information Theory. Cambridge University Press, 2007.